БОРИКА
БАНКОВИ УСЛУГИ

ПОЛИТИКА И ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНА УСЛУГА ЗА ЕЛЕКТРОННА ПРЕПОРЪЧАНА ПОЩА

Версия 1.1

Хронология на измененията на документа				
Версия	**Автор (и)**	**Дата**	**Състояние**	**Коментар**
1.0	Маргарита Бонева	1.08.2024	Утвърден	Първо издание
1.1	Маргарита Бонева	22.01.2025	Утвърден	Корекция – смяна на сертификат на услугата

СЪДЪРЖАНИЕ

Съкращения на български език 4
Съкращения на английски език 5
СПЕЦИФИЧНИ ТЕРМИНИ И ОПРЕДЕЛЕНИЯ КЪМ ДОКУМЕНТА 6
СЪОТВЕТСТВИЕ И УПОТРЕБА 8
1 ОБЩИ ПОЛОЖЕНИЯ 10
1.1 Удостоверяващ орган на „БОРИКА“ АД 10
1.2 Идентификатори в документа 11
1.3 Управление на Политиката 11
2 УЧАСТНИЦИ В ИНФРАСТРУКТУРАТА 11
2.1. „Удостоверяващия орган“ 11
2.2. Инфраструктурата на B-Trust® 11
2.3. Инфраструктурата на B-Trust® 12
2.4 Потребители 12
3 Профили на удостоверения 12
4 Квалифицираната препоръчана електронна поща - основни характеристики и предназначение 15
4.1 Първоначална идентификация и установяване на идентичност 15
5 ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНА УСЛУГА ЗА ЕЛЕКТРОННА ПРЕПОРЪЧАНА ПОЩА 16
6 ИДЕНТИФИКАЦИЯ НА ИЗПРАЩАЧ/ПОЛУЧАТЕЛ 18
7 АВТЕНТИКАЦИЯ 18
8 СЪЗДАВАНЕ НА ДОКАЗАТЕЛСТВА 19
8.1 Доказателства, свързани с подателя 19
8.2 Доказателства, свързани с получателя 19
8.3 Връчване на съдържание 20
9 АРХИВИРАНЕ 20
10 ПРЕКРАТЯВАНЕ НА УСЛУГАТА 20
11 ЗАДЪЛЖЕНИЯ НА ПОТРЕБИТЕЛИТЕ 20
12 ФИЗИЧЕСКИ КОНТРОЛ 21
12.1 Управление на достъпа 21
12.2 Операционна сигурност 21
12.3 Мрежова сигурност 21
12.4 Информационна сигурност 21
13 НЕПРЕКЪСВАЕМОСТ 22
14 ОЦЕНКА НА РИСКА 22
15 ПРОВЕРКА И КОНТРОЛ НА ДЕЙНОСТТА НА ДОСТАВЧИКА 22
16 ДРУГИ БИЗНЕС УСЛОВИЯ И ПРАВНИ АСПЕКТИ 22

Съкращения на български език

АД	Акционерно дружество
ДКУУ	Доставчик на квалифицирани удостоверителни услуги
ЕГН	Единен граждански номер
ЗЕДЕУУ	Закон за електронния документ и електронните удостоверителни услуги
КРС	Комисия за регулиране на съобщенията
КУКЕП	Квалифицирано удостоверение за квалифициран електронен подпис
КУКЕПечат	Квалифицирано удостоверение за квалифициран електронен печат
КУУ	Квалифицирани удостоверителни услуги
КУУЕП	Квалифицирано удостоверение за професионален усъвършенстван електронен подпис
КУУЕПечат	Квалифицирано удостоверение за професионален усъвършенстван електронен печат
ПИН	Персонален идентификационен номер
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
eIDAS	ЕС Регламент 910/2014
ETSI	European Telecommunications Standards Institute - Европейски институт за стандарти в далекосъобщенията
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
QERDS	Qualified Electronic Registered Delivery Service – Квалифицирана услуга за електронна препоръчана поща

СПЕЦИФИЧНИ ТЕРМИНИ И ОПРЕДЕЛЕНИЯ КЪМ ДОКУМЕНТА

Документ за самоличност – валиден документ, съдържащ данни за идентификация на физическо лице, съобразно с националното законодателство на съответната държава.

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

Лични данни - всяка информация съгласно определението в член 4, точка 1 от Регламент (ЕС) 2016/679.

Проверка на самоличност – процес, при който данните за идентификация на лице или средствата за електронна идентификация се съпоставят или се свързват със съществуващ профил, принадлежащ на същото лице.

Квалифицирана услуга за електронна препоръчана поща (QERDS) - УСЛУГА за електронна препоръчана поща, която отговаря на изискванията, предвидени в Регламент (ЕС) № 910/2014 и Регламент (ЕС) 2024/1183.

Доставчик на квалифицирана услуга за електронна препоръчана поща - субект, който предоставя УСЛУГАТА - Квалифициран доставчик на квалифицирани удостоверителни услуги, който предоставя квалифицирана услуга за електронна препоръчана поща.

ERDS доказателства – данни, генерирани от УСЛУГАТА, които служат за (неотменимо) доказателство, че определено събитие е настъпило в определен момент в процеса на електронната доставка.

Подател - физическо или юридическо лице, което изпраща определено съдържание.

Получател - физическо или юридическо лице, което получава определено съдържание.

e-Пратка - данни, включително потребителско съдържание и метаданни за изпращане към УСЛУГАТА.

Предаване - акт за успешно преминаване на потребителското съдържание през границата на инфраструктурата/системата на УСЛУГАТА към Получателя.

Доставка – акт за предоставяне на потребителското съдържание на разположение на Получателя в границите на инфраструктурата/системата на УСЛУГАТА.

Връчване – връчена доставка, когато изпратеното от подателя съдържание успешно постъпи в информационната система на получателя.

Потребителски агент - средство, състоящо се от софтуер и/или хардуер, чрез което Подателите и Получателите участват в обмена на данни с УСЛУГАТА.

Метаданни за предаване - данни, свързани със потребителското съдържание, които се генерират от УСЛУГАТА и се предават на потребителския агент.

СЪОТВЕТСТВИЕ И УПОТРЕБА

Този Документ:

- е разработен от „БОРИКА" АД, юридическото лице, регистрирано в Търговския регистър и регистъра на юридическите лица с нестопанска цел към Агенцията по вписванията с ЕИК 201230426;
- влиза в сила на 20.10.2024 г.;
- 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, в случаите в които е приложимо. 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:

- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market
- Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements;
- ETSI EN 319 411-2 Policy and security requirements for Trust Service Providers issuing certificates. Requirements for trust service providers issuing EU qualified certificates;
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps;
- ETSI EN 319 522-1 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 1: Framework and Architecture;
- ETSI EN 319 522-2 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 2 Semantic Contents;
- ETSI EN 319 522-3 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 3: Formats;

- ETSI EN 319 522-4-1 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 4-1: Message delivery bindings;
- ETSI EN 319 522-4-2 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 4-2: Evidence and identification bindings;
- ETSI EN 319 522-4-3 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 4-3 Capability and requirements bindings;
- ETSI TS 119 461 „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects“.
- ETSI EN 319 412-5 “Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements;
- ETSI TR 119 520-1 Electronic Signatures and Trust Infrastructures (ESI); Framework of ERDS/REM standards; Part 1: New (Q)ERDS/(Q)ERDSP standardization rationalized framework as a result of the new components brought by eIDAS 2.0;
- ETSI TR 119 520-2 Electronic Signatures and Trust Infrastructures (ESI); Framework of ERDS/REM standards; Part 2: Impact of emerging technologies on ERDS/REM Models.
- Закон за електронното управление (ЗЕУ) и Правилника към закона;
- Закон за електронна идентификация (ЗЕИ) и Правилник към закона;
- Закон за електронния документ и електронните удостоверителни услуги (ЗЕДЕУУ) и приложимите към закона нормативни уредби;

Допълнителна 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
Официална страница на доставчика: www.b-trust.bg

1 ОБЩИ ПОЛОЖЕНИЯ

Квалифицираната електронна препоръчана поща е дигитален еквивалент на класическата препоръчана поща с обратна разписка и има същата правна стойност. Квалифицираната електронна препоръчана поща предоставя доказателство за изпращането и получаването на данните и защитава предаваните документи срещу риск от загуба, кражба, или непозволени изменения. Услугата е предназначена за физически и юридически лица, държавни институции, общини и обществени организации. Данните, изпратени и получени чрез QERDS, могат да се използват в съдебни производства във всички държави-членки на ЕС. Правната сила и допустимостта на електронен документ като доказателство в съдебни производства не могат да бъдат оспорени единствено на основанието, че той е в електронна форма.

Услугата Препоръчана електронна поща обхваща:

- C2C (Client to Client) – Подател и Получател на потребителско съдържание са физически лица;
- B2C (Business to Client) – Подателят е юридическо лице, а Получател(и) са физически лица;
- C2B (Client to Business) – Подателят е физическо лице, а Получател е юридическо лице;
- B2B (Business to Business) – Подател и Получател са юридически лица, които обслужват/оперират бизнес-приложения.

Потребителските агенти, през които Подател и Получател комуникират с УСЛУГАТА са следните:

- Мобилно приложение B-Trust Mobile;
- Уеб портал My B-Trust;
- Приложен програмен интерфейс (API);

Услугата се предоставя в съответствие с чл. 44 от Регламент (ЕС) № 910/2014 и с Регламент (ЕС) 2024/1183 и позволява връчване на препоръчана поща от мобилно приложение към мобилно приложение, от мобилно приложение към специализиран уеб портал и обратно, от API към мобилно приложение и обратно.

1.1 Удостоверяващ орган на „БОРИКА“ АД

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

Акредитацията на „БОРИКА“ АД като ДКУУ е в съответствие с Регламента и 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 съответната услуга.

1.2 Идентификатори в документа

Политиката и Практиката на „БОРИКА“ АД относно УСЛУГАТА допълват общите политика и практика на предоставяните КУУ от Доставчика. Конкретно за този документ се описва какво предлага Доставчикът, за да покаже приложимостта на УСЛУГАТА, условията и правилата, към които той се придържа. Предоставяне на УСЛУГАТА се осъществява чрез обекта обозначен с идентификатор 1.3.6.1.4.1.15862.1.6.11 в документа „Практика при предоставяне на квалифицирани удостоверения и квалифицирани удостоверителни услуги от „БОРИКА“ АД (B-Trust CPSeIDAS)“:

Наименование на Политиката	Идентификатор на обект
QUALIFIED ELECTRONIC REGISTERED DELIVERY SERVICE POLICY AND PRACTICE	1.3.6.1.4.1.15862.1.6.11

1.3 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. Всяка представена и одобрена нова версия или редакция на този документ незабавно се публикува на сайта на Доставчика.

Документът може да бъде променян по всяко време и се съобщава на заинтересованите лица чрез сайта на дружеството в интернет. Настоящият документ е неразделна част от политиките и практиките за предоставяне на квалифицирани услуги.

2 УЧАСТНИЦИ В ИНФРАСТРУКТУРАТА

2.1. „Удостоверяващия орган“ на B-Trust® на ДКУУ „БОРИКА“ АД е организационно обособено звено, което осъществява дейност по издаване, предоставяне и поддържане на КУ и на КУУ за тях. УО няма самостоятелна правосубектност и всички осъществени действия и актове на служителите му се извършват в качеството им на служители на Доставчика, в рамките на предоставените им правомощия.

2.2. Инфраструктурата на B-Trust® има двустепенна йерархия на УО за издаване и поддръжка на КУКЕП и КУКЕПечат, както следва:

- Базов УО „B-Trust Root Qualified CA" - издава удостоверения на подчинените в йерархично отношение оперативни УО на Доставчика;

- Оперативен УО „B-Trust Operational Qualified CA" - издава КУКЕП и КУКЕПечат, съгласно Политиката за предоставяне на тези КУ;

2.3. Инфраструктурата на B-Trust® има двустепенна йерархия на УО за издаване и поддръжка на КУУЕП, КУУЕПечат и КУ за автентичност на уебсайт, както следва:

- Базов УО „B-Trust Root Advanced CA" - издава удостоверения на подчинените в йерархично отношение оперативни УО на Доставчика;
- Оперативен УО „B-Trust Operational Advanced CA" - издава КУУЕП и КУУЕПечат, съгласно Политиките за предоставяне на тези КУ.

ДКУУ си запазва правото да разшири инфраструктурата на B-Trust® с друга йерархия от УО.

Детайлно описание се съдържа в документа „ПРАКТИКА ПРИ ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНИ УДОСТОВЕРЕНИЯ И УДОСТОВЕРИТЕЛНИ УСЛУГИ ОТ „БОРИКА“ АД“.

2.4 Потребители

Всяко физическо или юридическо лице, което има сключен договор с „БОРИКА“ АД за квалифицирана услуга за електронна препоръчана поща е потребител на QERDS и може да влиза в ролята на изпращач и/или на получател.

Когато това може да бъде изпълнено на практика, удостоверителната услуга и продуктите за QERDS са налични и за хора с увреждания.

Трети страни, наричани още доверяващи се страни, са физически или юридически лица, които се доверяват на доказателствата, предоставени от доставчика във връзка с QERDS.

3 Профили на удостоверения

Профил на удостоверението на B-Trust Qualified Time Stamp Authority е посочен по-долу:

Поле	Атрибути	Значение/Стойност
Version	-	V3
Serial number	-	4431e2c388ab5130
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Operational Qualified CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	2023-03-14 T12:14:21Z
Validity to	-	2028-03-13 T12:14:21Z
Subject	CN =	B-Trust Qualified Time Stamp Authority
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97)	NTRBG-201230426

	=		
	C =	BG	
Public key	-	RSA(2048 Bits)	
Subject Key Identifier		c3 bb 28 36 0a 9f d9 b6 57 65 ca dc 8f bb 00 6c 6a d9 52 52	
Authority Key Identifier	KeyID =	27 cf 08 43 04 f0 c5 83 37 67 81 17 4d fc 05 e6 db 65 8b b0	
Issuer Alternative Name	URL=	http://www.b-trust.org	
Subject Alternative Name	URL=	http://tsa.b-trust.org	
Basic Constraints	Subject Type = Path length Constraint =	End Entity None	
Certificate Policy	-	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.6.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.b-trust.org/documents/cps [2]Certificate Policy: Policy Identifier=0.4.0.2042.1.2	
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.b-trust.org/repository/B-TrustOperationalQCA.crl	
Authority Information Access	-	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.b-trust.org [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.b-trust.org/repository/B-TrustOperationalQCAOCSP.cer	
Key Usage(critical)	-	Digital Signature, Non-Repudiation (c0)	
Enhanced Key Usage (critical)	-	Time Stamping (1.3.6.1.5.5.7.3.8)	
Thumbprint (Sha1)		2D:1E:10:B1:E7:1E:BC:05:80:50:F3:22:8F:80:10:36:8C:30:DB:F1	
Thumbprint (Sha256)		4A:D9:BA:68:27:5C:5B:73:0B:D8:78:6A:38:3A:54:9D:DA:74:7F:09:BD:D0:F1:B7:08:A9:BA:8D:C4:2C:38:4D	
Qualified Statement	Qualified Certificate Statement:	id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-SemanticsId-Legal (oid=0.4.0.194121.1.2)
		id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)	
		id-etsi-qcs-QcSSCD (oid=0.4.0.1862.1.4)	
		id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.b-trust.org/documents/pds/ts_pds_en.pdf language=en

Профил на удостоверението на B-Trust Qualified Electronic Registered Delivery Service е посочен по-долу:

Квалифицирано удостоверение за квалифициран електронен печат на квалифицираната услуга за електронна препоръчана поща. Чрез него електронно се подписват доказателства.

Поле	Атрибути	Значение/Стойност
Version	-	V3
Serial number	-	4959e0854eb14c61
Signature algorithm	-	Sha256RSA
Signature hash algorithm	-	Sha256
Issuer	CN =	B-Trust Operational Qualified CA
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Validity from	-	2025-01-22 T14:36:13Z
Validity to	-	2030-01-21 T14:36:13Z
Subject	CN =	B-Trust Qualified Electronic Registered Delivery Service
	OU =	B-Trust
	O =	BORICA AD
	OrganizationIdentifier(2.5.4.97) =	NTRBG-201230426
	C =	BG
Public key	-	RSA(4096 Bits)
Subject Key Identifier		3d0721d99ed3f1cb34accc8cd0646912e6c8f3bb
Authority Key Identifier	KeyID =	27cf084304f0c583376781174dfc05e6db658bb0
Issuer Alternative Name	URL=	http://www.b-trust.bg
Basic Constraints	Subject Type = Path length Constraint =	End Entity None
Certificate Policy	-	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.15862.1.6.1.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.b-trust.org/documents/cps [2]Certificate Policy: Policy Identifier=**1.3.6.1.4.1.15862.1.6.11.1**
CRL Distribution Points	-	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.b-trust.org/repository/B-TrustOperationalQCA.crl
Authority Information Access	-	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.b-trust.org [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name:

		URL=http://ca.b-trust.org/repository/B-TrustOperationalQCAOCSP.cer	
Key Usage(critical)	-	Digital Signature, Non-Repudiation (c0)	
Qualified Statement	Qualified Certificate Statement:	id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-SemanticsId-Legal (oid=0.4.0.194121.1.2)
		id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)	
		id-etsi-qcs-QcSSCD (oid=0.4.0.1862.1.4)	
		d-etsi-qcs-QcType (oid=0.4.0.1862.1.6)	d-etsi-qct-eseal (oid=0.4.0.1862.1.6.2)
		id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)	PdsLocations PdsLocation=https://www.b-trust.org/documents/pds/ts_pds_en.pdf language=en

4 Квалифицирана електронна препоръчана поща - основни характеристики и предназначение

Квалифицираната електронна препоръчана поща:

- Гарантира сигурна идентификация на адресата и изпращача;
- Осигурява поверителност, интегритет и автентичност на данните, които се изпращат;
- Осигурява неотменимо потвърждение за извършена доставка на данните.

Предоставя доказателства за всяка от стъпките в процеса на трансфера на данни между страните, които могат да бъдат използвани в съдебни производства. Цялата информация по предоставяне на QERDS се съхранява за период от 10 години, съобразено с националното законодателство на Република България (ЗЕДЕУУ).

4.1 Първоначална идентификация и установяване на идентичност

4.1.1. Установяване на самоличност на физическо лице

Установяването на самоличността на физическо лице се извършва чрез:

- отдалечена видео идентификация или
- физическото присъствие на физическото лице или на упълномощен представител на юридическото лице или
- средство за електронна идентификация, което отговаря на изискванията, посочени в член 8 от Регламент (ЕС) № 910/2014 и в Регламент (ЕС) 2024/1183 по отношение на нивата на сигурност „значителни“ или „високи“.

Минималният набор от данни за физическо лице, за което се прави проверка в достоверен източник включва: трите имена (собствено име, презиме, фамилно име), дата на раждане,

национален уникален идентификатор. Минималният набор от данни за физическо лице може да съдържат и допълнителни специфични данни: номер на мобилен телефон и адрес на електронна поща, място на раждане, адрес местоживеене и други.

С цел предотвратяване на неоторизирано използване на услугите и с оглед осигуряване на възможност за проверка на автентичността на данните, предоставени от Потребителя, в интерес както на Потребителя, така и на Доставчика е постигане на максимално високо ниво на сигурност чрез снемането на копие от документа за самоличност на Потребителя и съхраняването му в хартиен или електронен вид. Уговорка за снемане и съхраняване на копие от документа за самоличност на Потребителя може да бъде включена в сключения между страните Договор за удостоверителни услуги. В случай, че съгласие за снемане и съхранение на копие от документ за самоличност не бъде постигнато, Доставчикът може да откаже предоставянето на квалифицирана удостоверителна услуга предвид невъзможността да гарантира безпрепятственото предоставяне на УСЛУГАТА.

4.1.2. Установяване на идентичността на юридическо лице

Установяването на първоначална самоличност на юридическо лице се осъществява чрез автоматизирана проверка в първични регистри.

Минималният набор от данни за юридическо лице трябва да съдържа: наименование на юридическото лице, уникален национален идентификатор (За България това е ЕИК/БУЛСТАТ). Минималният набор от данни за юридическо лице може да съдържа допълнителни данни: адрес на управление, регистрационен номер по ДДС, други данни.

4.1.3. Установяване на самоличност на физическо лице, упълномощен представител на юридическо лице

За физическите лица се извършва първоначална проверка на самоличност по реда на **точка 4.1.1**. Представителната власт на физическо лице спрямо юридическо лице се проверява в съответния публичен регистър. В случай че физическото лице не е законен представител, упълномощаването се доказва с изрично нотариално заверено пълномощно.

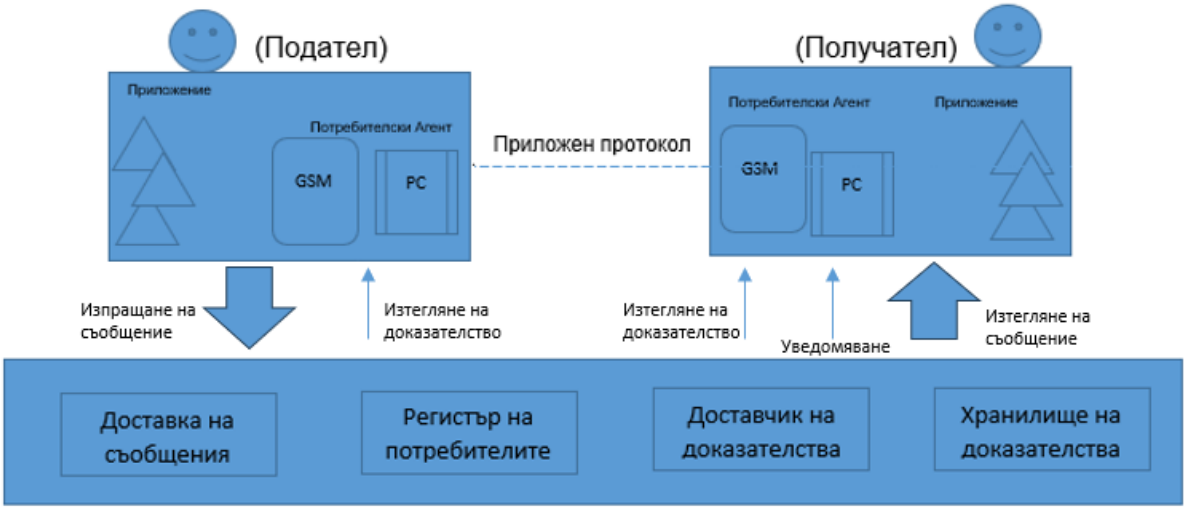
При извършване на повторна заявка за ползване на УСЛУГАТА не се извършва отново идентификация, а само проверка на актуалността на данните за самоличност.

5 ПРЕДОСТАВЯНЕ НА КВАЛИФИЦИРАНА УСЛУГА ЗА ЕЛЕКТРОННА ПРЕПОРЪЧАНА ПОЩА

QERDS се достъпва чрез способите на приложно-програмен интерфейс (Application Programming Interface/API), мобилно приложение или уеб портал. Използването на услугата изисква първоначална идентификация на изпращача и получателя, която се осъществява отдалечено или чрез лично явяване на лицата или техни представители пред РО.

В съответствие с документа ETSI EN 319 522-1 логическият модел на УСЛУГАТА следва модела на „черна кутия“. Този модел описва взаимодействията на УСЛУГАТА с Подателя и

Получателите (Фиг. 1).



Фиг. 1. Логически модел на УСЛУГАТА

Съгласно Закона за електронния документ и електронните удостоверителни услуги, моментът на изпращане е този момент, в който изпратеното съдържание не е под контрола на подателя. Момент на получаване на изпратеното съдържание е моментът, в който изпратеното от подателя съдържание успешно постъпи в информационната система на получателя и УСЛУГАТА позволява е-пратката да е достъпна за получаване от получателя.

При използване на мобилно приложение изпратеното съдържание се счита получено при постъпването на изпратеното електронно съдържание в мобилното приложение на получателя.

При използване на API изпратеното електронно съдържание се счита получено при постъпването му в информационната система на получателя през интерфейс или при постъпването му в мобилното приложение на получателя.

При използване на уеб портал изпратеното електронно съдържание се счита получено при постъпването му в мобилното приложение на получателя.

Всяко получено електронно съдържание се счита за надлежно връчено на получателя без необходимост от потвърждаване на получаването.

Съгласно представения логически модел УСЛУГАТА изпълнява процеса на е-доставка:

1. Подателят извършва първоначална идентификация или последваща автентикация пред УСЛУГАТА.

2. Подателят подготвя потребителско съдържание към един (или повече) Получател(и) и го изпраща на УСЛУГАТА. Подателят задава предварително за какъв период от време системата прави опити за доставяне на потребителското съдържание. Ако не се избере опция, то по подразбиране този срок е 7 дни.

3. УСЛУГАТА изпраща известие до Получателя за изпратено/доставяно потребителско съдържание по специфичен за нея начин, който гарантира поверителност.

4. Потребителското съдържание се предава на Получателя, т.е. преминава границата на (системата на) УСЛУГАТА по специфичен за УСЛУГАТА начин, който гарантира поверителност.

Целостта на потребителското съдържание и свързаните метаданни са защитени при предаване, особено когато се обменят с подателя/получателя или между разпределени компоненти на системата ERDS, и при съхранение. Потребителското съдържание е защитено чрез квалифициран електронен печат и изключва възможността данните да бъдат променени.

6 ИДЕНТИФИКАЦИЯ НА ИЗПРАЩАЧ/ПОЛУЧАТЕЛ

„БОРИКА“ АД извършва автоматизирана първоначална идентификация на изпращач/получател по един от следните начини:

- При използване на API – първоначалната идентификация се извършва чрез използването на мобилното приложение B-Trust Mobile.
- При използване на мобилно приложение – първоначалната идентификация се извършва чрез способите на отдалечената идентификация, внедрени в мобилното приложение.
- При използване на уеб портал – първоначалната идентификация се извършва чрез използването на мобилното приложение B-Trust Mobile, през което се автентифицират за достъп с уеб портала, чрез който се подават документите за изпращане и има възможност за получаване.

По време на автоматичния процес по отдалечена идентификация се извършва проверка на валидността на документа за самоличност чрез национална база данни с документи за самоличност и проверка по liveness detection (откриване на жизненост). Всяка успешна автоматизирана идентификация подлежи на незабавен последващ човешки контрол.

При определен процент несъответствие между Selfie и снимката от документа за самоличност на клиента се предлага възможността да инициира видеоконферентен разговор с оператор. По време на тази интерактивна сесия се установява пряка комуникация с клиента, който трябва да отговори на определени въпроси и да извърши определени действия. Видеоидентификационният процес се ръководи от специално обучени квалифицирани служители на „БОРИКА“ АД.

Всички събития, свързани с първоначалната проверка на самоличността на подателя/ получателя и по-нататъшното удостоверяване, се регистрират и съхраняват.

7 АВТЕНТИКАЦИЯ

При необходимост от повторна заявка на услугата не се извършва първоначална идентификация, а се проверява само актуалността на данните за самоличност. Потребителят може да използва QERDS след автентикация чрез мобилното приложение и/или когато това

може да бъде изпълнено с удостоверение за квалифициран електронен подпис, издадено от „БОРИКА“ АД.

8 СЪЗДАВАНЕ НА ДОКАЗАТЕЛСТВА

ERDS предоставя доказателства за събития, които се случват по време на прехвърлянето на данни между страните (напр. доказателство, че данните са били доставени на получателя). Това доказателство може да се използва за доказване на трети страни, ако е необходимо и в съдебно производство, че транзакцията е извършена по времето и между страните, както е посочено в доказателството. ERDS доказателство може да бъде два вида: незабавно доставено на подателя/получателя или на съхранение в хранилище за определен период от време. „БОРИКА“ АД съхранява доказателствата в защитена среда за срок от 10 години;

В доказателствата е посочена точна дата и час на изпращане, получаване и връчване на потребителското съдържание, обозначени с квалифициран електронен времеви печат. Доказателствата, свързани с действията по доставката на потребителското съдържание, са защитени с електронен печат и съответно е изключена възможността данните да се променят. Доказателствата се предоставят на подателя и получателя като отделен електронен документ в строго определен формат (четим PDF формат и XML машинно четим формат).

8.1 Доказателства, свързани с подателя

След успешно идентифициране и последващо автентифициране на подателя и взаимодействие с Услугата се създават доказателства за изпращане, които могат да се предоставят и на трета страна. В доказателствата е посочена точна дата и час на изпращане на потребителското съдържание от изпращача подпечатани с времеви печат.

1. **Успешно изпращане (SubmissionAcceptance)**

Подателят успешно предава потребителското съдържание към системата на подателя. Генерира се доказателство с вписани дата и час, че подателят е подал в системата пратка, която е била приета и ще се предприемат действия, за да бъде доставена към съответния получател(и).

2. **Отхвърлено изпращане (SubmissionRejection**)

Подателят предава потребителското съдържание към системата на подателя. Потребителското съдържание не е било прието от системата на подателя. Генерира се доказателство с вписани дата и час, че подателят е подал в системата пратка, която системата е отказала да достави.

8.2 Доказателства, свързани с получателя

След успешно идентифициране и последващо автентифициране на получателя и взаимодействие с Услугата се създава доказателство за получаване, което може да се предоставя и на трета страна. В доказателствата е посочена точна дата и час на получаване на потребителското съдържание.

1. **Успешна доставка на съдържание (ContentConsignment)**

Потребителското съдържание е предоставено на получателя. Пратката е била предоставена на получателя в рамките на предварително указаното време, след като получателят е бил първоначално идентифициран и правилно автентифициран.

2. **Невъзможна доставка на съдържание (ContentConsignmentFailure)**

Потребителското съдържание не е доставено в рамките на предварително указаното време, поради технически грешки и/или поради други причини.

8.3 Връчване на съдържание

1. **Връчване на съдържание (ContentHandover)**

Потребителското съдържание е връчено в точно определена дата и час на получателя.

2. **Невъзможно връчване на съдържание (ContentHandoverFailure)**

Потребителското съдържание не е връчено на получателя след определен брой опити или определено време на изчакване.

9 АРХИВИРАНЕ

„БОРИКА“ АД архивира най-малко следната информация:

Архивират се всички документи и данни, свързани с процеса на проверка на самоличността, всички искания, подадени от клиентите, цялата кореспонденция между клиентите и „БОРИКА“ АД, доказателства за изпращането, получаването и подписването на документи.

Дългосрочното съхраняване на данни се прави в сигурна и защитена среда.

10 ПРЕКРАТЯВАНЕ НА УСЛУГАТА

Услугата може да бъде прекратена чрез закриване на профил в мобилното приложение B-Trust Mobile. Прекратяването се извършва незабавно.

11 ЗАДЪЛЖЕНИЯ НА ПОТРЕБИТЕЛИТЕ

Потребителите имат задължението да спазват Договора и Общите условия към него, Политиките и Практиките при използване на Услугата, както и да използват Услугата само за законни цели.

12 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.

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

Физическата сигурност е съобразена с добри практики на международни стандарти и препоръки. Оборудването е защитено в изолирани помещения и е осигурена физическа неприкосновеност.

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.

12.1 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.

12.2 Операционна сигурност

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

12.3 Мрежова сигурност

Доставчикът използва съвременни технически средства за обмен и защита на информация на РО 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.

12.4 Информационна сигурност

Информационната сигурност на компонентите на B-Trust инфраструктурата, 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.

13 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.

14 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.
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.
В случай на компрометиране на услугите, „БОРИКА“ АД уведомява за това всички свои клиенти, които имат установени отношения за предоставяне на ERDS. Информацията, която „БОРИКА“ АД предоставя, показва, че доказателствата, издадени чрез компрометирания ключ, може да не са вече валидни от времето на компрометирането.

15 ПРОВЕРКА И КОНТРОЛ НА ДЕЙНОСТТА НА ДОСТАВЧИКА

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

16 ДРУГИ БИЗНЕС УСЛОВИЯ И ПРАВНИ АСПЕКТИ

Доставчикът гарантира, че РО изпълнява своите функции и задължения в пълно съответствие с условията в този документ, както и издадените вътрешни оперативни инструкции.
Потребителят трябва да спазва точно условията и процедурите на „онбординг“ процеса съгласно този документ.

Спорове или жалби относно използване на QERDS се решават въз основа на писмено подадена информация. В случай че не се намери решение на спора, страните могат да предадат решаването на спора от българския съд. За всички въпроси, неуредени в настоящия документ, се прилагат разпоредбите на българското законодателство.