Държавна агенция „Електронно управление“

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

за

„Изграждане и внедряване на eIDAS възел за нуждите на трансграничната електронна идентификация“, съгласно Регламент (ЕС) 910/2014

СЪДЪРЖАНИЕ

1. РЕЧНИК НА ТЕРМИНИ, ДЕФИНИЦИИ И СЪКРАЩЕНИЯ

1.1. Използвани акроними

Акроним	Описание
ДАЕУ	Държавна агенция "Електронно управление"
ЗЕИ	Закон за електронната идентификация
ЗЕУ	Закон за електронното управление
е-Авт	Изграден в ДАЕУ хоризонтален компонент на електронното управление за електронна автентикация, чрез който се идентифицират лица и информационни системи в електронна среда
ЕС	Европейски съюз
Регламент (ЕС) 910/2014	Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 година относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО
ДХЧО	Държавен хибриден частен облак
CEF Digital	Компонент относно цифровите технологии на програмата на ЕС „Механизъм за свързване на Европа“
WSDL	Web Service Definition Language
SAML	Security Assertion Markup Language
SAML-token	XML – базирана услуга, съдържаща идентификационни данни за заявител на електронни услуги
SDK	Software development kit
API	Application programming interface/Приложно програмен интерфейс

1.2. Технологични дефиниции

Термин	Описание
Държавен хибриден частен облак	Централизирана на ниво държава информационна инфраструктура (сървъри, средства за съхранение на информация, комуникационно оборудване, съпътстващо оборудване, разпределени в няколко локации, в помещения отговарящи на критериите за изграждане на защитени центрове за данни), която предоставя физически и виртуални ресурси за ползване и администриране от секторите и структурите, които имат достъп до тях, в зависимост от

	нуждите им, при гарантиране на високо ниво на сигурност, надеждност, изолация на отделните ползватели и невъзможност от намеса в работоспособността на информационните им системи или неоторизиран достъп до информационните им ресурси. Изолацията на ресурсите и мрежите на отделните секторни ползватели (е-Общини, е-Правосъдие, е-Здравеопазване, е-Полиция) се гарантира с подходящи мерки на логическо ниво (формиране на отделни клъстери, виртуални информационни центрове и мрежи) и на физическо ниво (клетки и шкафове с контрол на достъпа).
Софтуер с отворен 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.
Електронна идентификация	Процес на използване на данни в електронна форма за идентификация на лица, които данни представляват по уникален начин дадено физическо или юридическо лице, или физическо лице, представляващо юридическо лице.
Данни за идентификация на лица	Набор от данни, които позволяват да се установи самоличността на физическо или юридическо лице или на физическо лице, представляващо юридическо лице.
Схема за електронна идентификация	Система за електронна идентификация, при която средствата за електронна идентификация се издават на физически или юридически лица, или физически лица, представляващи юридически лица.
Средство за електронна идентификация	Материална и/или нематериална единица, която съдържа данни за идентификация на лица, която се използва за удостоверяване на автентичност за онлайн услуга.
Удостоверяване на автентичност (автентикация)	Електронен процес, който позволява електронна идентификация на физическо или юридическо лице или потвърждаването на произхода и целостта на данни в електронна форма.

Електронни административни услуги (ЕАУ)	Административните услуги, предоставяни на гражданите и организациите от административните органи, услугите, предоставяни от лицата, на които е възложено осъществяването на публични функции, както и обществените услуги, които могат да се заявяват и/или предоставят от разстояние чрез използването на електронни средства.
eIDAS възел (Системата)	Точка на свързване, по смисъла на Регламент за изпълнение на Комисията (ЕС) 2015/1501, която е част от архитектурата за оперативна съвместимост на електронната идентификация и участва в трансграничното удостоверяване на автентичността на лица, като е в състояние да разпознава и обработва или препраща предавания на данни към други възли, с което дава възможност на националната инфраструктура за електронна идентификация на една държава членка да се свързва с националната инфраструктура за електронна идентификация на други държави членки. eIDAS възелът може да има различни роли като eIDAS конектор (изисква трансгранично удостоверяване на автентичността) или eIDAS услуга (предоставя трансгранично удостоверяване на автентичността).
Оператор на eIDAS възел	Субект, който е отговорен за осигуряването на правилно и надеждно функциониране на възела като точка на свързване.
eIDAS мрежа	Техническата инфраструктура, която свързва националните схеми за електронна идентификация на държавите членки на ЕС, съставена от национални eIDAS възли.
eIDAS технически спецификации	Най-актуалната към момента на внедряване на eIDAS възел версия на технически спецификации за eIDAS възел (eIDAS eID Profile), предоставени от CEF Digital, разработени от Европейската комисия с помощта на държави членки на ЕС в съответствие с Регламент (ЕС) 910/2014 и Регламент за изпълнение на Комисията (ЕС) 2015/1501. Текущата версия на eIDAS технически спецификации (v.1.1) е съставена от 4 части: eIDAS Message Format; eIDAS Interoperability Architecture; eIDAS - Crypto Requirements for the eIDAS Interoperability Framework; и eIDAS SAML Attribute Profile. Участниците могат да свалят актуална версия на eIDAS технически спецификации от Интернет страницата на CEF Digital[1] или да получат копие от ДАЕУ при поискване.
eIDAS примерен софтуер	Най-актуалната към момента на внедряване на eIDAS възел версия на софтуер, предоставен от CEF Digital, разработен от Европейската комисия с помощта на държави членки на ЕС в

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Profile

	съответствие с eIDAS технически спецификации. Текущата версия на eIDAS примерен софтуер (v.2.0) е съставена от два инструмента: eIDAS възел и инструменти за тестване, включително демо-доставчик на електронни услуги и демо-издател на средства за електронна идентификация. Участниците могат да свалят актуална версия на eIDAS примерен софтуер от Интернет страницата на CEF Digital[2] или да получат копие от ДАЕУ при поискване.

2. ВЪВЕДЕНИЕ

2.1. Цел на документа

Целта на настоящия документ е да опише изискванията към изпълнението на обществена поръчка с предмет: „Изграждане и внедряване на eIDAS възел за нуждите на трансграничната електронна идентификация", съгласно Регламент (ЕС) 910/2014".

2.2. За възложителя – функции и структура

Възложител на настоящата обществена поръчка е Държавна агенция „Електронно управление" (ДАЕУ).

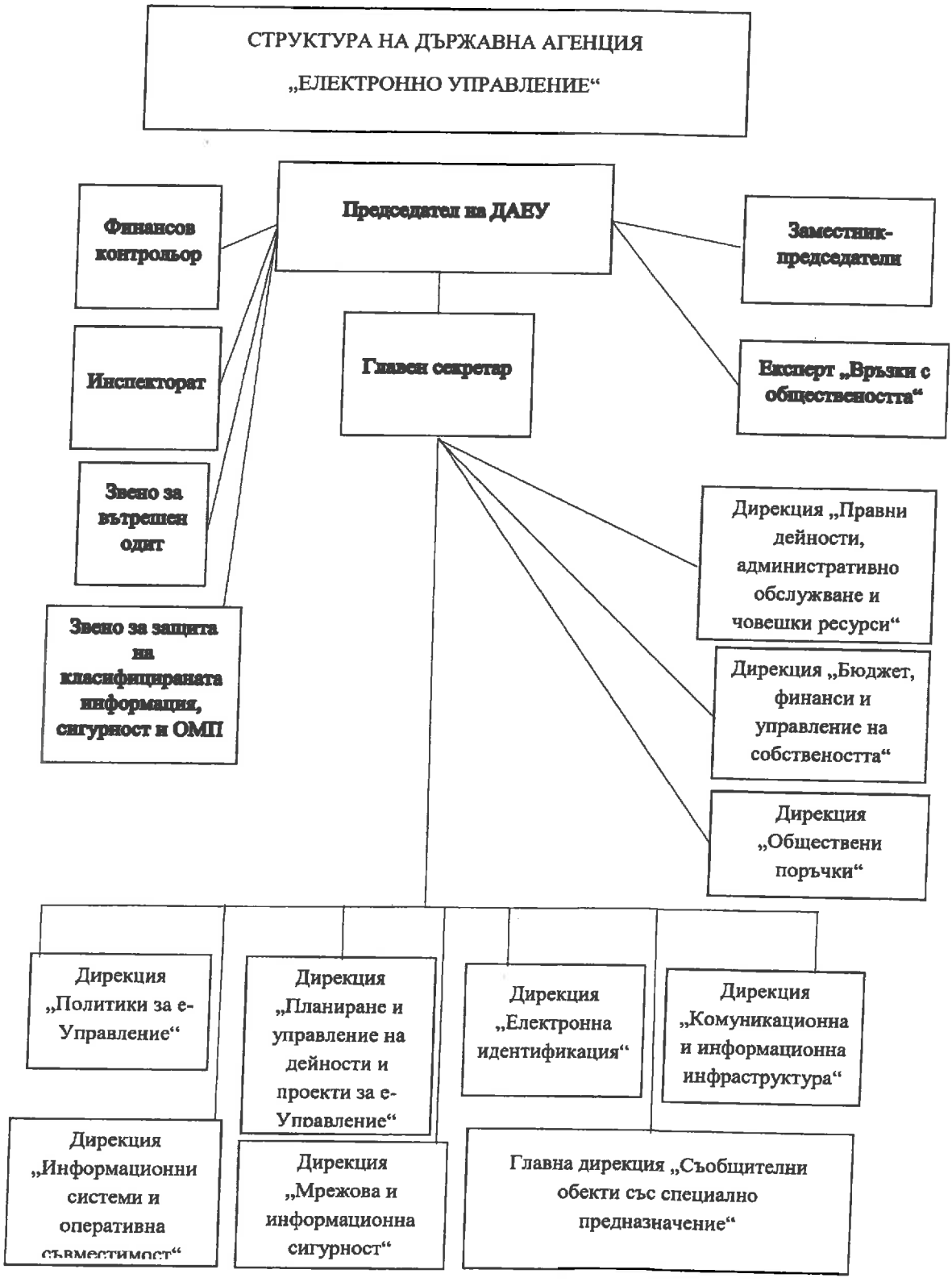
ДАЕУ е създадена към Министерския съвет и е юридическо лице на бюджетна издръжка със седалище в гр. София. Тя се ръководи и представлява от председател, който е първостепенен разпоредител с бюджет.

ДАЕУ има функции по издаване, налагане и контрол на политики, правила и добри практики в областта на електронното управление, стратегическо планиране и инициативи, бюджетно програмиране и контрол, координация на секторни политики, секторни и междуведомствени проекти. Агенцията поддържа централизирани регистри за нуждите на електронното управление, други централизирани регистри, държавен частен облак и комуникационната мрежа на държавната администрация.

ДАЕУ осъществява сътрудничество и взаимодействие по въпросите на електронното управление с компетентните органи на държавите членки на Европейския съюз (ЕС), с институциите на ЕС и други международни организации.

Структурата на ДАЕУ е представена във Фигура 1:

[2] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Node+integration+package



Фигура 1. Структура на ДАЕУ

2.3. За проекта

Проектът се реализира в съответствие с изпълнението на стратегическите цели и дейности по присъединяване на електронното управление на Република България към инициативата за трансгранична електронна идентификация, предвидени в Пътната карта за изпълнение на Стратегията за развитие на електронното управление в Република България 2016 – 2020 г.

Настоящата обществена поръчка се възлага във връзка с изпълнението на изискванията на чл. 6, т. 1 от Регламент (ЕС) 910/2014, относно задължителното признаване на средствата за електронна идентификация, издадени в други държави членки в рамките на схема за електронна идентификация, за която е извършено уведомяване пред Европейската комисия (ЕК).

2.4. Необходимост от реализация на проекта

През 2014 г. е приет Регламент (ЕС) 910/2014, който урежда електронната идентификация и редица доверителни услуги в целия ЕС. Една от целите на Регламента е да се премахнат съществуващите бариери пред трансграничната употреба на използваните в отделните държави членки средства за електронна идентификация. С него не се цели намеса по отношение на системите за управление на електронната самоличност и свързаните с тях инфраструктури, установени в държавите членки на ЕС. Целта е да се гарантира, че при достъпа до трансгранични електронни услуги, предлагани от държавите членки, е възможно да се осъществят сигурна електронна идентификация и сигурно електронно удостоверяване на автентичност на гражданите на ЕС.

В тази връзка до 29 септември 2018 г. държавите членки могат доброволно да признават средствата за електронна идентификация, издадени в друга държава членка в рамките на схема за електронна идентификация, за която е извършено уведомяване по чл. 9 от Регламент (ЕС) 910/2014 и която отговаря на изискванията на регламента. След тази дата такова взаимно признаване става задължително.

Следователно след 29 септември 2018 г. Република България ще бъде задължена да признава средствата за електронна идентификация, издадени в други държави членки, доколкото тези средства се издават в рамките на схема за електронна идентификация, за която е извършено уведомяване и които съответстват на ниво на осигуреност „значително" или „високо". Това ще позволи на граждани да използват своите средства за електронна идентификация, издадени в други държави членки за достъп до електронни административни услуги в България.

С влезлите в сила от 01 юли 2016 г. изменения в ЗЕУ председателят на ДАЕУ осигурява интеграция на информационните системи на административните органи с тези на държавите членки на ЕС, с цел създаване

на възможност за предоставяне на трансгранични електронни административни услуги.

За да се реализира взаимното признаване, е необходимо на национално равнище да бъде осигурена двукомпонентна технологична инфраструктура (хардуер/софтуер), която да осигури надеждно трансгранично удостоверяване на автентичност и да гарантира оперативната съвместимост със схемите за електронна идентификация, за които е извършено уведомяване. Централен компонент на тази инфраструктура е eIDAS възелът, който участва в трансграничното удостоверяване на автентичността на гражданите. Чрез него се приемат, обработват и препращат данни към други възли, с което се дава възможност на националната инфраструктура за електронна идентификация на една държава членка да се свързва с инфраструктурата на друга държава членка.

2.5. Финансиране

Проектът се финансира от бюджета на ДАЕУ. Финансовият ресурс, определен от Възложителя, за настоящата поръчка е до **70 000 (седемдесет хиляди) лева без включен ДДС.**

В стойността на услугата следва да се включат:

- Всички разходи по дейностите, включени в предмета на поръчката;
- Гаранционна поддръжка.

Определената от Изпълнителя цена да включва всички разходи за цялостно изпълнение на поръчката.

В случай че изпълнител предложи по-висока стойност, той ще бъде предложен за отстраняване от процедурата, на основание чл. 107, т. 2 , буква „а" ЗОП, тъй като не отговаря на предварително обявените условия на поръчката.

2.6. Нормативна рамка

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

- Стратегията за развитие на електронното управление в Република България 2014 – 2020 г.
- Пътна карта за изпълнение на Стратегията за развитие на електронното управление в Република България 2016 – 2020 г.;
- Закон за електронното управление;
- Закон за електронната идентификация;
- Закон за електронния документ и електронните удостоверителни услуги;

- Закон за обществените поръчки;
- Закон за защита на личните данни;
- Закон за достъп до обществена информация;
- Правилник за прилагане на Закона за електронната идентификация;
- Наредба за общите изисквания към информационните системи, регистрите и електронните административни услуги;
- Регламент (ЕС) 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентичност и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО;
- Регламент за изпълнение (ЕС) 2015/1501 на Комисията от 8 септември 2015 г. относно рамката за оперативна съвместимост съгласно чл. 12, параграф 8 от Регламент (ЕС) 910/2014 на Европейския парламент и на Съвета относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар;
- Регламент за изпълнение (ЕС) 2015/1502 на Комисията от 8 септември 2015 година за определяне на минимални технически спецификации и процедури за нивата на осигуреност за средствата за електронна идентификация съгласно член 8, параграф 3 от Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар.
- Международен стандарт ISO/EIC 29115
- Други

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

3.1. Общи и специфични цели на проекта

Проектът е насочен към изпълнението на задължението на Република България по чл. 6 от Регламент (ЕС) 910/2014 за взаимно признаване на средства за електронна идентификация, издадени в друга държава членка на ЕС, за целите на трансграничното удостоверяване на автентичност при достъп до ЕАУ, предоставяни в Република България. Цели се също осигуряване на технологична възможност за достъп до ЕАУ, предоставяни от органи от публичния сектор в други държави членки, чрез използване на средства за електронна идентификация, издадени в Република България, в рамките на

национална схема за електронна идентификация, за която е извършено уведомяване по смисъла на чл. 9 от Регламент (ЕС) 910/2014.

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

▪ Изграждане на eIDAS възел за трансгранична електронна идентификация на лица, притежаващи средство за електронна идентификация, издадено в рамките на национална схема за електронна идентификация на държава членка на ЕС, за която е извършено уведомяване;

▪ Сигурен защитен обмен на данни за електронната идентичност на лица при заявяването на ЕАУ, предоставяни от органи от публичния сектор в държави членки на ЕС;

▪ Осигуряване на системна интеграция на разработеният и внедрен eIDAS възел с разработената за нуждите на електронното управление хоризонтална система е-Авт. е–Авт осигурява еднократна автентикация на потребителите на електронни услуги, чрез интеграцията и със системите на лицата по чл.1 от ЗЕУ, чрез които се заявяват електронни услуги.

3.2. Обхват на проекта

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

▪ Дейност 1 – Проучване и оценка на възможностите за реализиране на eIDAS възел чрез използване на наличните хардуерни ресурси, с който разполага ДАЕУ, както и възможната нужда от осигуряване на допълнителни хардуерни компоненти;

▪ Дейност 2 - Изграждане и внедряване в продукционна среда на eIDAS възел в съответствие с eIDAS технически спецификации и с използване на разработеният и предоставен за ползване от държавите членки eIDAS примерен софтуер за нуждите на трансграничната електронна идентификация, съгласно чл. 6 от Регламент (ЕС) № 910/2014;

▪ Дейност 3 - Свързване на eIDAS възела с eIDAS мрежата;

▪ Дейност 4 – Интеграция на eIDAS възела с хоризонталната система е-Авт;

▪ Дейност 5 – Провеждане на тестове на eIDAS възела с използване на инструментите за тестване, предоставени от CEF Digital (eIDAS conformance testing service), чрез свързване с eIDAS възли на други държави членки на ЕС и с доставчици на ЕАУ посредством е-Авт, включително и заявяване на ЕАУ или

достъп до ресурсите на електронното управление чрез средство за електронна идентификация на физическо лице, издадено от държава членка;

▪ Дейност 6 - Изготвяне на документация за софтуерни разработчици, ключови потребители и администратори;

▪ Дейност 7 – Обучение на минимум 3 служителя от ДАЕУ за администриране на eIDAS възела;

▪ Дейност 8 – Гаранционна поддръжка на eIDAS възела за период от минимум 12 месеца след приемането му в експлоатация.

3.3. Целеви групи

Целевите групи, към които е насочен проектът, обхващат:

▪ ДАЕУ;

▪ Административните органи, лицата, осъществяващи публични функции, и организациите, предоставящи обществени услуги;

▪ Физически и юридически лица, които притежават средства за електронна идентификация, издадени в рамките на национална схема за електронна идентификация, за която е извършено уведомяване съгласно чл. 9 от Регламент (ЕС) 910/2014.

3.4. Очаквани резултати

Очакваните резултати от изпълнението на настоящата поръчка са:

▪ Изграден, тестван и въведен в експлоатация върху ресурсите на ДАЕУ eIDAS възел, в съответствие с изискванията на Регламент (ЕС) 910/2014 и с eIDAS технически спецификации, който е интегриран както с eIDAS мрежата, така и с е-Авт, и разполага с функционалностите, необходими за взаимно признаване на средства за електронна идентификация, издадени в държави членки на ЕС съгласно чл. 6 от Регламент (ЕС) 910/2014;

▪ Пълна техническа и експлоатационна документация относно eIDAS възела и интеграцията му с е-Авт, включително подробни технически спецификации и документация за софтуерни разработчици, ключови потребители и администратори.

▪ Проведено обучение на минимум 3 служителя от ДАЕУ за администриране на eIDAS възела.

3.5. Период на изпълнение

Периодът на изпълнение е 3 месеца, но не по късно от **01 септември 2018 г.**

Участниците трябва да изготвят подробен график, в който следва да се конкретизират сроковете за изпълнение на всяка дейност от настоящата поръчка. Графикът за изпълнение трябва да бъде съобразен с продължителността на дейността и не може да надвишава 3 месеца от дата на сключване на договора, но не по-късно от крайния срок на изпълнение на проекта **01 септември 2018 г.**

4. ТЕКУЩО СЪСТОЯНИЕ

След създаването на ДАЕУ държавната политика в областта на електронното управление се насочи към последователно и целенасочено развитие на хоризонталните компоненти и централни системи на електронното управление. Интеграцията с хоризонталните компоненти постепенно започна да става задължителна за информационните системи на администрацията.

Хоризонталната система е-Авт собственост на и поддържана от ДАЕУ е модул за идентификация на заявители на ЕАУ. Съществено предимство при използването на е-Авт е отпадането на необходимостта от надграждане на системите на администрациите при появата на ново средство за електронна идентификация (мобилно устройство, банкова карта, национална схема за електронна идентификация и др.). Новото средство се интегрира еднократно единствено със системата за е-Авт, която взаимодейства с всички останали системи и им предоставя новата възможност за идентификация.

е-Авт, реализира Single Sign-On функция, като издава атестати, идентифициращи потребителите (физически и юридически лица, информационни системи) в информационната среда на електронното управление. Атестатите важат за времето, в което потребителят има активна сесия в рамките на електронното управление, т.е. в системата, през която е осъществил вход и идентификация. В рамките на сесията на потребителя, атестатът се предава през защитен протокол „система-система“ към всяка следващата система, която участва в процеса, като на всяка стъпка може да бъде валидиран от е-Авт чрез автоматизирана услуга.

В атестата, издаван от е-Авт, не се пренасят чувствителни данни за идентифицираните лица, а само дискретни референции, чрез които необходимите данни могат да бъдат извлечени през програмен интерфейс, достъпен по защитен канал в инфраструктурата на електронното управление.

Необходимо е разширяване на функционалностите на модула, за да се изпълнят изискванията на Регламент (ЕС) № 910/2014 и да се осъществи

интеграция с eIDAS възел за взаимно свързване на схемите за електронна идентификация на държавите членки. Тази интеграция би позволила електронни услуги, предоставяни от административни органи в България и свързани с модула за е-Авт, да бъдат достъпвани чрез средствата за електронна идентификация, издадени от други държави членки и нотифицирани съгласно чл. 9 от Регламент (ЕС) 910/2014.

5. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕ НА ПОРЪЧКАТА

5.1. Общи изисквания към изпълнението на обществената поръчка

Обществената поръчка с предмет „Изграждане и внедряване на eIDAS възел за нуждите на трансграничната електронна идентификация", съгласно Регламент (ЕС) 910/2014 се финансира от бюджета на ДАЕУ. Изпълнителят следва да спазва всички нормативни изисквания по отношение на дейността на ДАЕУ и електронното управление в Република България, както и изискванията на приложимото законодателство на ЕС.

eIDAS възелът трябва да бъде функциониращо национално звено за трансгранична електронна идентификация и да е в пълно съответствие с изискванията на Регламент (ЕС) 910/2014 и подзаконовата нормативна уредба към него.

В тази връзка eIDAS възелът трябва да отговаря на eIDAS технически спецификации. В случай, че до въвеждането в експлоатация на eIDAS възела бъде публикувана нова версия на eIDAS технически спецификации, изпълнителят трябва да разработи eIDAS възела в съответствие с тази нова версия.

Изпълнителят трябва да се запознае, прегледа и анализира eIDAS Building Blocks, като използва предоставените от CEF Digital компоненти и услуги във възможно най-голяма степен при изпълнението на настоящата обществена поръчка, включително eIDAS примерен софтуер и услугите за тестване на eIDAS възел. В тази връзка, при изграждане на eIDAS възела, Изпълнителят трябва да променя, допълва и надгражда предоставения от CEF Digital примерен софтуер за eIDAS възел само доколкото това е необходимо за постигане на функционалностите описани в това техническо задание, включително интеграция на eIDAS възела с е-Авт.

Изпълнителят да разгледа и анализира и пилотният проект STORK 2.0 (https://www.eid-stork2.eu) относно това, кои компоненти могат да бъдат преизползвани при изпълнението на настоящата обществена поръчка.

5.2. Общи организационни принципи

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

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

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

Участникът трябва да прилага система за управление на сигурността на информацията, съответстваща на стандарт **БДС EN ISO 27001** или еквивалентен, с обхват: разработване, внедряване и поддръжка на софтуерни продукти и информационни системи, което се доказва със сертификат. Сертификатът трябва да е валиден и да е издаден от независими лица, които са акредитирани по съответната серия европейски стандарти от Изпълнителна агенция „Българска служба за акредитация“ или от друг национален орган по акредитация, който е страна по Многостранното споразумение за взаимно признаване на Европейската организация за акредитация, за съответната област или да отговарят на изискванията за признаване съгласно чл. 5а, ал. 2 от Закона за националната акредитация на органи за оценяване на съответствието. Възложителят приема еквивалентни сертификати, издадени от органи, със седалище в други държави членки.

Когато участникът не е имал достъп до такъв сертификат или е нямал възможност да го получи в съответните срокове по независещи от него причини, той може да представи други доказателства за еквивалентни мерки за система за управление на сигурността на информацията. В тези случаи участникът трябва да е в състояние да докаже, че предлаганите мерки са еквивалентни на изискваните.

Участникът, определен за изпълнител, трябва да има валиден сертификат през целия срок на изпълнение на договора, а когато е приложимо да прилага еквивалентните мерки.

Участникът трябва да прилага система за управление на ИТ услуги, съответстваща на стандарт **БДС EN ISO 20000-1** или еквивалентен, което се доказва със сертификат. Сертификатът трябва да е с обхват: предоставяне на услуги по проектиране, разработване, внедряване и поддръжка на информационни системи, да е валиден и да е издаден от независими лица, които са акредитирани по съответната серия европейски стандарти от Изпълнителна агенция „Българска служба за акредитация" или от друг национален орган по акредитация, който е страна по Многостранното споразумение за взаимно признаване на Европейската организация за акредитация, за съответната област или да отговарят на изискванията за признаване съгласно чл. 5а, ал. 2 от Закона за националната акредитация на органи за оценяване на съответствието. Възложителят приема еквивалентни сертификати, издадени от органи, установени в други държави членки.

Когато участникът не е имал достъп до такъв сертификат или е нямал възможност да го получи в съответните срокове по независещи от него причини, той може да представи други доказателства за еквивалентни мерки за система за управление на ИТ услугите. В тези случаи участникът трябва да е в състояние да докаже, че предлаганите мерки са еквивалентни на изискваните.

Участникът, определен за изпълнител, трябва да има валиден сертификат през целия срок на изпълнение на договора, а когато е приложимо да прилага еквивалентните мерки.

5.3. Управление на проекта[3]

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

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

Доброто управление на проекта трябва да осигури:

[3] Под „проект" следва да се разбира предметът на настоящата обществена поръчка

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

Методологията трябва да включва подробно описание на:

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

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

5.4. Управление на риска

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

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

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

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

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

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

6. ЕТАПИ НА ИЗПЪЛНЕНИЕ НА ПРОЕКТА

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

6.1. Анализ на наличните в ДАЕУ ресурси

Изпълнителят трябва да проучи и оцени възможностите за реализиране на eIDAS възел чрез използване на наличните хардуерни ресурси, с който разполага ДАЕУ, както и възможната нужда от осигуряване на допълнителни хардуерни ресурси. До 15 дни от началото на изпълнението на проекта Изпълнителят трябва да предостави на Възложителя така изготвената оценка, в която ясно да е посочено дали наличните в ДАЕУ хардуерни ресурси са достатъчни за реализиране на eIDAS възел. В случай, че бъде идентифицирана нужда от осигуряване на допълнителни ресурси, те трябва подробно да бъдат описани в оценката, изготвена от Изпълнителя.

6.2. Изготвяне на системен проект

Изпълнителят трябва да изготви системен проект, който подлежи на одобрение от Възложителя. В системния проект трябва да са описани всички изисквания за реализирането на eIDAS възела, изисквания за изграждане на служебен интерфейс към е-Авт и изготвяне на тестови сценарии за тестване с доставчик на електронни административни услуги в България. Изготвянето на системния проект включва следните основни задачи:

- Определяне на концепция на разработка на eIDAS възела на базата на техническото задание;
- Дефиниране на детайлни изисквания и бизнес процеси, които трябва да се реализират в eIDAS възела;
- Дизайн на системните модули, обхванатите интерфейси между тях, връзките с е-Авт, както и разработката на самостоятелните функционални модули. Предложеният системен дизайн трябва да включва дизайн на техническата инфраструктура, както и разположението на софтуерните модули в нея;
- Изготвяне на план за техническа реализация;
- Определяне на служебния интерфейс.

При документирането на изискванията, с цел постигане на яснота и стандартизация на документите, е необходимо да се използва стандартен език за описание на бизнес процеси – BPMN или еквивалент. Системният проект е необходимо да бъде разработен до 10 работни дни след утвърждаване на функционалната спецификация от Възложителя.

Системният проект подлежи на одобрение от Възложителя. В случай на забележки, корекции или допълнения от страна на Възложителя Изпълнителят е длъжен да ги отрази в системния проект в срок не по-късно от 5 работни дни.

6.3. Разработване на софтуерното решение

Етапът на изработване включва изпълнението на следните задачи:

- Разработка на модулите на eIDAS възела съгласно изискванията на настоящото техническо задание (включително eIDAS конектор и eIDAS услуга) и системния проект при използване на eIDAS примерен софтуер във възможно най-голяма степен;
- Разработване на служебен интерфейс, касаещ системна интеграция на eIDAS възел с хоризонталната система е-Авт;
- Провеждане на вътрешни тестове на eIDAS възела (в среда на разработчика);
- Изготвяне на детайлни сценарии за провеждане на приемателните тестове за етапи „Тестване“ и „Внедряване“ на проекта.

Представянето на софтуерните приложения и служебните интерфейси включват описание и документация на Source-кода на същите и самия Source-код на технически носител, като същия се съпровожда от документ за извършено вътрешно тестване и контрол на качеството за всички компоненти на софтуера съгласно вътрешните правила на Изпълнителя.

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

6.4. Тестване

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

След завършване на изработката на софтуерното решение се извършва тестване от представители на Изпълнителя и на Възложителя в необходимия брой итерации (повторения).

Изпълнителят има задължението да извърши инсталация на системата и всички необходими настройки за експлоатацията ѝ в тестова среда.

Изпълнителят следва да предложи и опише етапите, през които ще премине тестването.

Тестването се извършва от представители на Изпълнителя в присъствието на експерти на Възложителя, в тестовата среда на Възложителя и по предварително уговорен и утвърден между Възложителя и Изпълнителя график.

Изпълнителят следва да подготви тестови сценарии, обхващащи цялостно общите изисквания към eIDAS възела и функционалността му, логически обособените му компоненти и интеграцията помежду им, както и системната интеграция с хоризонталния модул е-Авт.

Всеки етап на тестването следва да приключи с протокол, който да съдържа обхвата на теста (тестови сценарии), резултатите от тестването и забележките на Възложителя. Броят на етапите на тестването се определя от удовлетвореността на Възложителя от реализацията на системата на база изпълнението на дефинираните изисквания на Възложителя.

Последният етап на тестването е приемателното тестване, при което се отчита изпълнението на дефинираните изисквания на Възложителя, съдържащи се в това техническо задание, като съответствието на реализацията с функционалната и това техническо задание, както и представянето на системата при големи натоварвания.

В процеса на тестване трябва да се използват в тяхната цялост инструментите за тестване, предоставени от CEF Digital (CEF eID Conformance Testing Service), като се проведат всички предвидени в тях тестове.

eIDAS възелът следва да се тества за работа с доставчик на електронни административни услуги в България (посредством е-Авт), eIDAS възел в поне една друга държава членка на ЕС и централната платформа за тестове, предоставена от CEF Digital.

6.5. Внедряване

Изпълнителят трябва да внедри софтуерното решение в информационната и комуникационна среда на ДАЕУ. Това включва инсталиране, конфигуриране и настройка на програмните компоненти на eIDAS възела в условията на експлоатационната среда на ДАЕУ.

За всяка промяна в програмното решение екипът на Изпълнителя ще предоставя билд с нова подверсия, пач и т.н. в електронен формат, който ще е придружен от следните документи:

- Описание на направените промени (release notes).
- Документ (release content), съдържащ номерата и кратко описание на проблемите или възложеното актуализиране, които влизат в билда, както и кои модули на приложния слой на програмното решение са засегнати от промените.
- Инструкция за инсталация, описваща последователността от действия по инсталиране на предоставения билд.
- Преди внедряване на промяна в програмното решение на eEIDAS възела и свързаната с него интеграция с е-Авт , екипът на Изпълнителя следва да представи пред представители на Възложителя направените промени в софтуерното решение на ниво програмен код за наличие на неоптимизиран, зловреден или злонамерен код.

За всеки билд (и за тестова, и реална среда) Изпълнителят предоставя на Възложителя протокол на хартиен носител в два екземпляра (по един за Изпълнител и Възложителя) придружен от носител на информация - CD/DVD съдържащ промените.

6.6. Обучение

Изпълнителят трябва да организира и да проведе обучения от 3 дни за трима служители на ДАЕУ, ангажирани с администрирането на eIDAS възела. Обучението включва следните дейност:

- Инсталация на eIDAS възела в продукционна среда на Възложителя;
- Процедури по възстановяване на системата след срив на същата и възможност за миграция към по-нова версия на програмната реализация;
- Функциониране и поддръжка на eIDAS възела;
- Тестване.

За провеждането на обученията Изпълнителят е длъжен да осигури за своя сметка учебни материали и лектори.

6.7. Гаранционна поддръжка

Изпълнителят трябва да осигури за своя сметка гаранционна поддръжка за период от минимум 12 месеца след приемане в експлоатация на системата.

При необходимост, по време на гаранционния период трябва да бъдат осъществявани дейности по осигуряване на експлоатационната годност на eIDAS възела и ефективното му използване от Възложителя, в случай че настъпят явни отклонения от нормалните експлоатационни характеристики, заложени в системния проект, както и в случай на промени в eIDAS техническите спецификации (настъпили след внедряване на eIDAS възела в експлоатация) по отношение на оперативната съвместимост на eIDAS възела с eIDAS възли на други държави членки на ЕС.

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

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

Минималният обхват на поддръжката трябва да включва:

- Извършване на диагностика на докладван проблем с цел осигуряване на правилното функциониране на системите и модулите;
- Отстраняване на дефектите, открити в софтуерните модули, които са модифицирани или разработени в обхвата на проекта;
- Консултации за разрешаване на проблеми по предложената от Изпълнителя конфигурация на средата (операционна система, база данни, middleware, хардуер и мрежи), използвана от приложението, включително промени в конфигурацията на софтуерната инфраструктура на мястото на инсталация;
- Възстановяването на системата и данните при евентуален срив на системата, както и коригирането им в следствие на грешки в системата;
- Експертни консултации по телефон и електронна поща за системните администратори на Възложителя за идентифициране на дефекти или грешки в софтуера;
- Актуализация и предаване на нова версия на документацията на системата при установени явни несъответствия с фактически реализираните функционалности, както и в случаите, в които са извършени действия по отстраняване на дефекти и грешки, в рамките на гаранционната поддръжка.

Времето за отговор в случай на заявка за поддръжка, изпратена по e-mail при открити проблеми във функционирането на eIDAS възела е 6 часа, а срокът за отстраняване е до 24 часа.

7. ОБЩИ ИЗИСКВАНИЯ ЗА ИНФОРМАЦИОННИ СИСТЕМИ В ДЪРЖАВНАТА АДМИНИСТРАЦИЯ

7.1. Функционални изисквания към информационната система

7.1.1. eIDAS възел

7.1.1.1. Общи положения

eIDAS мрежата се състои от eIDAS възли, внедрени на ниво държави членки на ЕС. eIDAS решението има следните възможности:

1. Изискване на трансгранична автентикация

Когато доставчик на електронни услуги (Service Provider), свързан с национална схема за електронна идентификация, получи заявка за услуга от потребител от друга държава членка, тази заявка за услуга се препраща от eIDAS възела на държавата на доставчика (приемащата държава членка) чрез eIDAS конектор (eIDAS Connector) с искане за трансгранична автентикация към eIDAS възела в държавата на потребителя (изпращащата държава членка).

2. Предоставяне на трансгранична автентикация

eIDAS възелът в държавата на потребителя (изпращащата държава членка), заявил услуга в друга държава, предоставя трансгранична автентикация чрез eIDAS услуга (eIDAS Service). Тази eIDAS услуга може да се осъществи по два начина:

- **eIDAS прокси услуга (eIDAS Proxy Service)**: eIDAS услуга, управлявана в изпращащата държава членка и предоставяща лични идентификационни данни.

- **eIDAS Middleware услуга**: eIDAS услуга, използваща Middleware. Тази услуга, също така, изисква приставка (plugin) за Middleware услуга (предоставена от изпращащата държава членка) да бъде интегрирана в eIDAS възела на получаващата държава, която не използва Middleware, и която предоставя лични идентификационни данни.

Поради разграничението между eIDAS прокси услуга и eIDAS Middleware услуга, са възможни ***четири различни комбинации по отношение на искането или предоставянето на трансгранична автентикация***:

- **прокси услуга към прокси услуга**: потребител от държава с eIDAS прокси услуга заявява електронна услуга в друга държава с eIDAS прокси услуга;
- **Middleware услуга към прокси услуга**: потребител от държава с eIDAS Middleware услуга заявява електронна услуга в държава с eIDAS прокси услуга;
- **прокси услуга към Middleware услуга**: потребител от държава с eIDAS прокси услуга заявява електронна услуга в държава с eIDAS Middleware услуга;
- **Middleware услуга към Middleware услуга**: потребител държава с eIDAS Middleware услуга заявява електронна услуга в държава с eIDAS Middleware услуга.

7.1.1.2. Осигуряване на общи интерфейси

Тъй като е необходимо различни страни да бъдат свързани с eIDAS мрежата, ***eIDAS възелът осигурява четири различни интерфейса***:

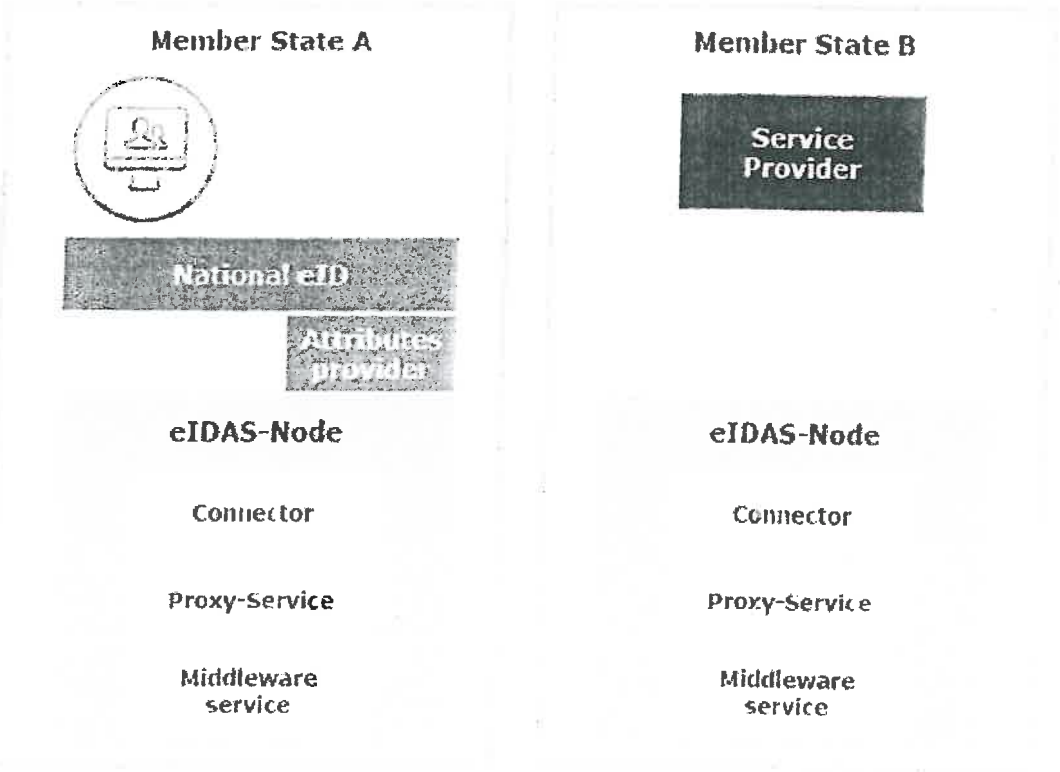
- **Интерфейс за национални доставчици на идентичност** (издатели на средства за електронна идентификация и центрове за електронна идентификация) **и доставчици на атрибути** (управляват информация относно електронна идентичност, която е в допълнение на минималния набор от данни): този интерфейс е специфичен за всяка държава-членка и се използва за свързване на eIDAS възела в държавата-членка на потребителя с неговите национални доставчик на идентичност и доставчик на атрибути. В България, свързването на eIDAS възела с националните доставчици на идентичност и на атрибути следва да се осъществи посредством интеграция с е-Авт;
- **Интерфейс за доставчиците на електронни услуги в държавата-членка, в която е разположен eIDAS възелът:** чрез този интерфейс, доставчикът на електронни услуги изпраща искания за автентикация до eIDAS-възела и получава отговорът за автентикация. В България, свързването на eIDAS възела с доставчиците на електронни услуги следва да се осъществи посредством интеграция с е-Авт;
- **Интерфейс за други eIDAS-възли в държави-членки с eIDAS прокси услуга:** Този интерфейс се осъществява чрез eIDAS услуга от едната страна и eIDAS конектор от другата страна. Те съответно изискват и предоставят информация за идентичността към другия eIDAS възел;

▪ **Интерфейс за потребители, които заявяват достъп до доставчик на електронни услуги:** Този интерфейс се използва за комуникация между eIDAS-възела и прокси на потребителя чрез неговия браузъра. Използва се, когато се поиска от потребителя да избере страната си на произход. В България тази функционалност следва да се осигури посредством интеграцията на eIDAS възела с е-Авт.

▪ **Интерфейс за предоставяне на информация за настъпили събития към Журнала на събитията**, който е елемент от хоризонталната система е-Авт на електронното управление.

7.1.1.3. Преглед на ключовите компоненти

Целта на eIDAS решението е да се постигне максимална степен на оперативна съвместимост между различни национални и международни схеми за идентификация. Диаграмата по-долу илюстрира основните компоненти в eIDAS решението.



Видно от графиката, ключовите компоненти на eIDAS решението са следните:

▪ Две държави-членки (Member State A & B) – държава А и държава Б; в примера и двете са държави с eIDAS прокси услуга и не работят със собствен Middleware;

▪ Потребител (гражданин);

▪ Доставчик на електронни услуги (Service Provider) – публични администрации и частни доставчици на електронни услуги;

▪ eIDAS-възел (eIDAS-Node) в държавата-членка на доставчика на електронни услуги;

▪ eIDAS-възел (eIDAS-Node) в държавата-членка на потребителя, състоящ се от:

▪ четири интерфейса (описани по-горе в това техническо задание);

▪ eIDAS конектор (Connector);

▪ eIDAS прокси услуга (Proxy-Service);

▪ Една или повече приставки за Middleware (при необходимост) за комуникация с държави с eIDAS Middleware услуга;

▪ Национален доставчик на идентичност (National eID) в държавата-членка на потребителя;

▪ Доставчик на атрибути (Attributes Provider) в държавата-членка на потребителя.

В България, ще има и допълнителен компонент – е-Авт. Чрез интеграция с е-Авт, eIDAS възелът ще се свързва с национални доставчици на идентичност и атрибути, както и с доставчиците на електронни услуги в България.

7.1.1.4. Примерни модели на взаимодействие

i. От държава с eIDAS прокси услуга към държава с eIDAS прокси услуга

Основни компоненти:

▪ Две държави-членки – държава А и държава Б; и двете са държави с eIDAS прокси услуга и не работят със собствен Middleware;

▪ Потребител (гражданин);

▪ Доставчик на електронни услуги (публични администрации и частни доставчици на електронни услуги);

▪ eIDAS-възел в държавата-членка на доставчика на електронни услуги;

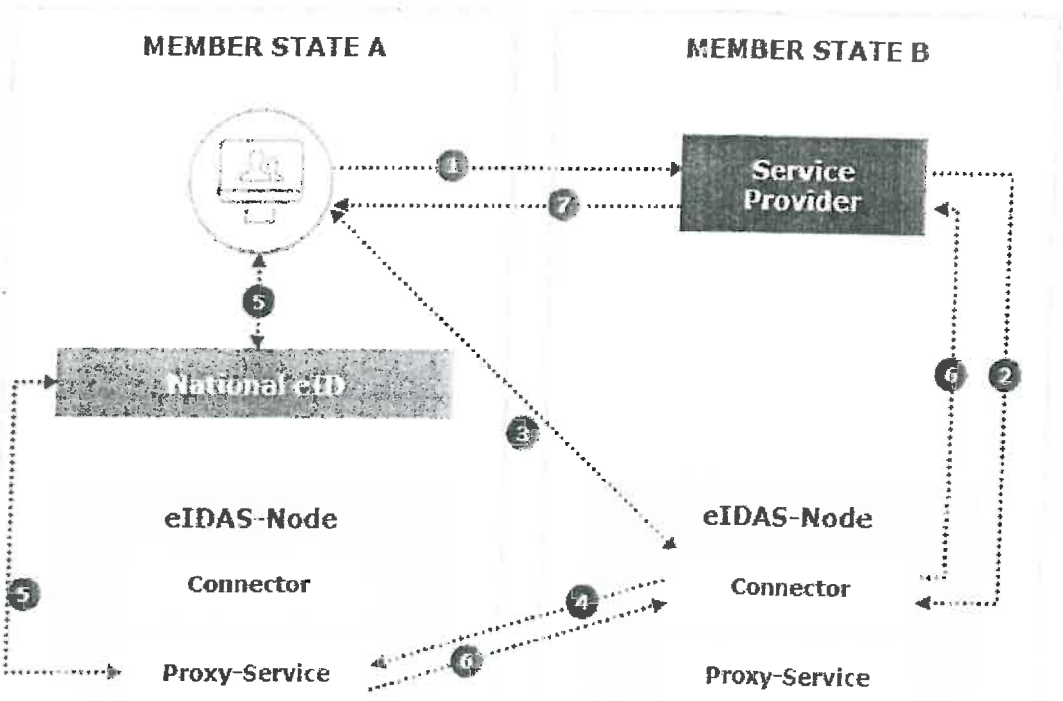
▪ eIDAS-възел в държавата-членка на потребителя, състоящ се от:

- четири интерфейса;
- eIDAS конектор;
- eIDAS прокси услуга;

▪ Национален доставчик на идентичност на държавата-членка на потребителя;

▪ Доставчик на атрибути на държавата-членка на потребителя.

В България, ще има и допълнителен компонент – е-Авт. Чрез интеграция с е-Авт eIDAS възелът ще се свързва с национални доставчици на идентичност, както и с доставчиците на електронни услуги в България.



Описание на хипотезата:

1. Потребителят от държава-членка А заявява услуга от доставчик на електронни услуги в държава-членка Б;
2. Доставчикът на електронни услуги в държавата Б изпраща искане до eIDAS конектор в същата държава. Ако България е държава Б, то eIDAS конекторът ще се свърже с доставчик на електронни услуги посредством интеграцията с е-Авт;

3. При получаване на искането, eIDAS конекторът на държавата Б пита потребителя за страната му на произход (протокол TLS). Ако България е държава Б, то тази стъпка ще се осъществи посредством интеграцията на eIDAS конектора с е-Авт;
4. Когато страната на произход бъде посочена от потребителя, SAML искането се препраща от eIDAS конектора към eIDAS прокси услугата на държавата-членка на потребителя – държава А;
5. eIDAS прокси услугата изпраща SAML искане до националния доставчик на идентичност за автентикация. Потребителят се автентикира, използвайки националната си електронна идентичност. След като бъде удостоверена, тази идентичност се връща на eIDAS прокси услугата. В зависимост от изпълнението може да има две допълнителни подстъпки в стъпка 5:

   - потребителят да избере атрибутите, които трябва да бъдат предоставени (следователно да даде съгласие)
   - потребителят да приеме стойностите на атрибутите, които трябва да бъдат предоставени.

   Ако България е държава А, то eIDAS услугата ще се свърже с националния доставчик на идентичност посредством интеграцията с е-Авт.

6. eIDAS прокси услугата изпраща потвърждение (SAML Assertion) до eIDAS конектора в държава Б, който предава отговора на доставчика на електронни услуги. Ако България е държава Б, то eIDAS конекторът ще се свърже с доставчика на електронни услуги посредством е-Авт.
7. Доставчикът на електронни услуги предоставя достъп на потребителя.

Взаимодействието с потребителя става само на етапи 1, 3, 5 и 7. Останалата част от процеса е автоматизирана и невидима за потребителя.

Доставчикът на идентичност и доставчикът на атрибути са в държавата-членка А.

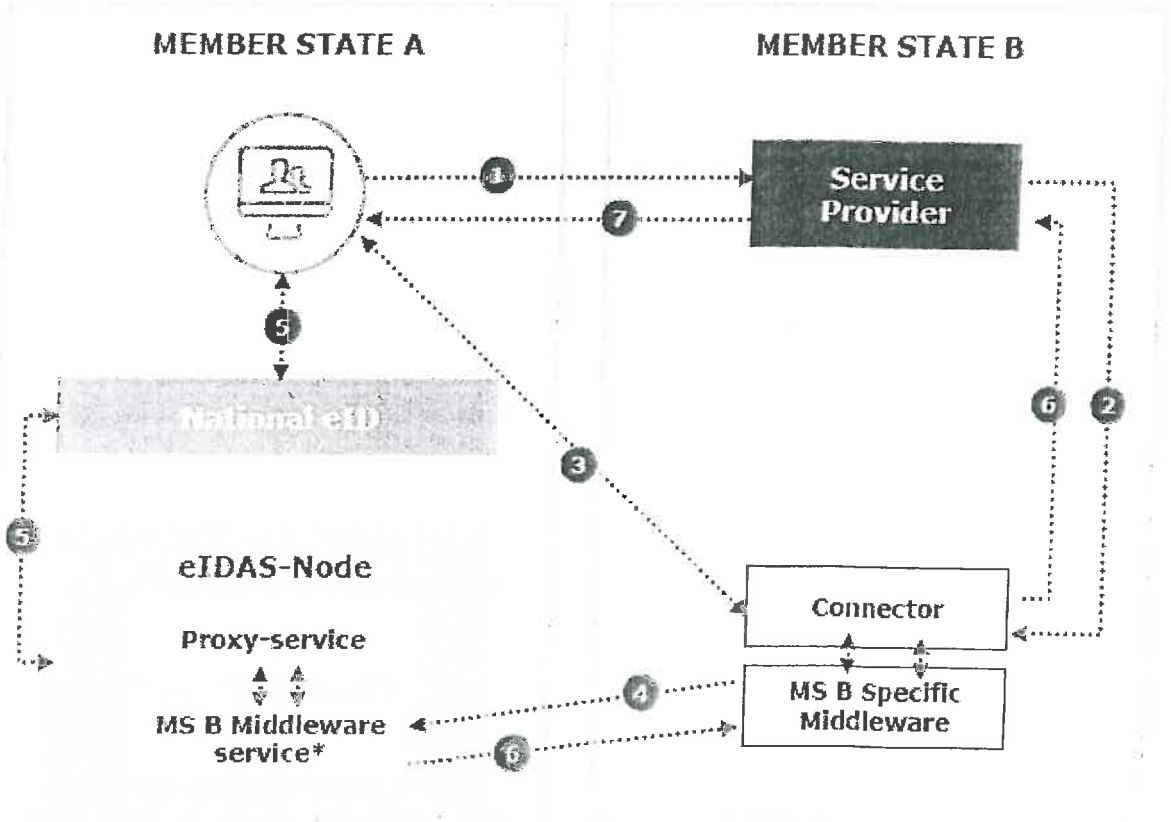
ii. От държава с eIDAS прокси услуга към държава с eIDAS Middleware услуга

Основни компоненти:

▪ Две държави-членки - държава А с eIDAS прокси услуга държава Б с eIDAS Middleware услуга;

- Потребител (гражданин);
- Доставчик на електронни услуги (публични администрации и частни доставчици на електронни услуги);
- eIDAS-възел в държавата-членка на потребителя, състоящ се от:
  - eIDAS конектор;
  - една или повече Middleware приставки за комуникация с държави с eIDAS Middleware услуга;
- Национален доставчик на електронна идентичност в държавата-членка на потребителя;
- Инфраструктурата на eIDAS Middleware услуга в държавата-членка на доставчика на електронни услуги.

В България, е реализиран допълнителен компонент – е-Авт. Чрез интеграция с е-Авт eIDAS възелът ще се свързва с национални доставчици на идентичност , както и с доставчиците на електронни услуги в България.



Описание на хипотезата:

1. Потребителят в държавата А заявява услуга пред доставчик на електронни услуги в държавата Б;
2. Доставчикът на услуги изпраща искане до Middleware на своята държава чрез eIDAS конектор;
3. При получаване на искането, eIDAS конекторът пита потребителя за неговата страна на произход (използвайки протокола TLS);
4. Когато потребителят посочи страна на произход, заявката се препраща от Middleware на държавата Б към Middleware услугата на държавата А;
5. Потребителят се автентикира, използвайки своята национална електронна идентичност. След като бъде удостоверена, тази идентичност се препраща до eIDAS-възела на държава А (eIDAS прокси услуга). Ако България е държава А, то националният доставчик на електронна идентичност ще се свърже с eIDAS възела посредством е-Авт;
6. eIDAS-възелът предава информацията за електронната идентичност на искащата Middleware услуга в държава А, която изпраща отговор на Middleware в държавата Б, който го предава на доставчика на услуги чрез eIDAS конектор;
7. Доставчикът на електронни услуги предоставя достъп на потребителя.

Взаимодействието с потребителя става само на етапи 1, 3, 5 и 7. Останалата част от процеса е автоматизирана и невидима за потребителя.

Доставчикът на идентичност и доставчикът на атрибути са в държавата А.

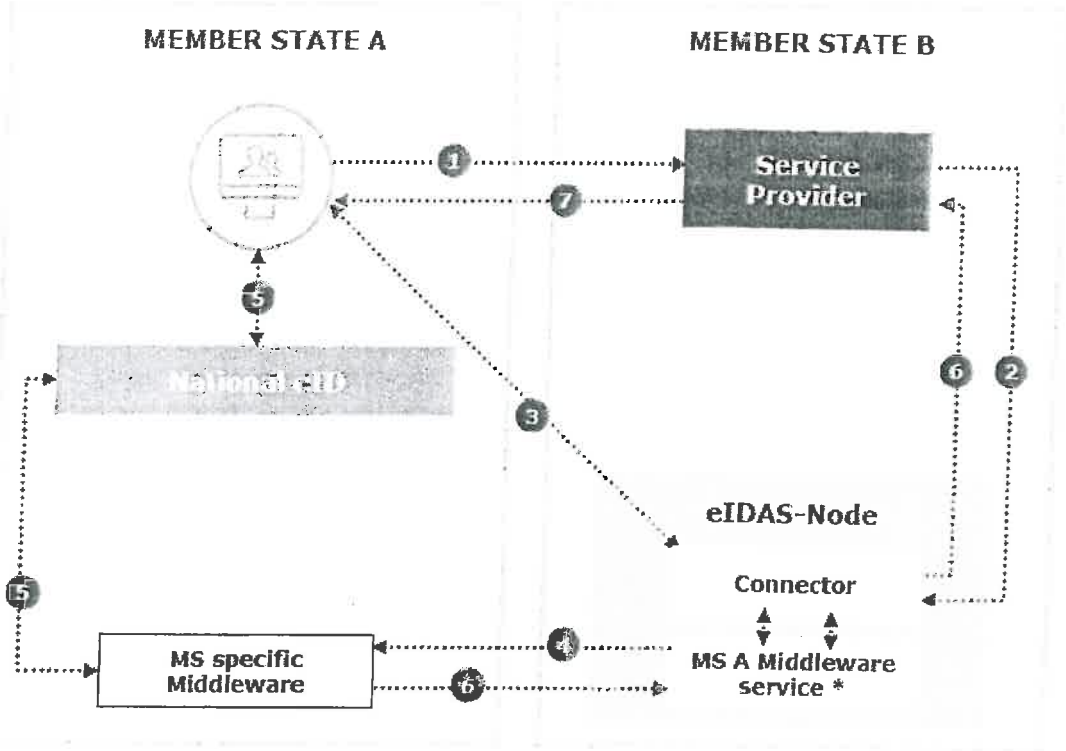
iii. От държава с eIDAS Middleware услуга към държава с eIDAS прокси услуга

Основни компоненти:

- Две държави-членки –държава А с eIDAS Middleware услуга и държава Б с eIDAS прокси услуга;
- Потребител (гражданин);
- Доставчик на електронни услуги (публични администрации и частни доставчици на електронни услуги);
- eIDAS-възел в държавата-членка на доставчика на услуги, състоящ се от:
  - eIDAS конектор;
  - една или повече Middleware приставки за комуникация с държави с eIDAS Middleware услуга;
- Инфраструктурата на Middleware в държавата-членка на потребителя;

▪ Национален доставчик на електронна идентичност в държавата-членка на потребителя.

В България, е реализиран допълнителен компонент – е-Авт. Чрез интеграция с е-Авт eIDAS възелът ще се свързва с национални доставчици на идентичност и атрибути, както и с доставчиците на електронни услуги в България.



Описание на хипотезата:

1. Потребителят от държава А заявява услуга от доставчик на електронни услуги в държава Б;
2. Доставчикът на електронни услуги изпраща заявка до eIDAS конектора в своята държава. Ако България е държава Б, то доставчикът на електронни услуги ще се свърже с eIDAS конектора посредством е-Авт;
3. При получаване на заявката, eIDAS конекторът пита потребителя за неговата страна на произход (използвайки протокола TLS). Ако България е държава Б, то тази стъпка ще се осъществи посредством интеграцията на eIDAS конектора с е-Авт;
4. Когато страната на произход бъде посочена от потребителя, искането се препраща от Middleware услугата в eIDAS възела на държава Б към специфичния Middleware на държава А (SAML искане);

5. Потребителят се автентикира, използвайки своята национална електронна идентичност и Middleware инфраструктурата в своята държава. В зависимост от изпълнението може да има две допълнителни подстъпки в стъпка 5:
   - потребителят да избере атрибутите, които трябва да бъдат предоставени (следователно да даде съгласие);
   - потребителят да приеме стойностите на атрибутите, които трябва да бъдат предоставени.
6. След като бъде извършена автентикацията, специфичният Middleware на държава А изпраща отговор на Middleware услугата в eIDAS възела на държава Б, която предава отговора на eIDAS конектора (SAML Assertion) на държавата Б. Тогава eIDAS конекторът изпраща информацията за електронната идентификационна на потребителя на доставчика на електронни услуги. Ако България е държава Б, то eIDAS конекторът ще се свърже с доставчика на електронни услуги посредством е-Авт.
7. Доставчикът на електронни услуги предоставя достъп на потребителя.

Взаимодействието с потребителя става само на етапи 1, 3, 5 и 7. Останалата част от процеса е автоматизирана и невидима за гражданите.

Доставчикът на идентичност и доставчикът на атрибути са в държава А. Обърнете внимание, че услугата Middleware може да се изпълнява в домейна на доставчика на електронни услуги. Процесът на автентикация обаче остава същият.

7.1.2. Интеграция на eIDAS възел с еАвт

eIDAS възелът трябва да поддържа интеграция в реално време с хоризонталния модул е-Авт, който предоставя възможност за унифициран подход съгласно критериите на регламент (ЕС) 910/2014 и осигурява изпълнение на законовите изисквания определени в ЗЕИ и Правилника за неговото прилагане. Интерфейсите за интеграция на е-Авт са публикувани на адрес: https://github.com/governmentbg/eAuthIntegration. На сайта за разработчици са дадени WSDL описанието с криптиране на съобщенията, като този вариант се използва при връзката система към система. На същото място е публикувано актуален WSDL на STS(Security Token service), който се използва от еАвт. Това е услугата без криптиране на съобщенията.

След сключване на договор с Изпълнителя, Възложителят му предоставя модел за интеграция с хоризонталната система е-Авт.

7.2. Нефункционални изисквания към информационната система

7.2.1. Оперативна съвместимост

Тъй като eIDAS възелът предполага използването на SAML 2.0, изпълнителят трябва да анализира евентуалната нужда от транслиране на съобщенията между SAML 2.0 и OpenID Connect 1.0 при трансгранична електронна идентификация и евентуалната нужда от разработка на прокси-услуга за транслиране на заявките. При идентифициране на такава нужда, изпълнителят трябва да реализира необходимата функционалност на eIDAS възела, която да позволява транслиране на съобщения и да осигурява оперативна съвместимост.

7.2.2. Авторски права и изходен код

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

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

Приложимите и допустими лицензи за софтуер с отворен код са:

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

- Mozilla Public License 2.0
- European Union Public License

Изходният код (Source Code), разработван по проекта, както и цялата техническа документация трябва да бъде бъдат публично достъпни онлайн като софтуер с отворен код от първия ден на разработка чрез използване на система за контрол на версиите и хранилището по чл. 7в, т.18 от ЗЕУ;

Да се изследва възможността резултатният продукт да се изгради във възможно най-голяма степен на базата на съществуващите софтуерни решения, предоставен от CEF Digital, които са софтуер с отворен код, включително eIDAS примерен софтуер. Изграждането на собствено софтуерно решение в цялост, от нулата може да се допусне само ако участникът писмено обоснове невъзможност за използване на предоставените от CEF Digital софтуерни решения. Избраният подход трябва да бъде детайлно описан в техническото предложение на участниците;

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

7.2.3. Системна и приложна архитектура

Доколкото, по оценка на Изпълнителя, това е съвместимо с eIDAS технически спецификации:

- Системата трябва да бъде реализирана като разпределена модулна информационна система. Системата трябва да бъде реализирана със стандартни технологии и да поддържа общоприети комуникационни стандарти, които ще гарантират съвместимост на Системата с бъдещи разработки. Съществуващите модули функционалности трябва да бъдат рефакторирани и/или надградени по начин, който да осигури изпълнението на настоящето изискване;
- Бизнес процесите и услугите трябва да бъдат проектирани колкото се може по-независимо с цел по-лесно надграждане, разширяване и обслужване. Системата трябва да е максимално параметризирана и да позволява настройка и промяна на параметрите през служебен (администраторски) потребителски интерфейс;
- Трябва да бъде реализирана функционалност за текущ мониторинг, анализ и контрол на изпълнението на бизнес процесите в Системата;

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

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

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

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

▪ Версията на програмните интерфейси, представени чрез уеб-услуги, трябва да поддържа версията по един или няколко от следните начини:

- Като част от URL-а
- Като GET параметър
- Като HTTP header (Accept или друг)

▪ За всеки отделен приложен програмен интерфейс трябва да бъде разработен софтуерен комплект за интеграция (SDK) на поне две от популярните развойни платформи (.NET, Java, PHP);

▪ Системата трябва да осигурява възможности за разширяване, резервиране и балансиране на натоварването между множество инстанции на сървъри с еднаква роля;

▪ При разработването на Системата трябва да се предвидят възможни промени, продиктувани от непрекъснато променящата се нормативна, бизнес и технологична среда. Основно изискване се явява необходимостта информационната система да бъде разработена като гъвкава и лесно адаптивна, като отчита законодателни, административни, структурни или организационни промени, водещи до промени в работните процеси;

▪ Изпълнителят трябва да осигури механизми за реализиране на бъдещи промени в Системата без промяна на съществуващия програмен код. Когато

това не е възможно, времето за промяна, компилиране и пускане в експлоатация трябва да е сведено до минимум. Бъдещото развитие на Системата ще се налага във връзка с промени в правната рамка, промени в модела на работа на потребителите, промени във външни системи, интегрирани със Системата, отстраняване на констатирани проблеми, промени в модела на обслужване и др. Такива промени ще се извършват през целия период на експлоатация на Системата, включително и по време на гаранционния период;

▪ Архитектурата на Системата и всички софтуерни компоненти (системни и приложни) трябва да бъдат така подбрани и/или разработени, че да осигуряват работоспособност 24/7 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);

▪ Изпълнителят трябва да проектира, подготви, инсталира и конфигурира като минимум следните среди за Системата: тестова, стейджинг, продуктивна;

▪ Системата трябва да бъде разгърната върху съответните среди (тестова за вътрешни нужди, тестова за външни нужди, стейджинг и продуктивна);

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

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

- В Техническото си предложение участникът трябва да опише добрите практики, които ще прилага по отношение на всеки аспект от системната и приложната архитектура на Системата;
- За търсене трябва да се използват системи за пълнотекстово търсене (например Solr, Elastic Search). Не се допуска използването на индекси за пълнотекстово търсене в СУБД;
- Трябва да бъде създаден административен интерфейс, чрез който може да бъде извършвана конфигурацията на софтуера;
- Всеки обект в системата трябва да има уникален идентификатор;
- Записите в регистрите не трябва да подлежат на изтриване или на промяна, а всяко изтриване или промяна трябва да представлява нов запис.

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

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

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

Подход за работа с външните софтуерни ресурси

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

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

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

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

7.2.5. Изграждане и поддръжка на множество среди

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

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

Управлението на средите трябва да става чрез автоматизирана система за провизиране и разгръщане на системните компоненти. При необходимост от страна на Възложителя Изпълнителят трябва да съдейства за изграждането на нови системни среди.

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

7.2.6. Процес на разработка, тестване и разгръщане

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

процесите по развитие и тестване на разработките през целия им жизнен цикъл.

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

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

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

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

- Документиране на Системата в изходния код, минимум на ниво процедура/функция/клас;
- Покритие на минимум 50% от изходния код с функционални тестове;
- Използване на continuous integration практики;
- Използване на dependency management.

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

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

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

7.2.7. Бързодействие и мащабируемост

7.2.7.1 Контрол на натоварването и защита от DoS/DDoS атаки

Доколкото, по оценка на Изпълнителя, това е съвместимо с eIDAS технически спецификации:

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

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

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

7.2.7.2 Кохерентно кеширане на данни и заявки

Доколкото, по оценка на Изпълнителя, това е съвместимо с eIDAS технически спецификации:

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

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

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

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

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

Като минимум разпределен кохерентен кеш трябва да се предвиди при:

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

▪ Извличане на информация от предефинирани периодични справки;

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

▪ Информация за извършените плащания;

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

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

7.2.7.3 Бързодействие

Доколкото, по оценка на Изпълнителя, това е съвместимо с eIDAS технически спецификации:

▪ Архитектурата на системата трябва да осигурява мащабируемост по отношение на броя на конкурентните заявки отправени към и от нея към други системи, предвид факта че същата е ключова по отношение на цялостния процес на идентификация на лицата при достъп до електронни услуги.

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

▪ Трябва да бъдат създадени тестове за натоварване.

7.2.7.4 Използване на HTTP/2

Доколкото, по оценка на Изпълнителя, това е съвместимо с eIDAS технически спецификации:

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

- Включена header compression;
- Използване на brotli алгоритъм за компресия;
- Включен HTTP pipelining;
- HTTP/2 Server push, приоритизиращ специфични компоненти, изграждащи страниците (CSS, JavaScript файлове и др.);
- Публичните потребителски интерфейси трябва да поддържат адаптивен избор на TLS cipher suites според вида на процесорната архитектура на клиентското устройство - AES-GCM за x86 работни станции и преносими компютри (с налични AES-NI CPU разширения), и ChaCha20/Poly1305 за мобилни устройства (основно базирани на ARM процесори);
- Ако клиентският браузър/клиент не поддържа HTTP/2, трябва да бъде предвиден fall-back механизъм към HTTP/1.1. Тази възможност трябва да може лесно да се реконфигурира в бъдеще и да отпадне, когато браузърите/клиентите, неподдържащи HTTP/2, станат незначителен процент.

7.2.7.5 Качество и сигурност на програмните продукти и приложенията

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

7.2.8. Информационна сигурност и интегритет на данните

Доколкото, по оценка на Изпълнителя, това е съвместимо с eIDAS технически спецификации:

▪ Не се допуска съхранението на пароли на администратори, на вътрешни и външни потребители и на акаунти за достъп на системи (ако такива се използват) в явен вид. Всички пароли трябва да бъдат защитени с подходящи сигурни алгоритми (напр. BCrypt, PBKDF2, scrypt (RFC 7914) за съхранение на пароли и където е възможно, да се използва и прозрачно криптиране на данните в СУБД със сертификати (transparent data-at-rest encryption);

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

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

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

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

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

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

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

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

- Трябва да бъде изграден модул за проследимост на действия и събития в Системата. За всяко действие (добавяне, изтриване, модификация, четене) трябва да съдържа следните атрибути:
  - Уникален номер;
  - Точно време на възникване на събитието;
  - Вид (номенклатура от идентификатори за вид събитие);
  - Данни за информационна система, където е възникнало събитието;
  - Име или идентификатор на компонент в информационната система, регистрирал събитието;
  - Приоритет;
  - Описание на събитието;
  - Данни за събитието.

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

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

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

8. ДОКУМЕНТАЦИЯ

8.1. Изисквания към документацията

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

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

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

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

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

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

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

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

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

- Обща информация, инструкции и процедури за администриране и поддръжка на приложните сървъри, сървърите за бази данни и др.
- Обща информация, инструкции и процедури за администриране, архивиране и възстановяване, и поддръжка на сървъра за управление на бази данни.

8.2. Прозрачност и отчетност

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

Документацията, предоставена от изпълнителя на възложителя, трябва да бъде:

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

Минимално изискуемата документация по проекта включва долуизброените документи.

8.3. Системен проект

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

При документирането на изискванията, с цел постигане на яснота и стандартизация на документите, е необходимо да се използва утвърдена

нотация за описание на бизнес модели. Изготвената детайлна техническа спецификация (системен проект) се представя за одобрение на Възложителя. В случай на забележки, корекции или допълнения от страна на Възложителя Изпълнителят е длъжен да ги отрази в детайлната техническа спецификация (системен проект).

8.4. 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;
- Доколкото е приложимо, документи за крайния ползвател – Изпълнителят трябва да предостави главното Ръководство на ползвателите на софтуера. Документът е предназначен за крайните ползватели. Той трябва да описва цялостната функционалност на приложния софтуер и съответното му използване от крайни ползватели;
- Детайлно описание на базата данни;
- Описание на софтуерните модули;
- Описание на изходния програмен код.

8.5. Протоколи

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

8.6. Комуникация и доклади

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

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

8.6.1. Встъпителен доклад

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

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

Встъпителният доклад следва да бъде одобрен от възложителя.

8.6.2. Междинни доклади

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

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

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

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

Всеки междинен доклад следва да бъде одобрен от възложителя.

8.6.3. Окончателен доклад

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

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

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

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

9. РЕЗУЛТАТИ

Очакваните резултати от изпълнението на настоящата обществена поръчка са следните:

- Изграден, тестван и въведен в експлоатация на хардуерни ресурси на ДАЕУ eIDAS възел, в съответствие с изискванията на Регламент (ЕС) 910/2014 и с eIDAS технически спецификации, който е интегриран както с eIDAS мрежата, така и с е-Авт и разполага с функционалностите, необходими за взаимно признаване на средства за електронна идентификация, издадени в държави членки на ЕС съгласно чл. 6 от Регламент (ЕС) 910/2014;
- Пълна техническа и експлоатационна документация относно eIDAS възела и интеграцията му с е-Авт, включително подробни технически спецификации и документация за софтуерни разработчици, ключови потребители и администратори.
- Проведено обучение на минимум 3 служителя от ДАЕУ за администриране на eIDAS възела.