Политика и практика при предоставяне на квалифицирана отдалечена и физическа идентификация за издаване на квалифицирани удостоверения и проверка на специфични атрибути

БОРИКА АД

Версия 2

В сила от:

1 МАРТ 2026 г.

Хронология на измененията на документа				
Версия	**Автор (и)**	**Дата**	**Състояние**	**Коментар**
1.0	Димитър Николов	01.01.2021	Утвърден	Първо издание
1.1	Маргарита Бонева	01.07.2021	Утвърден	Редакция
1.2	Маргарита Бонева	10.03.2023	Утвърден	Корекции
2	Маргарита Бонева	01.03.2026	Утвърден	Корекции

СЪДЪРЖАНИЕ

Съкращения на български език 5
Съкращения на АНГЛИЙСКИ език 6
СПЕЦИФИЧНИ ТЕРМИНИ И ОПРЕДЕЛЕНИЯ КЪМ ДОКУМЕНТА 7
СЪОТВЕТСТВИЕ И УПОТРЕБА 8
1 ОБЩИ ПОЛОЖЕНИЯ 11
1.1 Удостоверяващ орган на „БОРИКА“ АД 11
1.2 Други Удостоверяващи органи и Доверяващи се страни 12
1.3 Идентификатори в документа 12
1.4 Управление на Политиката 13
1.5 Други приложими документи 13
1.6. USE CASE Приложими сценарии 14
2 УЧАСТНИЦИ В „ОНБОРДИНГ“ ПРОЦЕСА 15
3 ЗАДЪЛЖЕНИЕ ЗА ПУБЛИКУВАНЕ И ВОДЕНЕ НА РЕГИСТЪР 16
4 ИДЕНТИФИКАЦИЯ И АВТЕНТИФИКАЦИЯ 16
4.1 Именуване 17
4.1.1 Използване на имена 17
4.1.2 Използване на псевдоним 17
4.1.3 Значимост на имената при вписване 17
4.1.4 Правила за интерпретация на имената 17
4.1.5 Уникалност на имената 17
4.2 Начално валидиране на идентичност 18
4.2.1 Мобилно приложение B-Trust - отдалечена идентификация в съответствие с чл. 24, параграф 1а, буква в 18
4.2.2 Интернет страница за идентификация - отдалечена идентификация в съответствие с чл. 24, параграф 1а, буква в 20
4.2.3 Видеоразговор - отдалечена идентификация в съответствие с чл. 24, параграф 1а, буква в 21
4.2.4 Идентификация въз основа на физическо присъствие и проверка на атрибути в съответствие с член 24, параграф 1а, букви г) 22
4.2.5 Специфични атрибути 22
4.2.6 Непотвърдена информация 23
4.3 Валидиране на идентичност при подновяване 23
4.4 Валидиране на идентичност при спиране/възобновяване 24
4.5 Валидиране на идентичност при прекратяване 24
5 Искане за издаване на удостоверение 24
5.1.1 Доставка на приложение и приемане на общи условия 24
5.1.2 Валидиране на е-мейл и смарт устройство (мобилен номер) и защита на приложение 24
5.2 „Онбординг“ процес и регистрация (валидиране на самоличност) 25
5.2.1 Заснемане на официалния документ за самоличност и селфи (selfie) през Интернет страница за идентификация 25
5.2.2 Заснемане на официалния документ за самоличност и селфи (selfie) през мобилното приложение B-Trust 25
5.2.3 Верифициране на официалния документ за самоличност и селфи 26
5.2.4 Валидиране на официалния документ за самоличност 26
5.3 Издаване на удостоверение 27
5.3.1 Функции по идентификация и автентификация 27
5.3.2 Идентификация и автентификация с асистент 27
5.3.3 Потвърждаване или отхвърляне на искане за издаване 27
5.3.4 Техническа заявка (PKCS#10) за издаване 28
5.3.5 Действие на Удостоверяващия орган 28
5.3.6 Известяване на Потребителя от Доставчика 28
5.4 Приемане и публикуване на удостоверението 29
5.5 Употреба 29
5.6 Подновяване на удостоверение 29
5.7 Подмяна на двойката криптографски ключове (Re-key) 29
5.8 Промяна в удостоверение 29
5.9 Прекратяване и спиране/възобновяване на удостоверение 29
5.10 Статус на удостоверение 29
5.11 Прекратяване на Договор за удостоверителни услуги 30
6 СРЕДСТВА, УПРАВЛЕНИЕ И ОПЕРАТИВЕН КОНТРОЛ 30
6.1 Физически контрол 30

6.2 Процедурен контрол 30
6.3 Квалификация и обучение на персонала 30
6.4 Изготвяне и поддържане на журнали 31
6.5 Архив и поддържане на архива 31
6.6 Промяна на ключ 31
6.7 Компрометиране на ключове и възстановяване след авария 31
6.8 Компрометиране на частен ключ 31
6.9 Прекратяване дейността на Доставчика 31
7 ФУНКЦИОНАЛЕН МОДЕЛ И СПЕЦИФИКАЦИЯ 31
7.1 Функционален модел 31
7.2 Спецификация 32
7.3 Управление на достъпа 33
7.4 Операционна сигурност 33
7.5 Мрежова сигурност 33
7.6 Информационна сигурност 33
7.7 Непрекъсваемост 33
8 ОЦЕНКА НА РИСКА 33
9 ПРОВЕРКА И КОНТРОЛ НА ДЕЙНОСТТА НА ДОСТАВЧИКА 35
10 ДРУГИ БИЗНЕС УСЛОВИЯ И ПРАВНИ АСПЕКТИ 35

Съкращения на български език

АД	Акционерно дружество
ВИ	видео идентификация
ВИС	видео идентификационен сървър
ДВ	Държавен вестник
ДКУУ	Доставчик на квалифицирани удостоверителни услуги
ЕГН	Единен граждански номер
ЕП	Електронен подпис
ЗЕДЕУУ	Закон за електронния документ и електронните удостоверителни услуги
КЕП	Квалифициран Електронен Подпис
КУ	Квалифицирано удостоверение
КУУ	Квалифицирани удостоверителни услуги
КУКЕП	Квалифицирано удостоверение за Квалифициран Електронен Подпис
КРС	Комисия за регулиране на съобщенията
МРС	Местна регистрираща служба
НОПДДУУ	Наредба за отговорността и за прекратяването на дейността на доставчиците на удостоверителни услуги
ОКЕП	Облачен КЕП
Е-ОКЕП	Еднократен ОКЕП
ПИН	Персонален идентификационен номер
Практика	Практика при предоставяне на КУ и квалифицирани удостоверителни услуги
Политика	Политика за предоставяне на квалифицирани удостоверителни услуги
Регламент	Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 година относно Електронната идентификация и Удостоверителните услуги, изменен с Регламент (ЕС) № 2024/1183
РО	Регистриращ орган
РО-ВИ	Регистриращ Орган чрез отдалечена видео идентификация
УО	Удостоверяващ орган

Съкращения на АНГЛИЙСКИ език

CA	Certification Authority – Удостоверяващ орган (УО)
CC	Common Criteria for Information Technology Security Evaluation - Международен стандарт (ISO/IEC 15408) за информационна сигурност
CEN	European Committee for Standardization - Европейски стандартизационен комитет
CP	Certificate Policy – Политика за предоставяне на удостоверителни услуги
CPS	Certification Practice Statement – Практика при предоставяне на удостоверителни услуги
CRL	Certificate Revocation List – Списък с прекратени и спрени удостоверения
CQES	Cloud Qualified Electronic Signature – Квалифициран Облачен КЕП/ОКЕП
DN	Distinguished Name – Уникално име
eIDAS	ЕС Регламент 910/2014
ETSI	European Telecommunications Standards Institute - Европейски институт за телекомуникационни стандарти
EU	European Union - Европейски съюз
HSM	Hardware Security Module – специализирана хардуерна криптосистема за съхранение и работа с криптографски ключове
ISO	International Standardization Organization - Международна организация за стандартизация
IP	Internet Protocol – Интернет протокол
OID	Object Identifier – Идентификатор на обект
OCSP	On-line Certificate Status Protocol – Протокол за онлайн проверка на статуса на удостоверения
PKCS	Public Key Cryptography Standards – Криптографски стандарт за публичен ключ
PKI	Public Key Infrastructure – Инфраструктура на публичния ключ
QC	Qualified Certificate – Квалифицирано удостоверение
QES	Qualified Electronic Signature – Квалифициран електронен подпис
QESeal	Qualified Electronic Seal – Квалифициран електронен печат
RA	Registration Authority – Регистриращ орган
QCP-n-qscd	certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a QSCD

СПЕЦИФИЧНИ ТЕРМИНИ И ОПРЕДЕЛЕНИЯ КЪМ ДОКУМЕНТА

Видео идентификация – процес на верифициране с последващо валидиране и регистриране на лични данни от национално утвърден документ за самоличност чрез видео-технология.

„Онбординг“ процес – идентификация на физическо лице пред доверяваща се страна (в случая, ДУУ „БОРИКА“ АД).

Видео идентификационен сървър (ВИС)/център за видео идентификация - информационен ресурс, управляващ и администриращ „онбординг“ процеса.

Агентски Портал (АП) - информационен ресурс, обслужващ процеса по регистрация и управление след валидиране на самоличността на физическо лице чрез „онбординг“ процеса и предоставяне на лични данни на УО за удостоверяване в квалифицирано удостоверение.

Регистриращ Орган на B-Trust за присъствена идентификация – орган, опериращ интегриран информационен ресурс, който обслужва Потребители при регистрация за издаване и управление на удостоверенията за КЕП/ОКЕП чрез процес на присъствена (лице-в-лице) идентификация с Оператор/Агент.

Регистриращ Орган на B-Trust за отдалечена видео идентификация (РО-ВИ) – орган, опериращ информационен ресурс (ВИС и АП), обслужващ Потребители при регистрация за издаване и управление на Облачен КЕП чрез неприсъствена отдалечена онлайн видео идентификация.

Потребител – физическо лице, което участва в „онбординг“ процеса и ще е Титуляр на КУ т.е. потребител на B-Trust.

Оператор (на РО-ВИ) – обучен служител на „БОРИКА“ АД, участващ в „онбординг“ процеса чрез АП.

Клиент – всяка трета доверяваща се страна, която може да ползва „онбординг“ процеса за отдалечена видео идентификация като „облачна услуга“ на „БОРИКА“ АД (например, друг ДУУ, финансова институция – банка/застраховател, др.).

Данни за идентификация на физическо лице – набор от данни, които позволяват да се установи еднозначно самоличността на физическо лице.

Документ за самоличност – валиден документ, съдържащ данни за идентификация на физическо лице (лична карта, международен паспорт, лична карта на чужденец и други, съобразно националното законодателство на съответната държава)

„Облачни услуги“ – онлайн услуги за анализ на видео изображения за целите на „онбординг“ процеса.

RegiX/Registry Information eXchange system – национален информационен хъб за достъп до национални бази данни (регистри) с първични данни.

СЪОТВЕТСТВИЕ И УПОТРЕБА

Този Документ:

- е разработен от „БОРИКА“ АД, юридическото лице, регистрирано в Търговския регистър към Агенцията по вписванията с ЕИК 201230426;
- влиза в сила на **1.03.2026 г.** ;
- е с наименование „Политика и практика при предоставяне на отдалечена и физическа идентификация за издаване на квалифицирани удостоверения и проверка на специфични атрибути“ ОТ „БОРИКА“ АД“.
- се асоциира с публикуваните актуални версии на документите „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPS-eIDAS)“ и „Политика при предоставяне на квалифицирани удостоверения за квалифициран електронен подпис, квалифициран облачен електронен подпис, квалифициран електронен печат и квалифициран облачен електронен печат от „БОРИКА“ АД (B-Trust CP-eIDAS QES/CQES/QESeal/CQESeal)”, които съдържат общите условия и изисквания към процедурите при идентификация, издаване и управление на КУ, изискванията за ниво на сигурност при генерация и съхраняване на частния ключ за тези удостоверения, както и тяхната приложимост;
- е разработен в съответствие с формалните изисквания за съдържание, структура и обхват, посочени в международната препоръка RFC 3647 и международните спецификации ETSI EN 319-401 и EN319 411-1/2, включвайки секциите, които са специфични и приложими за „онбординг“ процеса, КУ за ОКЕП и КУ за ОКЕПечат;
- адресира само Регистриращ орган за отдалечена видео идентификация (РО-ВИ), но включва текстове, обяснения и референции, които доказват, че РО-ВИ изпълнява изискванията за РО на КДУУ съгласно горепосочените международни препоръки и спецификации;
- има характер на общи условия по смисъла на чл. 16 от Закона за задълженията и договорите (ЗЗД). Тези условия са част от Договор за удостоверителни услуги, който се сключва между Доставчика и Потребителите на основание чл.23 от ЗЕДЕУУ. Договорът може да съдържа специални условия, които се ползват с предимство пред общите условия в настоящия документ;
- е публичен документ с цел установяване на съответствие на дейността на Доставчика „БОРИКА“ АД, и в частност на РО-ВИ със ЗЕДЕУУ и нормативната уредба;
- е общодостъпен по всяко време на интернет-страницата на Доставчика на адрес: https://www.b-trust.bg/documents;
- може да бъде променян от ДКУУ и всяка нова редакция се публикува на интернет-страницата на Доставчика;

Настоящият документ е изготвен в съответствие с:

- Закон за електронния документ и електронните удостоверителни услуги (ЗЕДЕУУ);
- Наредба за отговорността и за прекратяването на дейността на доставчиците на удостоверителни услуги (НОПДДУУ);
- Регламент (ЕС) № 910/2014 на европейския парламент и на съвета относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар;

- Регламент (ЕС) 2024/1183 на Европейския парламент и на Съвета от 11 април 2024 година за изменение на Регламент (ЕС) № 910/2014 по отношение на създаването на европейска рамка за цифрова самоличност;
- Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните).
- Директива (ЕС) 2018/843 на Европейския парламент и на Съвета от 30 май 2018 година за предотвратяване използването на финансовата система за целите на изпирането на пари и финансирането на тероризма
- Чл. 42 от Правилника за прилагане на Закона за мерките срещу изпиране на пари;
- Чл. 55, ал. 2 от Закона за мерките срещу изпирането на пари.

Съдържанието и структурата на документа е в съответствие с Регламент Регламент (ЕС) № 910/2014 г. изменен с Регламент (ЕС) 2024/1183 и се позовава на информация, съдържаща се в следните утвърдени международни препоръки, спецификации и стандарти:

- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
- ETSI EN 319 401: General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1/2: Policy and security requirements for Trust Service Providers issuing certificates;
- ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects;
- RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;

Цитираните по-горе ETSI стандарти и спецификации изискват самоличността на заявителя да бъде установена чрез процес, който осигурява достатъчна степен на надеждност в зависимост от приложимия контекст на идентификацията. Това може да се осъществи чрез физическо присъствие или чрез отдалечена идентификация, когато са приложени средства и процедури, осигуряващи изискуемото ниво на доказване на самоличността.

Настоящият документ представлява и практика на компонента за проверка на самоличността (identity proofing service component) в рамките на удостоверителните услуги на „БОРИКА“ АД и е разработен в съответствие с ETSI TS 119 461 „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects“. Документът се прилага във връзка с чл. 24, пар. 1а и когато е приложимо – пар. 1б от Регламент (ЕС) № 910/2014, изменен с Регламент (ЕС) 2024/1183, както и с Регламент за изпълнение (ЕС) 2025/1566 на Комисията относно референтните стандарти за проверка на самоличността и атрибутите на лице, на което ще бъде издадено квалифицирано удостоверение или квалифицирано електронно удостоверение за атрибути.

За целите на ETSI TS 119 461 настоящият документ служи като practice statement за процесите по физическа и отдалечена идентификация, прилагани от „БОРИКА“ АД, и определя приложимите сценарии (use cases), нивото на доказване на самоличността (LoIP), използваните доказателства за самоличност, методите за валидиране и обвързване на заявителя с представените доказателства, както и резултата от процеса по идентификация.

Регистриращият орган РО-ВИ, който се адресира в този документ използва „онбординг“ процес за отдалечена онлайн видео идентификация, осигуряващ ниво на сигурност, равностойно на физическо присъствие.

Всякаква информация, свързана с този документ, може да се получи от Доставчика на адрес:

бул. „Цар Борис III" № 41
София 1612
„БОРИКА“ АД
телефон: 0700 199 10
имейл адрес: info@borica.bg;
Официална страница на доставчика: www.b-trust.bg

1 ОБЩИ ПОЛОЖЕНИЯ

Този документ описва конкретните условия и изисквания, които ДКУУ „БОРИКА“ АД изпълнява чрез процес „онбординг“ - физическа и отдалечена видео идентификация на регистриращия орган РО-ВИ, за да провери самоличността и идентичността на физически лица, които участват в процеса при издаване на квалифицирани удостоверения. Физическото лице участва в „онбординг“ процеса в офис на БОРИКА АД, чрез интернет страница през браузър или чрез смарт устройство (смартфон или таблет) и мобилно приложение в него. Процесът на онлайн видео идентификация е сертифициран за еквивалентно ниво на осигуреност („equivalent assurance”) както физическо присъствие („лице-в-лице“) на лицата, за които Доставчикът събира, верифицира и валидира лични данни, за да ги удостовери в издавани за тях КУ. Идентификацията на физическите лица чрез „онбординг“ пред Доставчика е потвърдено от Орган за оценяване на съответствието на основание **чл. 24, ал. 1А (в, г) от Регламент (ЕС) № 910/2014 г., изменен с Регламент (ЕС) № 2024/1183 г.**

Документът съдържа описание на участниците в „онбординг“ процеса в B-Trust при идентифициране на физически лица (Титуляри/Създатели на КУ), както и описва общите оперативни процедури при този процес, а именно:

- проверка на действителното съществуване на физическото лице в реалния живот;
- проверка дали документът за самоличност принадлежи на това конкретно лице;
- доказателство, че настоящото лице е същото, както е посочено преди;
- проверка на законната валидност на документа за самоличност;

Издаването, публикуване, доставяне и приемане на издадените КУ чрез прилагане на „онбординг“ процес, както и мерките и следваните технически процедури от страна на Доставчика и физическото лице, които гарантират сигурността и надеждността на предоставяните КУ са също част от документа в съответствие със ЗЕДЕУУ и нормативната уредба.

ДКУУ „БОРИКА“ АД извършва отдалечена видео идентификация на Потребител на B-Trust чрез „онбординг“ процеса само:

- ако този Потребител и субекта (Subject) в КУ (т.е., Титуляря) е физическо лице;
- ако Потребителят е заявил това КУ да подписва е-документи от свое име, а не от името на трето лице.
- ако този Потребител е Създател за издаване на квалифицирано удостоверение на юридическо лице.

В случай на необходимост, идентифицирането на юридическо лице и установяване на представителната власт на физическо лице спрямо юридическо лице, при наличие на официален публичен търговски или дружествен регистър в държава членка, в която е регистрирано юридическото лице, се осъществява чрез извършване на справка в търговския регистър или в съответния публичен регистър по партидата на юридическото лице и документиране на предприетите действия по идентифицирането.

Приема се, че Потребител, който ползва този документ, има познания и разбиране относно инфраструктурата на публични ключове (PKI), удостоверенията и концепцията за електронен подпис. В противен случай се препоръчва той да се запознае с тези концепции както и с документа „Практиката при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги на „БОРИКА“ АД (B-Trust CPS-eIDAS)“, преди да ползва настоящия документ.

1.1 Удостоверяващ орган на „БОРИКА“ АД

ДКУУ БОРИКА” АД е изградила и оперира инфраструктурата за публични ключове (PKI), която функционира в съответствие с правната рамка на Регламент 910/2014 и ЗЕДЕУУ и с международните

спецификации и стандарти ETSI EN 319 411-1/5 и ETSI EN 319 412. Доставчикът използва идентификатори на обектите (OID) в B-Trust PKI-инфраструктурата, формирани на база код 15862, присвоен на „БОРИКА“ АД от IANA в клона iso.org.dod.internet.private.enterprise (1.3.6.1.4.1 - IANA Registered Private Enterprise) и в съответствие със стандартите ITU-T Rec. X.660 and the ISO/IEC 9834-1:2005 (Procedures for the Operation of OSI Registration Authorities: General Procedures and ASN.1 Object Identifier tree top arcs).

В документа B-Trust CPS-eIDAS са посочени обектите на инфраструктурата с техните присвоени идентификатори (OID). Удостоверяващият орган на B-Trust инфраструктурата е с идентификатор 1.3.6.1.4.1.15862.1.6.1 (B-Trust Operational Qualified CA). Чрез него „БОРИКА“ АД издава всички квалифицирани удостоверения, посочени в документа B-Trust QCP-eIDAS, включително и КУ за ОКЕП.

Тази Политика и Практика на Доставчика се изпълнява/реализира чрез обекта с идентификатор 1.3.6.1.4.1.15862.1.6.10 (B-Trust Remote Video Identification Service) и 1.3.6.1.4.1.15862.1.6.12 (B-Trust Identification with physical presence)

Повече информация за Регистриращия орган в B-Trust инфраструктурата на „БОРИКА“ АД може да се получи от документа B-Trust CPS-eIDAS.

„БОРИКА“ АД е уведомило КРС за започване на дейност като ДКУУ по реда на ЗЕДЕУУ и действащата нормативна уредба. Доставчикът уведомява Потребителите за своята акредитация при предоставяне квалифицирани удостоверителни услуги и за издадени удостоверения относно тях.

Акредитацията на „БОРИКА“ АД като ДКУУ е в съответствие с Регламента и ЗЕДЕУУ цели най-високо ниво на сигурност на предоставяните КУУ и по-добро хармонизиране на тази дейност със съответната такава в страните-членки на Европейския съюз.

В отношенията с Потребителите и трети лица е валидна само версия на този документ, която е актуална към момента на ползване на КУ.

1.2 Други Удостоверяващи органи и Доверяващи се страни

Съгласно тази Политика и Практика, в рамките на юридическо лице (трета страна), различно от ДКУУ „БОРИКА“ АД, може да бъде обособено звено като Регистриращ орган РО-ВИ, на което са делегирани права да осъществява дейности по „онбординг“ процеса или на част от тях от името на този Доставчик или за вътрешни цели на юридическото лице.

Всяка трета (доверяваща се страна, например друг ДУУ, финансова институция – банка/застраховател, др.) може да ползва „онбординг“ процеса (отдалечена видео идентификация) като „облачна“ услуга на „БОРИКА“ АД.

Отношенията на „БОРИКА“ АД и външен Доставчик относно РО-ВИ с „онбординг“ процес се уреждат с договор. Този доставчик гарантира, че дейността на РО-ВИ е съобразена с настоящата Политика и Практика. За целите на този документ, в рамките на договора се поддържа двустранен контакт с цел:

- доклади за всички инциденти със сигурността пред Доставчика/доверяваща се страна;
- промени в този документ след одобрение от Доставчика/доверяващата се страна;
- контрол на оперативните процедури по отношение на дейностите на РО-ВИ в съответствие с настоящата Политика.

1.3 Идентификатори в документа

Политиката и Практиката на ДКУУ „БОРИКА“ АД относно „онбординг“ процеса допълват общите политика и практика на предоставяните квалифицирани удостоверителни услуги от Доставчика. Конкретно за този документ, Политиката описва какво предлага Доставчикът, за да покаже приложимостта на „онбординг“ процеса и определя условията и правилата, към които той се придържа,

когато отдалечено идентифицира и регистрира Потребители. Практиката описва оперативните процедури, които Доставчикът следва, за да предостави този процес.

Практиката на Доставчика при предоставяне на отдалечена/онлайн видео идентификация се осъществява от обекта B-Trust Remote Video Identification Service (vRA) обозначен с идентификатор 1.3.6.1.4.1.15862.1.6.10:

„Онбординг“ процес за отдалечена видео идентификация (B-Trust Remote Video Identification/B-Trust vRA)	Идентификатор на обект
Практика на Доставчика на „онбординг“ процес	**1.3.6.1.4.1.15862.1.6.10**

В съответствие с настоящия документ, Практиката на Доставчика изпълнява Политика относно „онбординг“ процеса с идентификатор както следва:

Онбординг“ процес за **отдалечена видео идентификация** (B-Trust Remote Video Identification/B-Trust vRA)	Идентификатор на обект
Политика на Доставчика на „онбординг“ процес	**1.3.6.1.4.1.15862.1.6.10.1**

Практиката на Доставчика при предоставяне на физическа идентификация се осъществява от обекта B-Trust Identification with physical presence component: обозначен с идентификатор 1.3.6.1.4.1.15862.1.6.12:

„Онбординг“ процес за физическа идентификация (B-Trust with physical presence component)	Идентификатор на обект
Практика на Доставчика на „онбординг“ процес	**1.3.6.1.4.1.15862.1.6.12**

В съответствие с настоящия документ, Практиката на Доставчика изпълнява Политика относно „онбординг“ процеса с идентификатор както следва:

Онбординг процес за **физическа идентификация**	Идентификатор на обект
Политика на Доставчика на „онбординг“ процес	**1.3.6.1.4.1.15862.1.6.12.1**

1.4 Управление на Политиката

Допускат се промени, редакции и допълнения, които не засягат правата и задължения, произтичащи от този документ и стандартния договор за удостоверителни услуги между Доставчика и Потребителите/Доверяващи се страни. Те се отразяват в новата версия или редакция на документа.

Настоящите Политика и Практика трябва да бъдат преразглеждани най-малко веднъж годишно с цел да се отразяват потенциали изисквания и предпоставки относно промени в нивата на сигурност за „онбординг“ процеса. Всяка представена и одобрена нова версия или редакция на този документ незабавно се публикува на сайта на Доставчика.

1.5 Други приложими документи

Този документ само допълва основни общи документи на B-Trust („ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“ и „ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС, ОБЛАЧЕН КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС И КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПЕЧАТ“) и следва тяхната структура. В съдържателен аспект посочва референции към съответните части на тези документи и включва текст (коментари, кратки описания и референции), за да се докаже, че и как са изпълнени

изискванията за РО-ВИ в B-Trust инфраструктурата на КДУУ „БОРИКА“ АД съгласно стандартите ETSI EN 319 411-1/2, и ETSI EN 319 401.

Съгласно тази Политика и Практика, РО-ВИ изпълнява същите функции на РО в B-Trust инфраструктурата, но чрез идентификация на физическо лице посредством „онбординг“ процес. Всички липсващи части на „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“ и на „ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС, ОБЛАЧЕН КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС И КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПЕЧАТ“ в настоящия документ се считат за неприложими в контекста на РО-ВИ.

При всички случаи, настоящия документ следва да се ползва съвместно с основните общи документи на B-Trust:

- ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ;
- ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС, ОБЛАЧЕН КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС И КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПЕЧАТ.

Екраните на процеса по идентификация чрез интернет страница през браузър и инсталираното мобилно приложение в смарт устройство (смартфон или таблет) на Потребителя за участие в „онбординг“ процеса на B-Trust също могат да бъдат в помощ при използване на документа.

1.6. USE CASE Приложими сценарии

Процесите по идентификация, описани в настоящия документ, са организирани така, че да позволят постигане на приложимото ниво на доказване на самоличността съгласно ETSI TS 119 461 за съответния сценарий, вид услуга и приложим регулаторен контекст. В случаите, в които конкретен сценарий, използвано доказателство, наличен доверен източник или приложим национален контекст не позволяват постигане на Extended LoIP, „БОРИКА“ АД може да прилага сценарий, покриващ Baseline LoIP, само доколкото това е допустимо за съответната услуга и приложимата нормативна уредба.

В съответствие с ETSI TS 119 461 „БОРИКА“ АД заявява приложимост на следните сценарии за проверка на самоличността на физически лица:

Отдалечена идентификация без пряко участие на оператор в момента на заснемане, с последваща проверка - unattended remote context – hybrid manual and automated operation

Сценарий за идентификация, при който заснемането на документа за самоличност и изображението на лицето се извършва в автоматизирана интерактивна сесия, а валидирането и/или потвърждаването на резултата се извършва от оператор на по-късен етап. Процесът по тази точка представлява сценарий за отдалечена идентификация по смисъла на ETSI TS 119 461, при който събирането на доказателства за самоличност се извършва в дистанционна среда чрез мобилно приложение, а валидирането и обвързването на заявителя с представеното доказателство се извършват чрез комбинация от автоматизирани средства и контрол от регистрационен оператор.

Отдалечена идентификация с участие на оператор - attended remote context – hybrid manual and automated operation.

Сценарий за идентификация, при който заявителят представя документ за самоличност и своето изображение в реално време чрез мобилно приложение или интернет страница и при неуспешна автоматизирана идентификация оператор извършва видеоразговор – контрол, преглед и потвърждение

а) Идентификация при физическо присъствие - physical presence context – manual operation.

Сценарий за идентификация чрез представяне на физически документ за самоличност в офис на доставчика.
При наличие на правни, технологични или организационни ограничения „БОРИКА“ АД може да допуска само част от горепосочените сценарии за конкретен вид удостоверителна услуга.

Процес/канал за идентификация	Класификация по ETSI TS 119 461	Начин на изпълнение	Приложимост
Идентификация в офис на БОРИКА	physical presence context – manual operation	Присъствено	Услуги, за които се изисква най-висока степен на надеждност
Идентификация чрез мобилно приложение B-Trust	remote identity proofing	Автоматизирано заснемане и проверки, с последващ контрол от оператор	Издаване на КУ за ОКЕП и други приложими услуги
Идентификация чрез интернет страница	remote identity proofing	Автоматизирано заснемане и проверки, с последващ контрол от оператор	Еднократен ОКЕП и други услуги, за които е допустимо
Видеоразговор с оператор	attended remote context – hybrid manual and automated operation	Дистанционно, в реално време, с участие на оператор	При затруднение или ескалация на отдалечената идентификация

2 УЧАСТНИЦИ В „ОНБОРДИНГ“ ПРОЦЕСА

Страните, участващи в „онбординг“ процеса на „БОРИКА“ АД са:

- *Потребител* – физическо лице, чиято самоличност следва сигурно и надеждно да се провери и валидира преди да бъде успешно регистрирано в база данни на Доставчика. Регистрират се само лични данни, които следва да бъдат удостоверени в заявеното от Потребителя КУ. Потребителят е Титуляр („Subject” атрибут) в издаденото Удостоверение и той може електронно да подписва документи само от свое име;

- *Мобилно приложение* за онлайн видео идентификация – работи в смарт устройство (смартфон или таблет) на Потребителя. Чрез него Потребителят участва в „онбординг“ процеса на Доставчика;
- *Интернет страница за идентификация през браузър* - Потребител достъпва конкретен интернет адрес и следва инструкциите, като преминава процес по идентификация, в резултат на което му се издава еднократен ОКЕП.
- *Специализирана интернет страница* – Потребител активира КУ след доставка от куриер.
- *Доставчик*, който доставя и оперира Регистриращ орган РО-ВИ – интегриран информационен ресурс, който се достъпва от Потребителя чрез мобилното приложение. Контролира и управлява последователните стъпки при изпълнение на „онбординг“ процеса.

3 ЗАДЪЛЖЕНИЕ ЗА ПУБЛИКУВАНЕ И ВОДЕНЕ НА РЕГИСТЪР

Виж т. 2 в документа „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“.

Договорът за доставеното КУ за ОКЕП чрез „онбординг“ процес с референция към тази Политика и Практиката, както и удостоверените персонални данни на Потребителя в издадено КУ се показват на Потребителя в мобилното приложение. Той ги преглежда и приема, подписва Договорът с издадения ОКЕП и те се включват в доказателствения файл в базата данни на Доставчика.

Договорът за еднократен ОКЕП, както и удостоверените персонални данни на Потребителя в издаденото КУ се показват на Потребителя в специализирана Интернет страница. Той ги преглежда и приема, подписва Договора с издадения еднократен ОКЕП и те се включват в доказателствения файл в базата.

Договорът за КУ върху хардуерен носител, както и удостоверените персонални данни на Потребителя в издаденото КУ се показват на Потребителя в офис на БОРИКА или чрез специализирана Интернет страница за електронен документооборот. Той ги преглежда и приема, подписва Договора с издаденото КУ и те се включват в доказателствения файл в базата.

За услуги предоставяни през електронен канал на БОРИКА, за които не се подписват договорни отношения, между Потребителя и БОРИКА, се използват Общи условия, които имат силата на договор.

4 ИДЕНТИФИКАЦИЯ И АВТЕНТИФИКАЦИЯ

Доставчикът:

- приема искания за издаване на КУ чрез физическо присъствие, интернет страница през браузър или B-Trust мобилното приложение в смарт устройство (смартфон или таблет) на физическо лице - потребител;
- осъществява проверка за установяване на самоличността на Потребителя и на специфични атрибути за него чрез с изпълнение на „онбординг“ процес, а именно:
  - проверка на действително съществуване на физическото лице;
  - проверка за принадлежност на документа за самоличност на това лице;
  - проверка, че настоящото лице е същото както е посочено в документа;
  - проверка за законна валидност на документа за самоличност;
- регистрира искането за издаване на КУ след успешна проверка и валидация на личността или отхвърля заявеното искане;
- представя на Потребителя валидираните лични данни, които се удостоверяват (иска съгласие);
- уведомява УО да издаде КУ.

Доставчикът гарантира, че физическите лица са правилно идентифицирани, автентифицирани и че заявките за издаване на КУ са напълно, внимателно и надлежно проверени и одобрени, включително пълното име и доказателства за връзката между удостоверените данни и физическото лице.

Когато идентификацията се извършва **за физическо лице, което представлява юридическо лице**, освен идентификацията на самото физическо лице се събират и валидират данни за юридическото лице, за ролята на физическото лице по отношение на юридическото лице, както и за източника на представителната власт. Тази връзка се установява и/или валидира чрез доверени регистри, официални документи, удостоверения, упълномощителни документи или други допустими източници, осигуряващи достатъчна надеждност за съответния контекст.

4.1 Именуване

В процеса на отдалечена видео идентификация името и други лични данни на Потребител се проверява срещу копие на негов валиден законен документ за самоличност или паспорт.

4.1.1 Използване на имена

Виж документ „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“, приложима към КУ на физическо лице. РО-ВИ, работещ от името на Доставчика утвърждава, че имената в заявките за удостоверения съблюдават стандарта X.509.

4.1.2 Използване на псевдоним

Псевдоними (както и анонимност) не се приемат от РО-ВИ. Всички имена на Потребители на КУ са истински имена и са проверени срещу доказателства под формата на доставена снимка (selfie) и копие на документа за самоличност или паспорта при „онбординг“ процеса.

4.1.3 Значимост на имената при вписване

Виж документ „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“, т.3.1.3 (п. 2 и 3).

4.1.4 Правила за интерпретация на имената

Доставчикът включва в КУ лични данни от валидираната идентичност на Потребители, които са успешно проверени и потвърдени от РО-ВИ въз основа на сигурната и надеждна видео идентификация на Потребителя чрез „онбординг“ процеса и представените документи за самоличност. Във всички удостоверения, полето за обичайно име (Common Name, CN) съдържа името на физическото лице, с което то е обичайно обозначавано в дейността си.

4.1.5 Уникалност на имената

Виж документ „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“, приложима към КУ за физическо лице.

Полето "Subject" в удостоверението се формира от данните за Потребителя, които се предоставят отдалечено, автентифицират и валидират чрез „Онбординг“ процеса.

Минималният набор от лични данни за физическо лице, които се събират и проверяват с цел идентификация и попълване на полето „Subject” са:

- фамилно име (имена);
- собствено име (имена);
- бащино име (имена);

- национален уникален идентификатор, в съответствие с техническите спецификации за целите на трансграничната идентификация: за български граждани - ЕГН/ЛНЧ, номер на паспорт или номер на лична карта; за чужденец – национален личен номер, номер на паспорт или номер на лична карта; идентификаторът следва да се съдържа в официален документ за самоличност, чийто срок на валидност не е изтекъл и на който има снимка на идентифицираното лице;
- дата и място на раждане;
- валиден е-мейл адрес;
- страна, на която лицето е гражданин;
- държава на постоянно пребиваване и постоянен адрес.

Наборът от идентификационни данни за физическо лице може да съдържа допълнително:

- пол;
- телефонен номер;
- адрес на електронна поща;
- други (в зависимост от интеграция на РО-ВИ с доверяваща се страна и различните първични регистри и сигурни източници на данни).

В DN на Потребителя за КУ може да се включи името на РО-ВИ – уникален признак на РО-ВИ в B-Trust инфраструктурата, чрез който Доставчикът онлайн е верифицирал и валидирал самоличността.

4.2 Начално валидиране на идентичност

Искане пред Доставчика за първоначално издаване на КУКЕП, КУ за ОКЕП, еднократен ОКЕП и КУУЕП, може да се изпълни само от физическо лице, което ще бъде Титуляр в удостоверението. Доставчикът изпълнява „онбординг“ процес, който изисква, доставя и валидира необходима информация за сигурна идентификация на Титуляря в удостоверението. Допълнително, за целите на КУ за ОКЕП, РО-ВИ събира и верифицира идентификационни данни за мобилно смарт устройство (смартфон или таблет) със заредено мобилно приложение за Android или за iOS на заявителя на КУ за облачен КЕП.

Когато в рамките на услугите на „БОРИКА“ АД се използват средства за електронна идентификация те се издават след успешно приключване на процеса по идентификация (онбординг).

В този случай eID средството се използва като резултат от успешно проведен процес по установяване на самоличността.

4.2.1 Мобилно приложение B-Trust - отдалечена идентификация в съответствие с чл. 24, параграф 1а, буква в

Доставчикът изисква от Потребител да участва чрез мобилното приложениев „онбординг“ процеса на РО-ВИ. За целта Потребителят трябва да:

- изтегли и инсталира мобилното приложение за съответната операционна система;
- стартира процес по регистрация в мобилното приложение;
- приеме Общите условия;
- достави и валидира негов е-мейл адрес;
- достави и валидира притежаван от него телефонен номер на смарт устройството, с което ще работи;
- зададе парола за вход в приложението (или да активира биометрична автентификация за вход, ако смарт устройството поддържа такава).

За да издаде КУ за ОКЕП, Доставчикът изисква чрез РО-ВИ Потребител да регистрира искане за първоначално издаване на удостоверението. Регистрацията чрез „онбординг“ процес включва:

- събиране на лични идентификационни данни за Потребителя;
- сигурна верификация и валидация на данните за самоличност на Потребителя;

- визуализиране на смарт устройството на валидираните лични данни пред Потребителя и искане на съгласие за тяхното удостоверяване в КУ за ОКЕП.

Успешно верифицираните и валидирани данни за Потребителя се записват в регистър на потребителите на B-Trust на „БОРИКА“ АД – създава се профил на Потребителя на КУ за ОКЕП.

За целите на регистрацията и последваща идентификация е необходимо Потребителят да предостави мобилен номер и имейл, които се валидират, като се изпраща еднократна парола (OTP), за да се провери достъпът до заявения номер и имейл адрес. След валидиране на мобилния номер и имейла, Потребителят указва типа и заснема официалният си документ за самоличност и в зависимост от указания тип се изисква заснемане на една или повече страници от документа. Личните данни на Потребителя се въвеждат автоматизирано, след сканиране на документа за самоличност. Системата проверява качеството на снимката на документа – проверява за замъглявания, отблясъци или тъмни петна. Системата проверява изображението на документа - дали е истински документ, а не сканиран, снимка на разпечатан документ за самоличност, екранна снимка и др. Следваща стъпка е Потребителят да заснеме лицето си, като се извършва биометрична проверка.

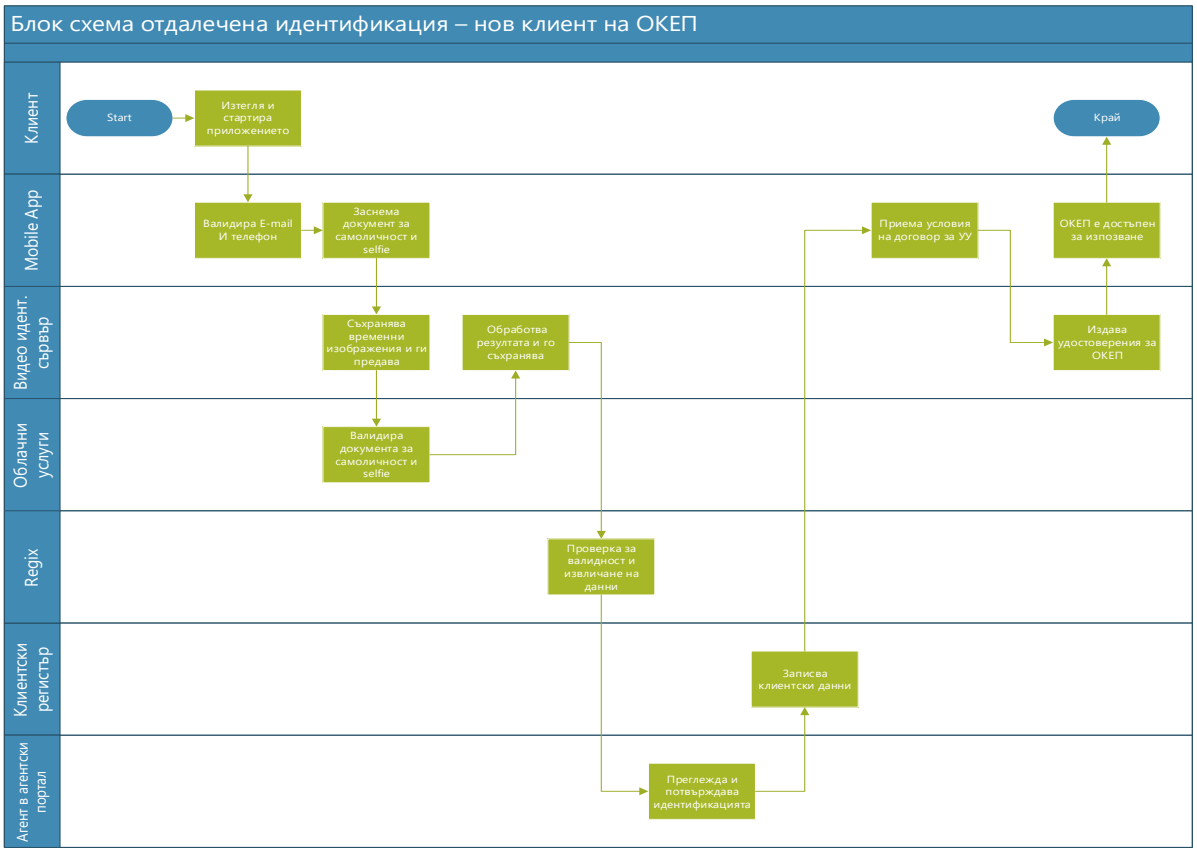
Получените данни от документите за самоличност се валидират автоматично спрямо достоверен източник, ако такъв е наличен, въз основа на интеграция с национални документи за самоличност или регистри за гражданство. В България е налице интеграция с достоверен източник на национално ниво, което прави възможно валидирането на всички данни напълно автоматизирано и получаването на снимка на лицето във формат с висока резолюция, качена в националната база данни..

Методът е национално признат от националния регулаторен орган – Комисията за регулиране на съобщенията, като част от регистрираната в Trust List национално определена услуга за електронна идентификация.

След премината успешна автоматична идентификация, процесът задължително минава и за проверка от оператор на БОРИКА АД.

Процесът по тази точка представлява сценарий за отдалечена идентификация по смисъла на ETSI TS 119 461, при който събирането на доказателства за самоличност се извършва в дистанционна среда чрез мобилно приложение, а валидирането и обвързването на заявителя с представеното доказателство се извършват чрез комбинация от автоматизирани средства и контрол от регистрационен оператор.

Отдалечената идентификация на Потребител протича съгласно представената по-долу блок-схема:



4.2.2 Интернет страница за идентификация - отдалечена идентификация в съответствие с чл. 24, параграф 1а, буква в

Потребител достъпва конкретен интернет адрес и следва инструкциите, като премине процес по идентификация, в резултат на което му се издава еднократен ОКЕП, с който да участва и да използва услугата електронна идентификация на „БОРИКА“ АД или КУКЕП който е заявил, през електронен канал на „БОРИКА“ АД

За целта Потребителят трябва да:

- достъпи конкретен интернет адрес;
- стартира процес по регистрация;
- приеме Общите условия;
- предоставя за целите информация за свой валиден мобилен телефон и адрес на електронна поща, които е необходимо да са изцяло под неговия контрол;
- избира тип документ с който ще се идентифицира - лична карта или паспорт;

За да издаде еднократен ОКЕП или КУКЕП, Доставчикът изисква чрез РО-ВИ Потребител да регистрира искане за първоначално издаване на удостоверението. Регистрацията чрез „онбординг“ процес включва:

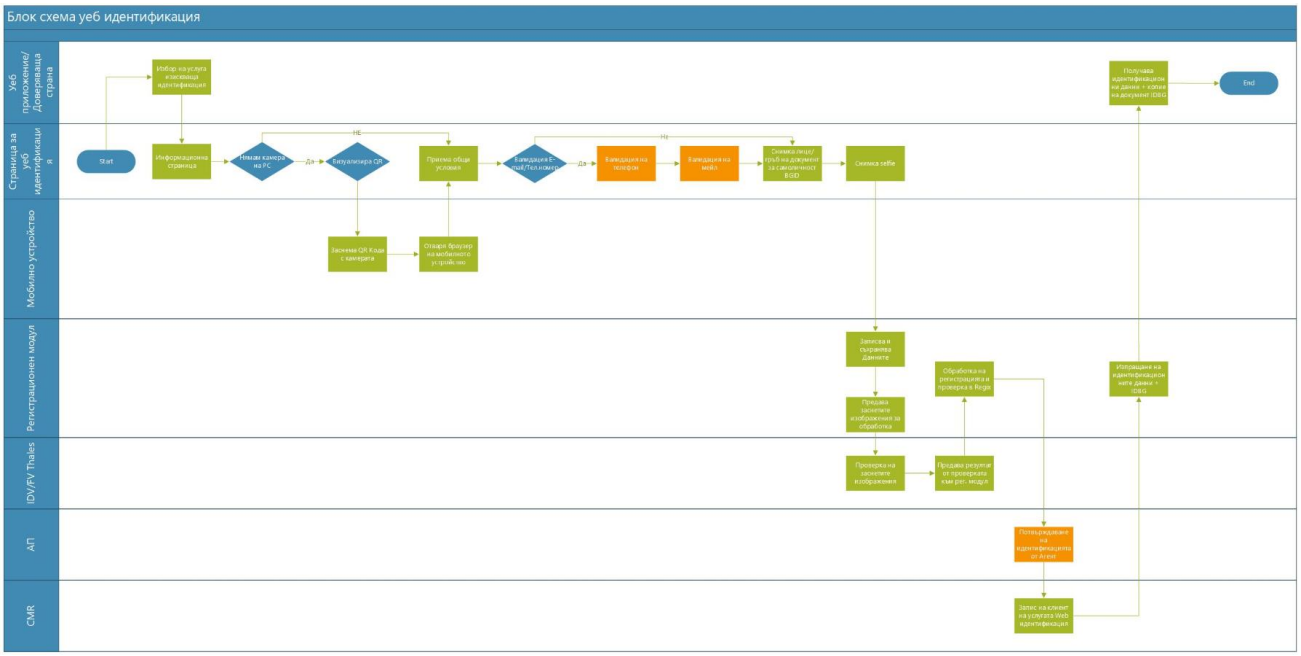
- събиране на лични идентификационни данни за Потребителя;
- сигурна верификация и валидация на данните за самоличност на Потребителя;
- визуализиране на валидираните лични данни пред Потребителя и искане на съгласие за тяхното удостоверяване в КУ за ОКЕП.

Успешно верифицираните и валидирани данни за Потребителя се записват в регистър на потребителите на B-Trust на „БОРИКА“ АД.

Проверките в процеса по отдалечена идентификация през УЕБ са аналогични на тези в процеса на онбординг, описан по-горе, при мобилно приложение.

Процесът по тази точка представлява отдалечена идентификация в уеб среда и се класифицира по ETSI TS 119 461 като remote identity proofing, при което представянето на доказателството за самоличност и изображението на заявителя се извършва дистанционно чрез браузър-базирана сесия.

Отдалечената идентификация на Потребител за еднократен ОКЕП, протича съгласно представената по-долу блок-схема:



4.2.3 Видеоразговор - отдалечена идентификация в съответствие с чл. 24, параграф 1а, буква в

Когато физическото лице - Потребител срещне трудности по време на „онбординг“ процеса, то може да инициира отдалечена видео идентификация през смарт-устройството с мобилното приложение или интернет страница за идентификация, като се свърже с квалифициран оператор на РО-ВИ за провеждане на видеоконферентен разговор и проверка на правно-валиден официален документ за самоличност (лична карта, международен паспорт, лична карта на чужденец и други съобразно националното законодателството на гражданина на съответна държава). РО-ВИ представя валидираните личните идентификационни данни на лицето като ги визуализира пред Потребителя на смарт-устройството или интернет страницата с искане на съгласие за тяхното удостоверяване в КУ, т.е. съгласие Доставчикът да издаде квалифицираното удостоверение.

Автоматично в регистъра на потребителите при Доставчика се създава профил на Потребителя на КУ след успешна идентификация.

Ако по време на видеоконферентния запис операторът прояви съмнение в хода на процеса, той отхвърля и преустановява идентификацията на лицето или се свързва с него. В случай на невалиден

документ за самоличност, операторът прекъсва връзката с лицето. То трябва наново да заснеме документа и отново да се свърже с оператора чрез приложението.

Процесът по тази точка съответства на attended remote identity proofing, тъй като представянето на документа за самоличност и визуалното/биометричното обвързване на заявителя се извършват в сесия, наблюдавана от регистрационен оператор.

4.2.4 Идентификация въз основа на физическо присъствие и проверка на атрибути в съответствие с член 24, параграф 1а, букви г)

Процесът по тази точка съответства на identity proofing in a physical presence context по смисъла на ETSI TS 119 461, при който заявителят се явява лично пред служител на регистрационния орган и представя физически документ за самоличност.
Лице може да бъде идентифицирано чрез посещение в офис на БОРИКА. Това може да се извърши както по инициатива на лицето, така и в случай на неуспешна отдалечена видео идентификация, осъществена чрез смарт устройство и мобилното приложение.
В тези случаи лицето се приканва да посети офис на Доставчика, където се извършва процесът по физическа идентификация.
При посещение в офис на БОРИКА служител на Доставчика извършва първоначална проверка на самоличността чрез представения документ за самоличност. Освен визуална проверка на данните, служителят проверява и актуалността и автентичността на документа, използвайки наличните технически средства в офисите, когато това е необходимо. Данните на лицето се проверяват и в националните регистри, преди да се премине към заявяване на услугата.

След успешна регистрация на Потребител чрез „онбординг“ процес, се подготвя заявка за издаване на КУКЕП като:

- генерира двойка ключове;
- избира опция за авторизация (принадлежност на смарт устройството с мобилното приложение) на Потребителя при подписване с ОКЕП.

Проверка за държане на частния ключ от физическото лице, съответстващ на издадения публичен ключ за КУ за ОКЕП е неприложима. Изпълнява се само ако двойката ключове се генерира при Потребителя. Двойката ключове за ОКЕП се генерира при Доставчика (в RQSCD/HSM).

Издаденото КУКЕП се предава на потребителя, като двойката ключове е генерирана пред него върху квалифицирано устройство. Издадено КУ за ОКЕП не се предава на Потребителя-Титуляр. Доставчикът го публикува в B-Trust Публичния регистър на удостоверенията, а генерираната двойка ключове за този облачен КЕП се съхранява в RQSCD (HSM) на платформата за облачен КЕП. Удостоверението и двойката ключове се асоциират с потребителския акаунт на Титуляря и с неговото мобилно устройство с мобилно приложение в смартфона/таблета.

4.2.5 Специфични атрибути

Когато наред с идентичността на заявителя следва да бъдат проверени и специфични атрибути, се извършва такава проверка чрез подходящи и надеждни източници на данни в зависимост от вида на атрибута, приложимата услуга и нормативния контекст.

РО проверява и потвърждава, че данните и атрибутите, предоставени от заявителя, съответстват на данните, съдържащи се в съответните национални, автентични или авторитетни източници на информация.
Проверката на специфични атрибути се извършва в съответствие **с чл. 24, пар. 1б от Регламент (ЕС) № 910/2014**, изменен с **Регламент (ЕС) № 2024/1183** и може да бъде осъществена пряко от доставчика или

чрез трета страна, когато това е допустимо съгласно приложимата нормативна уредба.
В зависимост от вида на атрибута, наличните източници на информация и използваните технологични средства, проверката може да включва един или комбинация от следните методи:

1. проверка чрез европейския портфейл за цифрова самоличност или чрез средство за електронна идентификация, за което е извършено уведомяване и което отговаря на изискванията на чл. 8 от Регламент (ЕС) № 910/2014 за ниво на осигуреност „високо“;
2. проверка чрез удостоверение за квалифициран електронен подпис или квалифициран електронен печат, когато такова удостоверение е използвано като доказателство за идентичността или атрибутите на лицето;
3. проверка чрез квалифицирано електронно удостоверение за атрибути, когато такова удостоверение е налично и валидно;
4. проверка чрез други методи, осигуряващи висока степен на надеждност, чието съответствие е потвърдено от орган за оценяване на съответствието;
5. проверка чрез достъп до официални регистри или други авторитетни източници на данни чрез защитени електронни канали за обмен на информация;
6. проверка на документ за самоличност чрез технически средства за удостоверяване на неговата автентичност, включително:
    - проверка на данните чрез защитен канал за връзка с първичен регистър или друг автентичен източник на информация,
    - проверка чрез NFC технология при наличие на интегриран RFID чип в документа за самоличност (напр. ICAO ePassport чип);
    - проверка на визуалните и защитните елементи на документа;
    - проверка чрез официални документи или други доказателства, удостоверяващи съответния атрибут.

Специфичен атрибут се счита за потвърден само когато е установена достатъчна връзка между идентифицираното физическо лице източника на информация съответния атрибут, който следва да бъде удостоверен.
Атрибути, които не могат да бъдат потвърдени чрез надежден източник или за които съществуват съмнения относно тяхната достоверност, не се включват в резултата от идентификацията.

4.2.6 Непотвърдена информация

Съгласно документ „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“, приложима към КУ за ОКЕП на физическо лице. Няма непроверена информация, използвана от РО и РО-ВИ, която се удостоверява в издаваното удостоверение.

4.3 Валидиране на идентичност при подновяване

Съгласно документ „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“.

КУ за ОКЕП и еднократен ОКЕП не се подновяват. При съществуващ и валиден Облачен КЕП, потребителят по всяко време може да заяви издаване на нов Облачен КЕП – след успешна автентикация с мобилното приложение.

Еднократният ОКЕП е издаден за конкретна цел. Удостоверението се издава с цел да подпише конкретен електронен документ. Удостоверението не може да се използва след извършване на действието, за което е било издадено.

Подновяване чрез „re-key” (генериране на нова двойка ключове) на издадено КУ за ОКЕП от РО-ВИ (посредством „онбординг“ процес) не се поддържа.

4.4 Валидиране на идентичност при спиране/възобновяване

Искането за спиране/възобновяване на КУ за ОКЕП и КУКЕП трябва да се извърши лично, от самия Титуляр.

Еднократният ОКЕП се издава с цел да подпише конкретен електронен документ. Удостоверението не може да се използва след извършване на действието, за което е бил издаден този ОКЕП.

Виж документ „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“.

4.5 Валидиране на идентичност при прекратяване

Искането за прекратяване на КУ за ОКЕП и КУКЕП трябва да се извърши лично, от самия Титуляр.

Еднократният ОКЕП се използва единствено за еднократното за подписване на конкретен документ. Удостоверението не може да се използва след извършване на действието, за което е бил издаден този ОКЕП.

5 Искане за издаване на удостоверение

Издаването на КУ се предхожда от регистриране на искане от страна на Заявителя чрез РО-ВИ с „онбординг“ процес на Доставчика. Искане за издаване на удостоверение може да направи само лично Потребител като се предхожда от инсталиране и инициализиране на мобилно приложение в мобилното смарт устройство на Заявителя или е достъпил интернет страница за идентификация с цел издаване на КУ, който да послужи за подписването на документите, предоставени от трета страна.

При неуспешен „онбординг“, Заявителят регистрира искане за издаване на удостоверение в онлайн режим чрез провеждане на видеоконферентен разговор с квалифициран оператор в РО-ВИ на Доставчика, който като оторизиран представител на Доставчика онлайн регистрира искане за издаване на КУ за ОКЕП или еднократен ОКЕП.

5.1.1 Доставка на приложение и приемане на общи условия

От електронен магазин (App Store или Google Play), в зависимост от операционната система на смарт устройството, Потребителят изтегля, инсталира и стартира мобилното приложение.

За да участва в „онбординг“ процеса при регистрация, Потребителят следва да приеме Общи условия и Декларация за предоставяне на лични данни.

Преди започване на процеса по идентификация на заявителя се предоставя ясна информация относно целта на идентификацията, приложимите общи условия, необходимите действия от страна на заявителя, категориите данни и атрибути, които ще бъдат събирани, използваните доказателства за самоличност, необходимите технически средства за участие в процеса, както и относно съхраняването на данните и доказателства.

5.1.2 Валидиране на е-мейл и смарт устройство (мобилен номер) и защита на приложение

Потребителят въвежда и изпраща валиден и притежаван от него е-мейл адрес, на който РО-ВИ изпраща съобщение с уникален код. Потребителят въвежда в мобилното приложение получения код, РО-ВИ го сравнява с изпратения и приема за валиден доставения е-мейл адрес.

Аналогична е процедурата за доставка и приемане на валиден мобилен номер на смарт устройство на Потребител от РО-ВИ на Доставчика чрез обмен на еднократен уникален код, изпратен към телефонния

номер или чрез друга техническа услуга, предоставяна от Доставчика, която гарантира поне същото ниво на сигурност.

5.2 „Онбординг“ процес и регистрация (валидиране на самоличност)

По отношение на този документ Потребителят е физическо лице, което е Титуляр/Създател на исканото КУ

За участие в „онбординг“ процес, Потребителят следва да притежава:

- валиден национален официален документ за самоличност;
- смарт устройство с инициализирано мобилно приложение за издаване на КУ за ОКЕП или устройство с браузър за уеб идентификация за издаване на КУ;
- интернет

Искането за издаване чрез „онбординг“ процеса на РО-ВИ включва цялата изискуема информация по ЗЕДЕУУ за Потребителя. Искането може да включва и допълнителна, непроверяема информация, която не се удостоверява, а улеснява контакта на Доставчика с физическото лице.

„Онбординг“ процесът предоставя възможност автоматизирано (без оператор) или чрез квалифициран/обучен оператор на РО-ВИ да генерира двойката криптографски ключове и да включи публичния ключ в заявката за издаване на удостоверението от УО на Доставчика.

5.2.1 Заснемане на официалния документ за самоличност и селфи (selfie) през Интернет страница за идентификация

Потребител достъпил интернет страницата за идентификация през браузър на компютър или мобилен браузър, приема общите условия за отдалечена идентификация.

Страницата подканва Потребителят да покаже документ за самоличност пред камерата (лице и гръб, в зависимост от избрания тип документ).

Потребителят преглежда и потвърждава заснетите изображения.

Страницата изисква от Потребителят да направи снимка на себе си (selfie), следвайки инструкциите за извършване и на liveness detection („снимане на живо“).

Заснетите изображения на официалния документ за самоличност и selfie се предават за временно съхранение на РО-ВИ на „БОРИКА“ АД.

5.2.2 Заснемане на официалния документ за самоличност и селфи (selfie) през мобилното приложение B-Trust

Приложението стартира камерата на смарт устройството (смартфон или таблет) и подканва Потребителя да постави лицевата страна на документа за самоличност пред камерата.

Потребителят указва типа на заснемания документ и в зависимост от указания тип Приложението изисква заснемане на една или повече страници от документа

Потребителят преглежда и потвърждава заснетите изображения.

Приложението изисква от Потребителя да направи снимка на себе си (selfie), следвайки инструкциите на приложението за извършване на „liveness detection“ („снимане на живо“).

Заснетите изображения на официалния документ за самоличност и selfie се предават за временно съхранение на РО-ВИ на „БОРИКА“ АД.

5.2.3 Верифициране на официалния документ за самоличност и селфи

РО-ВИ на Доставчика „БОРИКА“ АД достъпва облачни услуги, чрез които се извършва анализ на изображенията на документа за самоличност и на заснетото изображение на лицето. Анализът може да се подпомага от автоматизирани средства, включително алгоритми за машинно обучение, които сравняват характеристиките на документа със съответния модел на документа и откриват признаци на подправяне, манипулация или несъответствие.

Чрез тези услуги:

- се предават заснетите изображения на документа за самоличност и selfie;
- се извършва проверка за качеството на заснетите изображения;
- се извършва проверка за актуалност и използваемост на документа за самоличност;
- се извличат данните (OCR) и снимката на лицето от документа за самоличност;
- се извършва проверка за съвпадение между снимката на лицето от документа за самоличност и заснетото selfie.

След обработка РО-ВИ на Доставчика получава документ (статус-доклад) от използваните облачни услуги за онлайн видео идентификация. Информационният канал за обмен между РО-ВИ на Доставчика и облачните услуги е защитен (HTTPS/TLS протокол).

При присъствена идентификация могат да се използват допълнителни средства за проверка на защитните елементи на документа, включително увеличителни средства и други специализирани средства за проверка на автентичността на документа.

5.2.4 Валидиране на официалния документ за самоличност

РО-ВИ и РО използва получения документ (статус-доклад) за проверка на валидността на документа за самоличност:

- за български гражданин проверката е чрез националната система Regix и базата данни с първични документи за самоличност-МВР;
- за чужди граждани полученият документ (статус-доклада) се въвежда в списък с чакащи потвърждаване за валидност от Оператор.

За идентификация на физически лица „БОРИКА“ АД приема като официални документи за самоличност най-малко валидна лична карта, международен паспорт и други официални документи за самоличност, допустими съгласно националното законодателство на държавата, която ги е издала, когато същите отговарят на изискванията за надеждност в приложимия контекст.
За валидиране на данните и статуса на документите за самоличност „БОРИКА“ АД използва, когато са налични национални първични регистри, PRADO и други допустими авторитетни източници. Използването на конкретен регистър или източник може да бъде задължително или допълнително в зависимост от вида на документа, националността на лицето, вида на услугата и приложимия контекст на идентификация.

5.2.4.1 Достъпна услуга до първични регистри – физическо лице-български гражданин

РО-ВИ и РО извършва автоматизирана проверка на получените данни от национални първични регистри, с тези от официалния документ (статус-доклада), получен от ползваната услуга. След успешна проверка за валидност на документ за самоличност, данните за Потребителя се извличат и се записват в клиентския регистър на B-Trust („БОРИКА“ АД).

РО-ВИ и РО уведомява Потребителя за успешна идентификация на самоличността и регистрация.

5.2.4.2 Недостъпна услуга до първични регистри

При невъзможност за автоматизирана проверка, РО-ВИ уведомява Потребителя. Полученият документ (статус-доклада) след верификация на официалния документ за самоличност и селфи се записва в списък с чакащи потвърждаване за валидност от Оператор. Квалифициран Оператор на РО-ВИ получава известие за преглед на изчакващи записи с данни за идентификация.

Операторът достъпва списъка с чакащи записи и проверява статуса на регистрацията:

- За официални документи за самоличност на физическо лице-български гражданин предприема действие и следва инструкции за квалифицирана проверка на документа за самоличност;
- За чужди граждани – изпълнява проверка за валидност на документа за самоличност в PRADO; провежда телефонен разговор както и изисква допълнителна информация от Потребителя (напр., фактура за закупена стока/ битови сметки и др.);
- Установяването на идентичността на юридическо лице (Създател), се осъществява чрез проверка в съответните регистри по предоставен ЕИК, БУЛСТАТ или друг идентификационен номер на лицето.

Операторът потвърждава успешната идентификация на Потребителя чрез „онбординг“ процес като подписва електронно това си действие.

5.3 Издаване на удостоверение

5.3.1 Функции по идентификация и автентификация

РО и РО-ВИ чрез „онбординг“ процеса валидира самоличността на Заявителя-физическо лице, доставя персоналните данни, които Доставчикът ще удостовери в КУ и регистрира Потребителя. Виж т. 4.2 (Начално валидиране на идентичност) на този документ.

5.3.2 Идентификация и автентификация с асистент

Участие на Потребител с асистент в „онбординг“ процеса на РО и РО-ВИ на Доставчика се изпълнява съгласно т. 4.2.2 в документа „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“.

5.3.3 Потвърждаване или отхвърляне на искане за издаване

След успешно валидиране на идентичността на Потребител чрез „онбординг“ процеса на РО-ВИ, неговите идентификационни данни се регистрират (чрез утвърждаване от Оператор). Операторът потвърждава идентификацията на Потребителя/Създателя чрез „онбординг“ процес като подписва електронно това си действие.

С успешната регистрация на Потребителя при Доставчика е прието искането за издаване на КУ.

В приложението на смарт устройството/интернет страницата на Потребителя се визуализират валидираните идентификационни данни, които Доставчикът ще удостовери в КУ.

„Онбординг“ процесът се прекратява в случай на:

- невалиден официален документ за самоличност на физическото лице Заявител;
- породени съмнения в Оператор на РО-ВИ при изпълнение и преглед на видеоконферентния разговор с Заявителя;

Ако по време на прегледа на видеозаписа операторът прояви съмнение относно детайли от процеса, той отхвърля и преустановява идентификацията на лицето или се свързва с него за изясняване на процедурата.

РО-ВИ операторът незабавно уведомява Заявителя и посочва причините за отхвърляне на искането за издаване на КУ. Заявител с отхвърлено искане за издаване на КУ може отново да направи искане, чрез РО-ВИ „онбординг“ процес след като отстрани посочените причини за отхвърляне.

РО-ВИ надлежно съхранява и архивира елементи от изпълнение на „онбординг“ процеса както и потвърдената електронна заявка за издаване на удостоверение.

РО-ВИ контролира и утвърждава пред Доставчика верността и точността на включената информация в КУ само към момента на издаването му.

5.3.4 Техническа заявка (PKCS#10) за издаване

Потребителят следва:

- Да приеме и да се съгласи с Договора/общи условия и асоциираната Политика и Практика (този документ).
- да приеме визуализираните лични данни (съгласие за присъствие на националния му персонален идентификатор);
- да избере опция за потвърждаване при подписване с ОКЕП – кода за вход в мобилното приложение или самостоятелен ПИН, респективно биометрия (ако смарт устройството притежава).

След отговор от страна на Потребителя, РО-ВИ генерира:

- техническа заявка PKCS#10 за издаване на КУ, която утвърждава като я подписва и я изпраща към Удостоверяващия орган на Доставчика;
- Договор за удостоверителни услуги, който изпраща на мобилното приложение/специализирана интернет страница към Потребителя.

5.3.5 Действие на Удостоверяващия орган

УО на Доставчика електронно автентифицира РО-ВИ, утвърдил електронната заявка за издаване на КУ. УО генерира заявеното КУ, подписва го с електронния подпис на Доставчика и го публикува незабавно в Публичния си регистър.

Договорът за удостоверителни услуги се подписва с издаденото КУ за ОКЕП.

5.3.6 Известяване на Потребителя от Доставчика

Доставчикът, чрез Службата за известяване на Потребители на КУУ, незабавно известява Потребителя на издаденото и публикувано удостоверение. Службата за известяване изпраща до Потребителя електронно известие по имейл или push-нотификация до мобилното приложение с информация за издаденото КУ, неговия сериен номер и периода му на валидност.

5.4 Приемане и публикуване на удостоверението

Съгласно документ „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“, т. 4.4, приложима към КУ за ОКЕП на физическо лице.

5.5 Употреба

Предимствата на „онбординг“ процеса включват изключително лесно и бързо идентифициране на Потребител от всяко място и по всяко време. Използването на дигиталната онлайн видео идентификация е изцяло съобразена с действащото законодателство. Ползва се от физически лица, притежаващи валиден официален документ за самоличност.

Употребата за КУ е съгласно документ „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“, т. 4.5 и документ „ПОЛИТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ ЗА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС, ОБЛАЧЕН КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС, КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПЕЧАТ И ОБЛАЧЕН КВАЛИФИЦИРАН ПЕЧАТ“, приложими към КУ на физическо лице или КУ на юридическо лице.

5.6 Подновяване на удостоверение

Подновяване на КУ за Облачен КЕП/КЕПечат, КУУЕП и КУУЕПечат не се допуска. По искане на Потребителя, Доставчикът издава ново КУ, като изпълнява първоначална идентификация и установяване на самоличността му.

При съществуващ и валиден Облачен КЕП/КЕПечат, потребителят по всяко време може да заяви издаване на нов – след успешна автентикация с мобилното приложение.

5.7 Подмяна на двойката криптографски ключове (Re-key)

Подновяване чрез „re-key” (генериране на нова двойка ключове) на издадено КУ за Облачен КЕП/КЕПечат, КУУЕП и КУУЕПечат не се поддържа.

5.8 Промяна в удостоверение

Доставчикът допуска промени в съдържанието на информация в издадено и публикувано КУ само при спазване на изискванията и на условията за регистриране на искане за издаване на ново удостоверение пред РО-ВИ с „онбординг“ процес.

5.9 Прекратяване и спиране/възобновяване на удостоверение

Прекратяване на КУ се извършва лично, от самия Титуляр/Създател.

Съгласно документ „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“.

Спиране/възобновяване на КУ се извършва лично от самия Титуляр.

Съгласно документ „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“.

5.10 Статус на удостоверение

Съгласно документ „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“.

5.11 Прекратяване на Договор за удостоверителни услуги

Съгласно документ „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“.

6 СРЕДСТВА, УПРАВЛЕНИЕ И ОПЕРАТИВЕН КОНТРОЛ

6.1 Физически контрол

Въведени са средства за физически контрол за работните места на оператори, които се ползват за обработка и съхраняване на личните данни на записване, получени чрез „онбординг“ процеса, за да се предотврати неоторизиран достъп до тези места - център за идентификация и център за данни (клиентски регистър). Само оторизирани лица, свързани с дейността по изпълнение на „онбординг“ процеса – оператори и системни администратори имат достъп до тях.

В допълнение, Доставчикът ползва резервираност, за да сведе до минимум въздействието от бедствия. В центровете за идентификация не се съхраняват данни за постоянно.

Виж т. 5.1 на документ „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“ за допълнителна информация.

6.2 Процедурен контрол

Доставчикът реализира „концепция за роля“, която гарантира, че съответните задачи на РО-ВИ с „онбординг“ са разделени по такъв начин, че да осигурят ефективен контрол. Достъпът до събиране и обработка на данни се предоставя само на служители със съответните роли и квалификация. Права се предоставят само ако конкретната роля е била възложена със задача, която изисква такъв достъп до лични данни.

Виж т. 5.2 на документ „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“ за допълнителна информация.

6.3 Квалификация и обучение на персонала

Доставчикът гарантира, че Операторите, извършващи „онбординг“ процеса чрез видеоконферентен разговор и регистриране, притежават необходимата квалификация и умения. Това се осъществява чрез провеждане на обучение след назначаване на оператори и преди изпълнение на производствени операции в центровете за видео идентификация. Доставчикът предоставя подробен план за обучение, в който са изброени всички първоначални и периодични обучения. Документирането на обучението е част от системата за управление на човешките ресурси и се съхранява в огнеупорен сейф. Отговорността за провеждането на обучението е на ръководителя на екипа на РО-ВИ с „онбординг“ процес (центъра за идентификация) и мениджъра по човешки ресурси.

Надеждността на всеки служител се определя от Доставчика, като се изискват всички съответни документи (удостоверение за съдимост, автобиография, декларация за липса на конфликт на интереси, информация за кредитоспособност и др.) на този служител.

Виж т. 5.3 на документ „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“ за допълнителна информация.

6.4 Изготвяне и поддържане на журнали

Регистрационните файлове за одит се генерират от РО и РО-ВИ за всички събития, свързани със сигурността на „онбординг“ процеса и свързаните с него услуги. Когато е възможно, файловете за одит на сигурността се събират автоматично. Когато това не е възможно, Оператор използва дневник, хартиен формуляр или друг физически механизъм. Всички файлове за одит на сигурността, както електронни, така и неелектронни, се запазват и предоставят по време на одитите за съответствие.

Събираните регистрационни записи, журнали, видео- и образни материали, извлечени данни, резултати от автоматизирани проверки, резултати от проверки в регистри, действия на оператор и електронни потвърждения се съхраняват като доказателства за проведената идентификация за сроковете и при условията, приложими към съответната удостоверителна услуга и нормативния контекст.

Виж т. 5.4 на документ „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“ за допълнителна информация.

6.5 Архив и поддържане на архива

Виж т. 5.5 на документ „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“.

6.6 Промяна на ключ

Доставчикът може да промени ключа на РО-ВИ, съответстващ на издадено КУ на центъра за идентификация (ВИС), само като издаде ново удостоверение или поднови текущото с „Re-Key”.

Виж т. 5.6 на документ „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“ за допълнителна информация.

6.7 Компрометиране на ключове и възстановяване след авария

Виж т. 5.7 на документ „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“.

6.8 Компрометиране на частен ключ

Виж т. 5.8 на документ „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“.

6.9 Прекратяване дейността на Доставчика

Съгласно т. 5.9 на документ „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“.

7 ФУНКЦИОНАЛЕН МОДЕЛ И СПЕЦИФИКАЦИЯ

7.1 Функционален модел

РО-ВИ с „онбординг“ е функционален елемент към звеното Регистриращ Орган в PKI инфраструктурата на B-Trust на „БОРИКА“ АД. Изпълнява всички стандартни функции на РО съгласно т. 1.4.2 на документа „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“, но използва „онбординг“ процес (онлайн видео идентификация) на Заявител на КУ като алтернатива на

стандартната присъствена идентификация (лице-в-лице). Този функционален елемент автоматизира процедурите на искане за издаване на удостоверение, на събиране, автентифициране и валидиране на лични данни с цел сигурна регистрация на искането за КУ.

След успешната идентификация на самоличност, РО-ВИ регистрира искането за успешно, предоставя в смарт устройството данните за удостоверяване в КУ за ОКЕП/ОКЕПечат и иска тяхното одобрение от Потребителя.

Функциите, които изпълнява РО-ВИ с „онбординг“ процес са:

- приема искания за издаване на КУ за ОКЕП/ОКЕПечат от смарт-устройство (смартфон или таблет) или еднократен ОКЕП, КУКЕП/КУУЕП/КУКЕПечат/КУУЕПечат през интернет страница за идентификация през браузър на физическо лице – потребител.
- осъществява проверка за установяване на самоличността на Потребителя и на специфични данни за него чрез изпълнение на „онбординг“ процес, а именно:
    - проверка на действително съществуване на физическото лице;
    - проверка за принадлежност на официалния документ за самоличност на това лице;
    - проверка, че настоящото лице е същото както е посочено в документа;
    - проверка за законна валидност на официалния документ за самоличност;
    - при необходимост се извършва проверка на действително съществуване на юридическо лице и връзката на физическото лице с юридическото.
- регистрира искането за издаване на КУ след успешна проверка и валидация или отхвърля заявеното искане;
- представя на Потребителя валидираните лични данни, които ще се удостоверяват с искане на съгласие;
- уведомява УО да издаде КУ.

Функционалният модел на „онбординг“ процеса на РО-ВИ на Доставчика „БОРИКА“ АД следва и е в съответствие с т. 5 (5.2 - 5.11) на този документ.

7.2 Спецификация

ДКУУ „БОРИКА“ АД имплементира отдалечена регистрация на Потребители на КУУ на B-Trust инфраструктурата с конпонентата РО-ВИ към звеното Регистриращ орган на тази инфраструктура.

РО-ВИ включва следните съставящи компоненти:

- Видео идентификационен сървър/Видео идентификационен център (ВИС);
- Агентски портал (АП);
- Мобилно приложение в смарт устройство (смартфон или таблет);
- Специализирана Страница през интернет браузър за активация на удостоверение.

В допълнение, РО-ВИ използва външни за B-Trust инфраструктурата утвърдени и сертифицирани източници на услуги с цел сигурно и надеждно валидиране на самоличността на физическо лице от разстояние - неприсъствена идентификация:

- Сертифицирани и утвърдени „облачни услуги“ за анализ на видео изображения;
- Национално утвърдена и използвана услуга за достъп до публични национални първични регистри.

7.3 Управление на достъпа

Всички компоненти, изискващи физическа и логическа защита относно критични данни и информация (сървъри, комуникационно оборудване, ключове, архиви, др.), са обособени в помещения и зони с висока защита на достъпа. Физическият и логически контрол на достъпа до инфраструктурата на B-Trust® на ДКУУ е в съответствие с документа „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“ и е приложим към РО-ВИ, част от звеното РО в B-Trust PKI инфраструктурата на Доставчика.

7.4 Операционна сигурност

Операционната сигурност на РО-ВИ отговаря на изискванията за сигурността на компютърните системи в инфраструктурата на B-Trust съгласно документа „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“

7.5 Мрежова сигурност

Доставчикът използва съвременни технически средства за обмен и защита на информация на РО-ВИ с Потребители, с Удостоверяващия орган и със средствата, доставящи външни услуги (анализ на видеоизображения и достъп до национални регистри), за да гарантира мрежова сигурност на системите срещу външни интервенции и заплахи.

Информационните системи и компоненти, чрез които се извършва проверката на самоличността и се формира решението за приемане, отхвърляне или ескалация на процеса по идентификация, са логически и/или физически отделени от некритични информационни системи на „БОРИКА“ АД, включително офисни, административни и спомагателни системи.

7.6 Информационна сигурност

Информационната сигурност на компонентите на B-Trust инфраструктурата, включително и на РО-ВИ, е в обхвата на общата Политика на информационна сигурност на „БОРИКА“ АД, утвърдена от ръководството на фирмата. Тази политика установява организационните мерки и процедури по управление на сигурността на всички системи и информационните активи, чрез които „БОРИКА“ АД предоставя всички свои услуги. Персоналът, имащ пряко отношения към тези системи и активи е запознат и изпълнява тази Политика. Подписани/подпечатени електронни документи с КЕП/КЕПечат могат да съдържат информация, която да се счита за лични данни. В съответствие с нормативната уредба относно такъв тип данни, „БОРИКА“ АД като ДКУУ, респективно като Доставчик на УСЛУГАТА, е регистрирана от КЗЛД като администратор на лични данни

7.7 Непрекъсваемост

Съгласно прилаганите от Доставчика общи мерки, гарантиращи непрекъсваемост на функционирането на B-Trust инфраструктурата, в това число, на квалифицирани удостоверителни услуги, базиращи се на резервираност на критичните компоненти на инфраструктурата.

8 ОЦЕНКА НА РИСКА

Отчитайки установени бизнес и технически проблеми при доставка, опериране и поддръжка на удостоверителните услуги, Доставчикът извършва оценка на риска, за да идентифицира, анализира и оцени свързаните с това рискове.

Избират се подходящи мерки за избягване на идентифицирани рискове като се отчитат резултатите от оценката на риска. Приеманите мерки гарантират ниво на сигурност, съизмеримо със степента на идентифицираните рискове.

Доставчикът документира чрез Практиката и Политиката, включени като части от настоящия документ, изискванията към сигурността и оперативните процедури, необходими за избягване на идентифицирани рискове за „онбординг“ процеса на РО-ВИ.

Периодично се изпълнява преглед и оценка на риска с цел преодоляване на идентифицирани рискови фактори. Резултатите се докладват на Мениджмънта на „БОРИКА“ АД, който одобрява резултатите от оценката на риска, предписаните мерки за преодоляване на идентифицирани рискови фактори и приема установения остатъчен риск относно прилагания „онбординг“ процес за отдалечена видео идентификация на Потребители на B-Trust.

Оценката на риска по отношение на процесите по идентификация се извършва и преразглежда регулярно от „БОРИКА“ АД с цел да се гарантира, че използваните процедури, технологии и организационни мерки осигуряват надеждно установяване на самоличността на заявителите.

Прегледът на оценката на риска се извършва най-малко веднъж годишно, както и при всяка съществена промяна в процесите по идентификация, използваните технологични средства, източниците на данни или видовете доказателства за самоличност, използвани при „онбординг“ процеса.

В рамките на този преглед се анализират потенциални заплахи и уязвимости, които могат да повлияят върху надеждността на процеса по установяване на самоличността, включително, но не само:

- опити за представяне на фалшиви или манипулирани документи за самоличност; атаки, свързани с представяне на изкуствено създадени изображения или видеоматериали (presentation attacks);
- опити за инжектиране на предварително записано или генерирано съдържание в процеса на идентификация (injection attacks);
- използване на технологии за създаване на синтетично или манипулирано изображение или deep fake
- опити за измама чрез социално инженерство или подвеждане на оператора или на автоматизираните системи;
- други заплахи, които могат да доведат до неправилно установяване на самоличността на заявителя или до компрометиране на процеса по идентификация.

При идентифициране на нови рискове или промени в нивото на съществуващите рискове „БОРИКА“ АД предприема подходящи технически, организационни и процедурни мерки за тяхното ограничаване, включително актуализиране на процедурите по идентификация, подобряване на използваните технологични средства, въвеждане на допълнителни проверки или обучение на персонала, участващ в процеса.

Резултатите от оценката на риска се документират и се представят на ръководството на „БОРИКА“ АД, което одобрява необходимите мерки за управление на риска и приема остатъчния риск, свързан с предоставянето на услугата по идентификация.

Оценката на риска отчита и приложимото ниво на доказване на самоличността (LoIP), което следва да бъде постигнато при съответните сценарии на идентификация.

9 ПРОВЕРКА И КОНТРОЛ НА ДЕЙНОСТТА НА ДОСТАВЧИКА

Съгласно т. 9 на документа „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“.

10 ДРУГИ БИЗНЕС УСЛОВИЯ И ПРАВНИ АСПЕКТИ

Доставчикът отговоря и гарантира, че спазва точно условията в настоящия документ, изискванията на ЗЕДЕУУ и на нормативната уредба при осъществяване на дейността на регистриран ДКУУ.

Доставчикът гарантира, че РО-ВИ с „онбординг“ процес изпълнява своите функции и задължения в пълно съответствие с условията в този документ, с изискванията и процедурите в Политиката и Практиката приложими за КУ, както и издадените вътрешни оперативни инструкции.

Потребителят трябва да спазва точно условията и процедурите на „онбординг“ процеса съгласно този документ при искане за издаване на КУ чрез РО-ВИ и съответната Политика за ползване на това удостоверение.

Подробна информация относно бизнес условията и правните аспекти в отношенията на Доставчика „БОРИКА“ АД с Потребители на удостоверителни услуги приложими за КУ се съдържа в т. 10 на документа „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ“.