ISO 9001:2015 ISO 27001:2022
ISO 20000-1:2018 ISO 22301:2019
Regulation (EU) 910/2014
Regulation (EU) 2016/679

ПОЛИТИКА И ПРАКТИКА

ПРИ ОБЕЗБЕДУВАЊЕ НА УСЛУГАТА ЗА ЕЛЕКТРОНСКА ИДЕНТИФИКАЦИЈА

Верзија: 2.0

ЗА ЈАВНА УПОТРЕБА

СОДРЖИНА

1. ВОВЕД 4
1.1. ПРЕГЛЕД 4
1.2. УСОГЛАСЕНОСТ 5
1.3. УСОГЛАСЕНОСТ СО ПОДЗАКОНСКИТЕ АКТИ....5
1.4. УЧЕСНИЦИ ВО ИНФРАСТРУКТУРАТА 6
1.4.1. ОРГАН ЗА СЕРТИФИКАЦИЈА....6
1.4.2. КОРИСНИЦИ....6
1.4.3. ЗАСЕГНАТИ СТРАНИ....6
1.4.4. ДРУГИ УЧЕСНИЦИ 7
1.5. ПРИМЕНЛИВОСТ И УПОТРЕБА НА УСЛУГАТА ЕЛЕКТРОНСКА ИДЕНТИФИКАЦИЈА ..7
1.5.1. ПРИМЕНЛИВОСТ НА УСЛУГАТА....7
1.5.2. КОРИСТЕЊЕ НА УСЛУГАТА ЗА ЕЛЕКТРОНСКА ИДЕНТИФИКАЦИЈА 7
1.5.3. КОРИСТЕЊЕ НА СЕРТИФИКАТ ЗА КВАЛИФИКУВАН АТРИБУТ ОД СТРАНА НА ЗАСЕГНАТИТЕ СТРАНИ 8
1.5.4. ЗАБРАНА ЗА КОРИСТЕЊЕ НА УСЛУГА ЗА ЕЛЕКТРОНСКА ИДЕНТИФИКАЦИЈА 8
1.6. УПРАВУВАЊЕ СО ПОЛИТИКАТА И ПРАКСАТА 8
2. ДЕФИНИЦИИ....9
3. ЈАВЕН РЕГИСТАР 9
4. ОПЕРАТИВНИ АКТИВНОСТИ ПРИ ОБЕЗБЕДУВАЊЕ НА УСЛУГА ЗА ЕЛЕКТРОНСКА ИДЕНТИФИКАЦИЈА....10
4.1. СРЕДСТВАТА ЗА ЕЛЕКТРОНСКА ИДЕНТИФИКАЦИЈА....10
4.1.1. ИНТЕРОПЕРАБИЛНОСТ 10
4.2. ШЕМА НА ПРОЦЕС ЗА АВТЕНТИКАЦИЈА НА ЕЛЕКТРОНСКИОТ ИДЕНТИТЕТ....12
4.2.1. EID-ШЕМА ПРЕКУ МОБИЛНАТА АПЛИКАЦИЈА *EVROTRUST*....12
4.2.2. ШЕМА ЗА EID ПРЕКУ ВЕБ-ИНТЕРФЕЈС 14
4.3. РАСКИНУВАЊЕ НА ДОГОВОРОТ СО EVROTRUST....15
4.4. ИДЕНТИФИКАЦИЈА И ПРОВЕРКА НА ИДЕНТИТЕТОТ ПО ЗАТВОРАЊЕ НА ПРОФИЛОТ 15
5. КОНТРОЛА НА ФИЗИЧКА БЕЗБЕДНОСТ....16
5.1. ПРОСТОРИИ И ИЗГРАДБА НА ПРОСТОРИИТЕ....16
5.2. ФИЗИЧКИ ПРИСТАП 16
5.3. СКЛАДИРАЊЕ НА НОСИТЕЛИ НА ПОДАТОЦИ....16
5.4. ОТСТРАНУВАЊЕ НА ОТПАД....16
6. ОРГАНИЗАЦИСКА КОНТРОЛА И ЧОВЕЧКИ РЕСУРСИ 17
7. ЕВИДЕНЦИЈА НА НАСТАНИ И ВОДЕЊЕ НА ДНЕВНИЦИ 18
8. АРХИВИРАЊЕ 19
9. БЕЗБЕДНОСТ НА АКТИВНОСТА....19
9.1. ПОЛИТИКА ЗА БЕЗБЕДНОСТ НА ИНФОРМАЦИИ....20
9.2. МРЕЖНА БЕЗБЕДНОСТ 21
10. РАНЛИВОСТ И ПРОЦЕНКА....21
10.1. ПРОЦЕНКА НА РИЗИК....21
10.2. УПРАВУВАЊЕ СО ИНЦИДЕНТИ 22
11. ПРЕСТАНОК НА ДЕЈНОСТА НА EVROTRUST 23
11.1. ПРЕСТАНОК НА ДЕЛОВНИ АКТИВНОСТИ....23
11.2. ПРЕНОС НА АКТИВНОСТ НА ДРУГ ДАВАТЕЛ НА ШЕМИ ЗА ЕЛЕКТРОНСКА ИДЕНТИФИКАЦИЈА....23
11.3. ПОВЛЕКУВАЊЕ НА СТАТУСОТ НА EVROTRUST КАКО РЕГИСТРИРАН ДАВАТЕЛ НА ШЕМАТА ЗА ЕЛЕКТРОНСКА ИДЕНТИФИКАЦИЈА 24
12. БЕЗБЕДНОСТ НА ИТ СИСТЕМИТЕ 24
12.1. БЕЗБЕДНОСТ НА ЖИВОТНИОТ ЦИКЛУС НА ТЕХНОЛОШКИОТ СИСТЕМ 25
13. МРЕЖНА БЕЗБЕДНОСТ 25
14. ТЕХНИЧКИТЕ И БЕЗБЕДНОСНИТЕ КАРАКТЕРИСТИКИ НА СРЕДСТВАТА ЗА ЕЛЕКТРОНСКА ИДЕНТИФИКАЦИЈА 25
14.1. EID ПРЕКУ МОБИЛНАТА АПЛИКАЦИЈА EVROTRUST 25
14.2. EID ПРЕКУ ВЕБ ИНТЕРФЕЈС 26

15. ВЕРИФИКАЦИЈА И КОНТРОЛА НА АКТИВНОСТИТЕ НА EVROTRUST 27
15.1. ВНАТРЕШНИ РЕВИЗИИ.....27
15.2. НЕЗАВИСНА НАДВОРЕШНА РЕВИЗИЈА 27
15.3. РЕВИЗИЈА ОД СТРАНА НА НАЦИОНАЛЕН НАДЗОРЕН ОРГАН.....27
16. ФИНАНСИСКИ ОБВРСКИ 27
17. ДЕЛОВНО ОСИГУРУВАЊЕ 27
18. ПРИВАТНОСТ НА ЛИЧНИТЕ ПОДАТОЦИ 28
18.1. ПРАВА НА ИНТЕЛЕКТУАЛНА СОПСТВЕНОСТ.....28
19. ОБВРСКИ, ОДГОВОРНОСТ И ГАРАНЦИИ НА EVROTRUST 28
19.1. ГАРАНЦИИ И ОБВРСКИ 28
19.2. ОДГОВОРНОСТИ 30
20. ОБВРСКИ НА КЛИЕНТИТЕ 30
21. ОДГОВОРНОСТ НА КЛИЕНТИТЕ.....30
22. ОДРЕКУВАЊЕ 31
23. РЕШАВАЊЕ НА СПОРОВИ 31
24. ВАЖЕЧКИ ЗАКОН 31

1. ВОВЕД

Евротруст Технолоџис дооел Скопје (*Evrotrust*) е правно лице регистрирано во Централниот регистар на Република Северна Македонија со следните податоци:

- адреса: ул. Венијамин Мачуковски бр. 1/2-31; Скопје
- ЕМБС 7435800
- ЕДБ 4080020591119
- *E-mail* адреса: office@evrotrust.mk

Evrotrust е компанија која ја обезбедува услугата за Шема за Електронска Идентификација (*eID*) со висок степен на безбедност на територијата на Република Северна Македонија под трговската марка „ *Evrotrust*“.

Evrotrust на своите клиенти им ја нуди услугата Електронска Идентификација (*eID*) преку мобилната апликација *Evrotrust*, која се ослонува на квалификувани услуги за автентикација. Услугата обезбедува брзо, лесно, сигурно и безбедно креирање на профил на корисниците, како и безбедна автентикација на личните податоци кон доверливи страни. Предностите на услугата вклучуваат и исклучително лесна и брза идентификација во секое време и на секое место. Користењето на услугата за Електронска Идентификација е целосно усогласена со Македонското законодавство, поточно со Законот за Електронски Документи, Електронска Идентификација и Доверливи Услуги како и со Европската Регулатива (ЕУ) бр. 910/2014. Пристапот до услугата е овозможен за сите лица кои имаат важечки документ за лична идентификација.

Услугата ги задоволува потребите за идентификација преку услуга за автентикација во смисла на чл. 13, ст. 1, b."a" од Директивата (ЕУ) 2018/843 на Европскиот парламент и на Советот од 30 мај 2018 година за изменување и дополнување на Директивата (ЕУ) 2015/849 за да се спречи употребата на финансискиот систем за целите на перење пари и финансирање на тероризам и да ги измени директивите 2009/138/ЕЗ и 2013/36/ЕУ.

1.1. ПРЕГЛЕД

„Политика и практика за обезбедување на услуга за електронска идентификација“ (Политиката) е документ кој ги опишува општите правила и норми што ги применува *Evrotrust* при проверка на личните податоци на физичките лица и, доколку е потребно, сите специфични атрибути поврзани со лицата и издавање сертификати кои ги содржат овие податоци. Во овој документ се опишани општите барања за обезбедување на услугата за електронска идентификација и безбедносните мерки, права и обврски за сите учесници во инфраструктурата со јавни клучеви на *Evrotrust*, вклучувајќи ги органите за сертификација, корпоративните клиенти, крајните клиенти и засегнатите страни. Кога се обезбедува преку мобилна апликација на *Evrotrust*, услугата обезбедува сигурно и сигурно креирање на изјава за давање лични или други податоци, издавање на квалификуван атрибутивен сертификат за квалификуван електронски потпис, со кој изјавата се потпишува со личен или друг податоци,

далечинско потпишување на изјавата со квалификуван електронски потпис придружен со атрибутивниот квалификуван сертификат и давање на потпишаната изјава на трети лица. Кога се обезбедува преку веб-интерфејс, услугата обезбедува генерирање на датотека што содржи лични податоци на поединци и нивно обезбедување во машински читлива форма според одреден технолошки стандард за засегнатата страна.

Овој документ е составен дел од Општите услови на договорот за обезбедување на услуга за електронска идентификација. Овој документ е креиран во целосна согласност со Регулативата (ЕУ) бр. 910/2014, Регулативата (ЕУ) 2016/679 (GDPR) и важечкото законодавство во Република Северна Македонија. Политиката е јавен документ и може да се промени во секое време од страна на Evrotrust. Секоја нова ревизија се доставува до заинтересираните страни.

1.2. УСОГЛАСЕНОСТ

Evrotrust обезбедува услуга за електронска идентификација во согласност со следните документи:

- Регулатива (ЕУ) бр. 910/2014 на Европскиот парламент и на Советот од 23 јули 2014 година за услуги за електронска идентификација и автентикација за електронски трансакции на внатрешниот пазар и за укинување на Директивата 1999/93/ЕЗ (Регулатива (ЕУ) бр. 910 /2014) и со важечката легислатива во Република Бугарија;
- Регулатива (ЕУ) 2016/679 на Европскиот парламент и на Советот од 27 април 2016 година за заштита на поединци во однос на обработката на личните податоци и за слободно движење на тие податоци и укинување на Директивата 95/46/ЕЗ (Општо Регулатива за заштита на податоците);
- ETSI EN 319 401 Електронски потписи и инфраструктура (ESI); Општи барања за политики за доверливи даватели на услуги;
- ETSI EN 319 411-1 Општи барања;
- TS 119 612 Доверливи листи.
- чл. 13, ст. 1, b."a" од Директивата (ЕУ) 2018/843 на Европскиот парламент и на Советот од 30 мај 2018 година за изменување и дополнување на Директивата (ЕУ) 2015/849 за да се спречи употребата на финансискиот систем за целите на перење пари и финансирање на тероризам и измена на директивите 2009/138/ЕЗ и 2013/36/ЕУ.

1.3. УСОГЛАСЕНОСТ СО ПОДЗАКОНСКИТЕ АКТИ

Evrotrust обезбедува услуга за електронска идентификација во согласност со важечката легислатива.

1.4. УЧЕСНИЦИ ВО ИНФРАСТРУКТУРАТА

1.4.1. ОРГАН ЗА СЕРТИФИКАЦИЈА

Кога е обезбедено преку мобилната апликација Evrotrust, органот за сертификација на EvrotrustБугарија ги исполнува следните специфични обврски според задачата на Evrotrust Македонија:

- Прифаќање на електронско барање за издавање на квалификувани сертификати за атрибуција;
- Издавање на сертификат за квалификуван атрибут;
- Објавување и одржување на издадени квалификувани сертификати за атрибуција;
- Далечинско потпишување со квалификуван електронски потпис;
- Чување на записите (дневниците) на процесот на електронска идентификација, издавање сертификати за квалификувани атрибути и далечинско потпишување со квалификуван електронски потпис.

Кога се обезбедува преку веб-интерфејс, органот за сертификација на Evrotrust Бугарија ги извршува следните должности во име на Evrotrust Македонија:

- Прифаќање на електронско барање за идентификација;
- Идентификација преку вградената функционалност преку веб-интерфејс;
- Чување на евиденцијата (дневниците) на процесот на електронска идентификација.

1.4.2. КОРИСНИЦИ

Корисник на оваа услуга е секое физичко лице кое има договор со Evrotrust за услуга за електронска идентификација. Онаму каде што е изводливо, доставениот сертификат треба да биде достапен за лицата со попреченост.

1.4.3. ЗАСЕГНАТИ СТРАНИ

За да се обезбеди услуга за електронска идентификација, засегнати страни се корпоративни клиенти како што се банки, осигурителни компании, владини организации, телекомуникациски оператори итн., кои имаат договор со Evrotrust за интеграција и кои и веруваат на услугата за автентикација за потребите на воспоставување комерцијални односи, професионални, административни и други односи или извршување на различни операции или трансакции. Засегнатите страни треба да имаат знаење и вештини во врска со употребата на сертификатите за квалификуван атрибут и да им веруваат на околностите заверени во нив само во поглед на важечката Политика, особено во однос на нивото на безбедност при проверката на идентитетот на лицата на кои им се издаваат квалификуваните сертификати атрибутивни сертификати, како и во однос на ограничувањата за нивната употреба внесени во сертификатите. Evrotrust им дава можност на доверливите страни за сигурна, сигурна, лесна и удобна квалификувана валидација на автоматизиран начин на квалификувани електронски потписи за кои се издадени атрибутивните сертификати.

1.4.4. ДРУГИ УЧЕСНИЦИ

Шемата за електронска идентификација се заснова на автентикација во согласност со eIDAS и услуги за eID обезбедени од „Evrotrust Technologies“ АД Бугарија. „Evrotrust технолоџис“ АД Бугарија има регистрирано услуга за електронска идентификација во Доверливата листа на Комисијата на ЕУ, поради што е призната од македонскиот закон според чл. 20 (2) од Законот за eIDAS. Услугата за електронска идентификација преку мобилната апликација на Evrotrust се заснова на средства за електронска идентификација - квалификуван атрибутивен сертификат за електронски потписи - квалификувана услуга за сертификација, исто така признаена со македонскиот закон според чл. 37 (2) од Законот за eIDAS - https://webgate.ec.europa.eu/tl-browser/#/tl/BG/6. Услугата за електронска идентификација преку веб-интерфејс се заснова на средства за електронска идентификација - стандардизиран документ во машински читлива форма, признат со македонскиот закон според чл. 37 (2) од Законот за eIDAS - https://eidas.ec.europa.eu/efda/tl-browser/#/screen/tl/BG/7/17. „Evrotrust Технолоџис“ ДОО е оператор на шемата за електронска идентификација и е регистрирана во Доверливата листа во Министерството за информатичко општество и администрација на Република Северна Македонија, но го довери создавањето на средствата за електронска идентификација и работењето на услугата кон „Evrotrust Технолоџис“ АД Бугарија .

1.5. ПРИМЕНЛИВОСТ И УПОТРЕБА НА УСЛУГАТА ЕЛЕКТРОНСКА ИДЕНТИФИКАЦИЈА

1.5.1. ПРИМЕНЛИВОСТ НА УСЛУГАТА

Применливоста на услугата за електронска идентификација е поврзана со автентикација на лични и други податоци на физички и правни лица од страна на Evrotrust, кои податоци се вклучени во:

1. издадените квалификувани сертификати за атрибуција, како и во изјавите на клиентите за обезбедување на лични и други податоци на барање на засегната страна, соодветно во

2. креираните стандардизирани документи во машински читлива форма, испратени до засегнатата страна на барање на клиентите.

Evrotrust спроведува соодветни технички и организациски мерки при давањето на услугата со цел да се избегнат можните прекршувања на безбедноста на податоците. Личните и другите податоци се обработуваат на начин што обезбедува високо ниво на безбедност на овие податоци, вклучително и заштита од неовластена или незаконска обработка и од случајно губење, уништување или оштетување, со примена на соодветни технички и организациски мерки.

1.5.2. КОРИСТЕЊЕ НА УСЛУГАТА ЗА ЕЛЕКТРОНСКА ИДЕНТИФИКАЦИЈА

Со услугата за електронска идентификација преку мобилна апликација на Evrotrust,

корисниците можат еднаш да ги користат автентицираните податоци во квалификуваните сертификати за атрибути за да потпишат изјава за давање лични податоци, со која се идентификуваат и дадат согласност за давање податоци. Откако ќе се регистрираат во мобилната апликација Evrotrust, поединците можат да користат и да се идентификуваат електронски неограничен број пати, но за секоја автентикација се користи еднократно генериран нов приватен клуч со нов квалификуван сертификат за атрибут. Времетраење на сертификатот за квалификуван атрибут и поврзаниот приватен клуч е 2 (два) часа.

Со услугата за електронска идентификација со веб-интерфејс, клиентите можат да ги користат автентицираните податоци во стандардизираниот документ во машински читлив формат само еднаш кога ќе се идентификуваат и ќе ја користат услугата. Регистрацијата на корисникот не е креирана во апликацијата Evrotrust. Доколку се сака да се генерира ново средство за електронска идентификација, корисниците мора повторно да поминат низ процесот на идентификација.

1.5.3. КОРИСТЕЊЕ НА СЕРТИФИКАТ ЗА КВАЛИФИКУВАН АТРИБУТ ОД СТРАНА НА ЗАСЕГНАТИТЕ СТРАНИ

Со услугата за електронска идентификација преку мобилната апликација на Evrotrust, засегнатите страни мора да ги користат податоците на лицата заверени во атрибутивните сертификати и декларирани од клиентите само по проверка на нивниот статус и проверка на електронскиот потпис на органот за сертификација кој го издал сертификатот. Со услугата за електронска идентификација на веб-интерфејс, засегнатите страни мора да му веруваат на стандардизираниот документ за лични податоци во машински читлива форма само ако е примен преку воспоставено API поврзување со Evrotrust. Evrotrust не е одговорен доколку засегнатата страна не ги исполнува наведените барања, нема право да ги обработува личните податоци на клиентот или ги обработува спротивно на важечката легислатива.

1.5.4. ЗАБРАНА ЗА КОРИСТЕЊЕ НА УСЛУГА ЗА ЕЛЕКТРОНСКА ИДЕНТИФИКАЦИЈА

Услугата за електронска идентификација не смее да се користи на начин што може да доведе до прекршување на доверливоста, интегритетот и безбедноста на податоците.

1.6. УПРАВУВАЊЕ СО ПОЛИТИКАТА И ПРАКСАТА

Раководството на Evrotrust е одговорно за управувањето со овој документ.

Секоја верзија на Политиката е ефективна додека не се одобри нова верзија. Секоја нова верзија е развиена од овластени компетентни вработени во Evrotrust и, по одобрување од раководството на Evrotrust, се става на располагање на заинтересираните страни. Клиентите и засегнатите страни се обврзани да се усогласат само со важечката верзија на Политиката во моментот на користење на услугата.

Лице за контакт за управување со документот „Политика и пракса при обезбедување на услуга за електронска идентификација“ е извршниот директор на Evrotrust.

Дополнителни информации може да се добијат на следната адреса:

Evrotrust Технолоџис дооел Скопје

- адреса: ул. Венијамин Мачуковски бр. 1/2-31; Скопје
- ЕМБС 7435800
- ЕДБ 4080020591119
- *E-mail* адреса: nm@evrotrust.com

2. ДЕФИНИЦИИ

Терминоте употребени во овој документ се дефинирани во Регулативата (ЕУ) бр. 910/2014., вклучувајќи:

„Лични податоци за идентификација“ е збир на податоци што овозможува да се утврди идентитетот на физичко или физичко лице кое претставува правно лице;

„Автентикација“ е електронски процес кој овозможува електронска идентификација на физичко лице или потврда за потеклото и интегритетот на податоците во електронска форма;

„Засегната Страна“ е поединец кој се потпира на услугата за автентикација за електронска идентификација;

„Потврда за електронски потпис“ е електронски документ кој ги поврзува податоците за валидација на електронски потпис со физичко лице и го потврдува барем името или псевдонимот на тоа лице;

„Квалификуван сертификат за електронски потпис“ е сертификат за електронски потпис кој е издаден од давател на квалификувани услуги за автентикација и ги исполнува условите предвидени во Регулативата (ЕУ) бр. 910/2014.

3. ЈАВЕН РЕГИСТАР

Регистарот на Evrotrust е складиште во кое се наоѓаат тековните и претходните верзии на електронски документи (Политики и практики, сертификати на тела за сертификација и други информации) наменети за клиенти и заинтересирани страни. Регистарот е управуван и контролиран од Evrotrust. Пристапот до информации е постојан (24/7/365). Регистарот е достапен преку Интернет: https://www.evrotrust.com и преносот се одвива преку протоколот HTTP/HTTPS. Evrotrust презеде мерки, логични и физички механизми за заштита од неовластено додавање, отстранување и менување на информациите објавени во складиштето. По откривање на прекршоци, Evrotrust презема соодветни активности за да го врати интегритетот на информациите. Доколку е потребно, Evrotrust наметнува правни санкции, ги известува засегнатите субјекти и ги надоместува нивните загуби.

4. ОПЕРАТИВНИ АКТИВНОСТИ ПРИ ОБЕЗБЕДУВАЊЕ НА УСЛУГА ЗА ЕЛЕКТРОНСКА ИДЕНТИФИКАЦИЈА

4.1. СРЕДСТВАТА ЗА ЕЛЕКТРОНСКА ИДЕНТИФИКАЦИЈА

Средството за електронска идентификација според шемата за електронска идентификација на Evrotrust е нематеријален субјект кој ги содржи податоците за идентификација на лицето. Во случај на идентификација преку мобилната апликација Evrotrust, таа се состои од PDF + XML документ кој ги содржи личните податоци за идентитетот на лицето, вклучувајќи графички елементи како што се копија од лична карта, слика со потпис, фотографија итн.; атрибути на квалификуван потпис на потпишаниот PDF/XML документ и сертификат за квалификуван атрибут кој го поддржува квалификуваниот потпис кој ги содржи сите лични податоци кои можат да бидат вклучени во сертификатот според стандардот X.509. Ова средство (токен) се генерира на барање на крајниот корисник во реално време, вклучувајќи го и генерирањето на пар клучеви и поврзаниот сертификат за квалификуван атрибут. Средството автоматски се доставува до засегнатата страна што ја потврдува автентичноста за онлајн услугата. Засегнатата страна може да ги извлече информациите и од PDF/XML документот и од сертификатот за квалификуван атрибут. Квалификуваниот атрибутивен сертификат за квалификуван електронски потпис се издава под истите услови како и стандардниот квалификуван сертификат за електронски потпис, но се разликува по видот и обемот на податоците заверени во него. Дополнителните специфични податоци не влијаат на интероперабилноста и препознавањето на квалификувани електронски потписи, се додека внесените податоци се во согласност со важечките стандарди. Применливоста на квалификуваниот атрибутивен сертификат е поврзана со идентификацијата на лицата на засегнатите страни. Правната вредност на сертификатот за квалификуван атрибут како квалификуван сертификат за квалификуван електронски потпис е призната низ Европската унија. Можноста за автентичност на личните податоци со издавање квалификувани сертификати за атрибуција за квалификувани електронски потписи е регулирана со Преамбулата (54) во врска со чл. 24 (1) и чл. 28, точка 3 од Регулативата (ЕУ) бр. 910/2014 од податоците за идентитетот на корисникот, според eIDAS.

Во случај на идентификација преку веб-интерфејс, средството за електронска идентификација се состои од стандардизиран документ во структуриран формат, кој секогаш содржи ист обем на лични податоци за секој корисник. Податоците се преземени од страна на засегнатата страна од е-идентификацискиот капацитет обезбеден преку API.

4.1.1. ИНТЕРОПЕРАБИЛНОСТ

Evrotrust гарантира високо ниво на безбедност и интероперабилност на електронската идентификација што ја обезбедува. Evrotrust презеде технички и организациски мерки при издавање средства за електронска идентификација за да обезбеди интероперабилност на шемите за електронска идентификација во согласност со националните и меѓународните

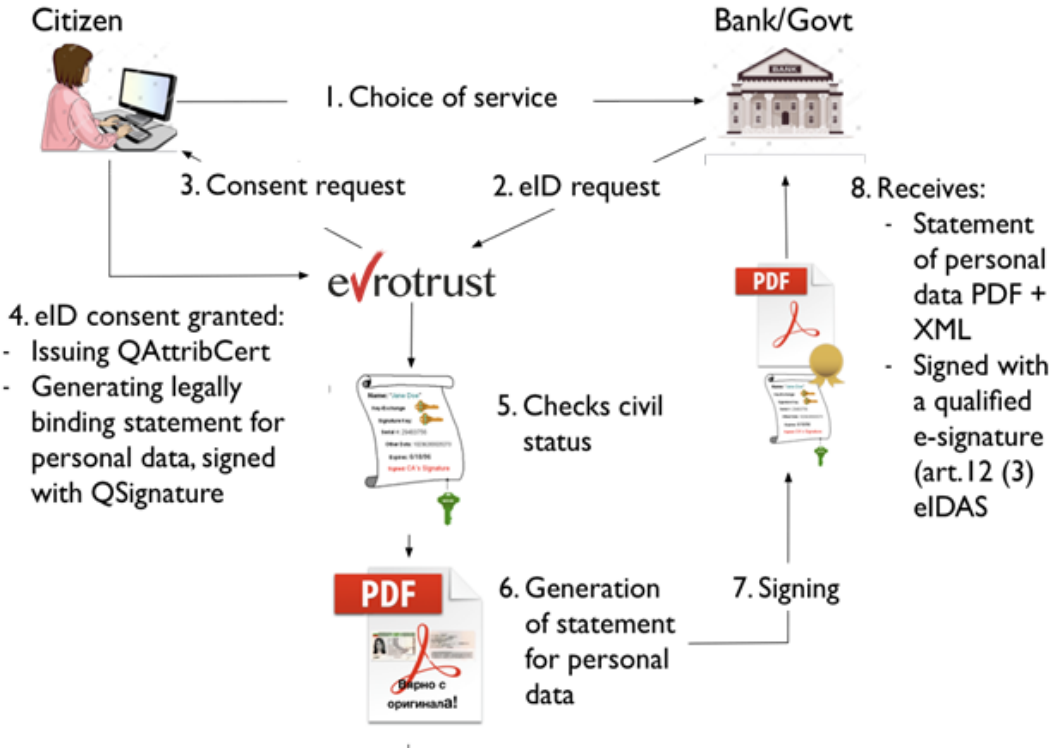
стандарди во оваа област.

Evrotrust имплементира стандардизирани безбедносни процедури за управување и користи доверливи системи и производи, вклучително и безбедни електронски комуникациски канали, со цел да се обезбеди сигурност на околината за обезбедување услуги за автентикација и електронска идентификација. Инфраструктурата на Evrotrust е физички и логички одвоена и не се користи за други активности што ги врши Evrotrust. Преземените мерки во однос на физичката заштита се елемент на развиениот и имплементиран Информатички безбедносен систем, кој одговара на барањата на стандардот ISO/IEC 27001 Evrotrust обезбедува физичка заштита и контрола на пристапот на просториите каде што се инсталирани критичните компоненти во неговата инфраструктура . Evrotrust обезбедува високо ниво на заштита на своите средства, вклучувајќи ги и информациските средства. На персоналот на Evrotrust им се доделуваат доверливи улоги од страна на повисокото раководство врз основа на „најмали привилегии“ кога пристапуваат или конфигурираат привилегии за пристап. Пристапот до системот е ограничен на овластени лица. Контролите (на пр. заштитните ѕидови) ги штитат внатрешните мрежни домени на Evrotrust од неовластен пристап, вклучително и пристап од корисници и трети страни. Системот на Evrotrust обезбедува доволно компјутерски безбедносни контроли. За таа цел се одвоени функциите на безбедносната администрација и управување. Evrotrust користи доверливи системи и производи кои се заштитени од модификации и гарантираат техничка сигурност и доверливост на процесите што ги поддржуваат. Evrotrust врши анализа на безбедносните барања при дизајнирање на нови системи и нови услуги за да се обезбеди нивната безбедност. Применува процедури за контрола на промени на софтверот и конфигурацијата на технолошките системи. Интегритетот на системите и информациите на Evrotrust е заштитен од вируси, малициозен и неовластен софтвер. Средствата што се користат во системите на Evrotrust се безбедно обработени за да се заштитат записите од оштетување, кражба, неовластен пристап и застареност.

Евротруст Технолоџис дооел Скопје поседува валиден ISO/IEC 27001 сертификат, кој ги исполнува техничките барања потребни за сертификација за интероперабилност.

4.2. ШЕМА НА ПРОЦЕС ЗА АВТЕНТИКАЦИЈА НА ЕЛЕКТРОНСКИОТ ИДЕНТИТЕТ

4.2.1. eID-ШЕМА ПРЕКУ МОБИЛНАТА АПЛИКАЦИЈА *EVROTRUST*



Evrotrust го проверува идентитетот на лице со користење на систем за далечинско идентификација на физички и правни лица. Оперативните активности во обезбедувањето на услуга за електронска идентификација вклучуваат издавање на атрибутивен сертификат за електронски потпис и генерирање изјава за обезбедување на лични и други податоци, потпишана со издадениот сертификат и доставен до засегната страна на барање. на клиент на Evrotrust. Evrotrust гарантира дека информациите содржани во сертификатите за атрибуција се точни и веродостојни во моментот на нивното издавање. Барањето за далечинско користење на услуга за сертификати за електронска идентификација се врши на барање на клиент на Evrotrust заради воспоставување, измена или раскинување на неговите правни односи со доверителот - клиент на услугата на Evrotrust (на пр. банка, осигурување компанија и сл.) преку посебен развиен комуникациски интерфејс.

Заради проверка на идентитетот, физичкото лице му доверува на Evrotrust издавање квалификуван атрибутивен сертификат за електронски потпис, креирање документ - изјава за обезбедување на лични и други податоци по електронски пат, далечинско потпишување со квалификуван електронски потпис придружен со атрибутивен сертификат и обезбедување на потпишаната изјава со атрибутивниот квалификуван електронски потпис на засегната страна. Процесот на обезбедување на услугата е иницира од страна на доверлива страна која испраќа барање до Evrotrust барајќи идентификација до клиентот преку специјализиран веб-портал, API интерфејс или преку SDK модул. Клиентот му дава инструкции на Evrotrust да му ја генерира изјавата со бараното. Изјавата за приватност е достапна за поединецот во читлив PDF формат преку мобилната апликација Evrotrust или порталот за потпис за поединецот да

ја прегледа пред да ја потпише. Во изјавата се додава и сервисна XML-датотека со истите податоци во машински читлив формат за обработка од страна на засегнатата страна на автоматизиран начин. Во случај лицето да не е клиент на Evrotrust, мора да помине низ процес на регистрација и идентификација со Evrotrust и да стане клиент на Evrotrust. Податоците што засегнатата страна може да ги побара од клиентот на Evrotrust може да бидат (неисцрпно): презиме (или имиња), име (или имиња), датум на раѓање, национален единствен идентификатор, доколку ги има, во согласност со техничките спецификации за целите на прекугранична идентификација, која ќе остане непроменета што е можно подолго, мобилен број и адреса на е-пошта. Дополнителни конкретни податоци кои операторот може да ги собере се: име (или имиња) и презиме (или имиња) при раѓање, место на раѓање, постојана адреса и пол. Evrotrust го задржува правото, во зависност од реализацијата на интеграцијата со различните видови лични документи, примарни регистри и веродостојни извори на податоци, да го дополни конкретниот сет на податоци.

Evrotrust ја потврдува веродостојноста на информациите со сите законски дозволени средства. Проверката на валидноста на документот за идентификација на физичко лице се врши преку национална база на податоци за лични документи (во присуство на релевантна интеграција), доверливи извори на податоци или идентификација на операторот. За да го потврди идентитетот на физичките лица и, доколку е потребно, специфичните атрибути поврзани со лицата, Evrotrust користи далечински систем за видео идентификација. Системот за далечинска идентификација е потврден и потврден од страна на Управата за верификација на усогласеноста дека обезбедува ист степен на безбедност како и личниот изглед врз основа на чл. 24 (1), б. „г“ од Регулативата (ЕУ) 910/2014.

Кога засегната страна поднесува барање од одреден клиент до Evrotrust за идентификација, Evrotrust испраќа порака на мобилната апликација на Evrotrust до клиентот во мобилната апликација барајќи негова согласност за идентификација. На поединецот му се дава можност да се запознае со обемот на лични и други податоци што се потребни од страна на засегнатата страна за да одлучи дали да се идентификува или не. По активирањето на функционалноста со која клиентот сака да се идентификува, Evrotrust подготвува документ за доделување на клиентот - изјава за обезбедување лични податоци, генерира пар криптографски клучеви и издава атрибутивен квалификуван сертификат за јавниот клуч на парот , овозможувајќи му на лицето да ја потпише изјавата за давање на лични и други податоци. Клиентот го внесува својот PIN/биометриски податоци, со што од далечина се активира приватниот клуч, кој се чува на HSM на Evrotrust во безбедна просторија, со што се создава квалификуван електронски потпис на изјавата за обезбедување на лични и други податоци, врз основа на атрибутивниот сертификат. Атрибутивниот сертификат што го издава Evrotrust е еднократен, со краток период на важност и содржи заверен јавен клуч, податоци од документ за идентификација и дополнителни атрибути, надвор од оние потребни за квалификуван сертификат, кои произлегуваат од Регулативата (ЕУ) бр. 910/2014, во

согласност со применливоста на сертификатите и договорните односи со клиентот. Личните податоци се обработуваат на начин што гарантира високо ниво на безбедност, вклучително и заштита од неовластена или незаконска обработка и од случајно губење, уништување или оштетување, со примена на соодветни технички и организациски мерки.

Засегнатата страна ја добива потпишаната PDF/XML датотека со изјавата на клиентот за обезбедување на лични и други податоци, потпишана со атрибутивниот квалификуван сертификат, според интерфејс договорен со Evrotrust.

4.2.2. ШЕМА ЗА eID ПРЕКУ ВЕБ-ИНТЕРФЕЈС

Шемата за електронска идентификација на веб-интерфејс е систем за далечинско идентификација на физички и правни лица преку веб-базирана апликација во целосна согласност со Регулативата (ЕУ) бр. 910/2014. Електронската идентификација е поврзана со собирање, обработка, верификација и автентикација на лични и други податоци на физички лица на барање на доверлива страна.

За да започне процесот на далечинско идентификација, лицето треба да отвори интернет страница во претходно познат и поддржан прелистувач, во кој далечинското решение за електронска идентификација е интегрирано преку веб-интерфејсот на Evrotrust. Evrotrust може да имплементира различни технологии кои ги исполнуваат барањата опишани во оваа политика. За целите на регистрација и последователна идентификација, потребно е лицето да го фотографира својот документ за лична идентификација со камерата на уредот што се користи и податоците добиени од машински читливата област на документот за идентификација и сликата. се обработуваат автоматски, вклучително и проверка за валидност со посебен софтвер. Шемата е развиена на технологија која автоматски ги препознава податоците за идентитетот и ги испраќа на автентикација до доверлив извор (регистар на документи за идентитет), преку вградена комуникациска линија во реално време (ако е

интегрирана). Кога лицето е правно лице, застапничкиот орган и податоците за идентитетот на правното лице се проверуваат од комерцијален регистар или друг применлив регистар, доколку има соодветен пристап. Кога документот за идентификација има вградени податоци во чип на ICAO и уредот поддржува NFC технологија, податоците се извлекуваат од таму со приближување до мобилен уред, доколку таквата функционалност на решението е достапна. Процесот на автоматска идентификација на видеото бара споредба на фотографијата на лицето добиена од личната карта и фотографијата направена од камерата на уредот во режим на снимање видео. Добиениот резултат е генериран од високотехнолошки софтвер кој врши биометриска анализа на обликот и уникатните карактеристики на лицето. Процесот вклучува 3D верификација за жив објект.

За да се утврди идентитетот на физичко лице кое е застапник на правно лице (менаџери, членови на одбори, обвинители и сл.), кога застапничката овластување произлегува од закон, се врши автоматска проверка во соодветните регистри во присуство. на таквата интеграција.

Во случај на неуспешна автоматска видео идентификација (на пример, поради можни промени на лицето, ниска резолуција и слаб квалитет на снимање итн.), процесот се префрла на видео идентификација од страна на операторот на Evrotrust. Операторот за време на видео-конференциски повик со лицето во реално време, визуелно го идентификува лицето и врз основа на компаративна анализа со документот за идентификација и фотографијата извлечена од него, го автентицира лицето и ги потврдува податоците.

Секоја идентификација, без разлика дали е автоматизирана или направена од оператор, може да биде подложена на последователна човечка контрола, во согласност со утврдената методологија. По успешна идентификација на лицето и валидација на собраните податоци за него, датотека со структурирани податоци се обезбедува преку безбеден канал до засегнатата страна, преку интернет конекција, во стандардизиран формат.

4.3. РАСКИНУВАЊЕ НА ДОГОВОРОТ СО EVROTRUST

Договор за обезбедување на услуга за електронска идентификација преку мобилната апликација Evrotrust, достапна преку апликацијата Evrotrust, се раскинува со затворање на профилот на клиент во мобилната апликација Evrotrust. Договорот за давање услуга за електронска идентификација преку веб-интерфејс се раскинува со обезбедување на средствата за електронска идентификација на засегнатата страна, а пред тој момент - во секое време на иницијатива на клиентот, престанок на неговото учество во идентификацијата. процес.

4.4. ИДЕНТИФИКАЦИЈА И ПРОВЕРКА НА ИДЕНТИТЕТОТ ПО ЗАТВОРАЊЕ НА ПРОФИЛОТ

При овозможување на функционалност преку мобилната апликација Evrotrust за бришење

профил и кога некое лице сака да обезбеди услуга за идентификација преку мобилната апликација Evrotrust по одреден временски период, мора да помине низ нов процес на регистрација и идентификација во апликацијата.

5. КОНТРОЛА НА ФИЗИЧКА БЕЗБЕДНОСТ

5.1. ПРОСТОРИИ И ИЗГРАДБА НА ПРОСТОРИИТЕ

Evrotrust има специјално изградена и опремена просторија со највисок степен на физичка контрола на пристап, во која се сместени органот за сертификација на Evrotrust и сите централни компоненти на инфраструктурата.

5.2. ФИЗИЧКИ ПРИСТАП

Физичката безбедност на системите за издавање и управување со сертификати и креирање и управување со електронски идентитет е во согласност со барањата на меѓународните стандарди и препораки. Физичкиот интегритет е обезбеден за опремата во безбедните и изолирани простории на Evrotrust. Има двофакторна контрола на пристап и 24 часовно физичко обезбедување. Пристап до орманот со опремата не е дозволен на помалку од 2 (две) овластени технички лица. Секој пристап до просториите со критична инфраструктура е документиран во посебни дневници. Зградата е заштитена со 24-часовно обезбедување. Просториите на Evrotrust имаат систем за алармна сигнализација, систем за видео надзор, систем за сигнално известување и систем за контрола на пристап.

5.3. СКЛАДИРАЊЕ НА НОСИТЕЛИ НА ПОДАТОЦИ

Сите медиуми што содржат софтвер, архиви на податоци или информации за ревизија се чуваат во огноотпорен сеф во посебни простории за пристап со поставена контрола на пристап. Во просторијата со архивата на Evrotrust е изграден систем на физичка и логичка заштита. Снимањето и складирањето на релевантните информации се врши преку ефективен систем за управување со евиденција, земајќи ги предвид применливите закони и добрата практика во однос на заштитата и задржувањето на податоците. Evrotrust води база на податоци во која се чуваат информации за активноста поврзана со обезбедувањето електронска идентификација. Базата на податоци се одржува диференцирана: База на податоци, системи за Датотеки и Архиви.

5.4. ОТСТРАНУВАЊЕ НА ОТПАД

Електронските медиуми кои содржат значајни информации за безбедноста на Evrotrust се уништуваат по истекот на наведениот период на складирање според внатрешните правила. Медиумите за складирање на криптографските клучеви и шифрите за пристап што се користат за нивно складирање се сечат со соодветни уреди. Ова се однесува на медиуми кои не дозволуваат трајно бришење на зачуваните податоци и нивна повторна употреба. Во

одредени случаи, информациите за отстранлив медиум се уништуваат со бришење или форматирање на уредот без враќање.

6. ОРГАНИЗАЦИСКА КОНТРОЛА И ЧОВЕЧКИ РЕСУРСИ

Сите процедури поврзани со безбедноста при издавањето, администрирањето и користењето на квалификувани сертификати за атрибути и креирањето и управувањето со електронската идентификација се вршат од доверлив персонал на Evrotrust. Evrotrust одржува доволен број квалификувани вработени за да обезбеди усогласеност со постојното законодавство и внатрешните правила и прописи на компанијата во секој момент од нејзината активност.

За управување со човечки ресурси при обезбедување на услугата за електронска идентификација Evrotrust ги применува следниве барања:

- Evrotrust гарантира дека вработените и изведувачите ги почитуваат барањата за доверливост на активноста;
- Evrotrust ангажира вработени и подизведувачи кои ја поседуваат потребната експертиза, доверливост, искуство и квалификации и кои поминале обука за правилата за безбедност и заштита на личните податоци соодветни на дејноста што ја вршат;
- Вработените во Evrotrust периодично (најмалку на секои 12 месеци) поминуваат низ обука за да ја зголемат својата стручност, искуство и квалификации. Обуката вклучува обука за безбедност на информации, потенцијални закани и добри безбедносни практики;
- Вработените кои ги прекршуваат политиките на Evrotrust подлежат на соодветни дисциплински санкции;
- Улогите и одговорностите за безбедноста на информациите се документирани во описот на работните места;
- Evrotrust дефинира доверливи улоги од кои зависи безбедноста на услугата активност за валидација на потпис/печат;
- Раководството на Evrotrust ги дефинира одговорностите на доверените улоги;
- Доверливите улоги се одобрени и прифатени од раководството;
- Вработените во Evrotrust (и привремени и постојани) имаат опис на работните места дефинирани во однос на улогите што ги извршуваат со поделба на должностите и најмалите привилегии, со чувствителност на позицијата одредена врз основа на должностите и нивоата на пристап, квалификација и диплома;
- Описите на работните места ги вклучуваат барањата за вештини и искуство и прават разлика помеѓу општите и посебните должности;
- Вработените спроведуваат административни и менаџерски процедури и процеси кои се дел од процедурите за управување со безбедноста на информациите на Evrotrust;
- Менаџментот има познавање за обезбедените услуги за автентикација, познавање на безбедносни процедури, искуство во областа на безбедноста на информациите и проценка на ризик доволно за извршување на функциите на управување;

- Сите вработени во Evrotrust кои имаат доверливи улоги се ослободени од конфликт на интереси што може да влијае на непристрасноста на активностите на Evrotrust;
- Доверливите улоги ги вклучуваат следните одговорности:
  a) Администратор за безбедност - офицерите за безбедност се одговорни за целокупната одговорност за управување и имплементација на процедурите за безбедност на системите: развиваат безбедносна политика; презема мерки за техничка заштита на податоците и системите; утврдува оперативни безбедносни мерки; врши директна контрола во однос на усогласеноста со безбедносните барања на информациските системи, преку следење на усогласеноста со безбедносните процедури при инсталација, конфигурација, одржување и промени во информациските системи или мрежата;
  b) Системски администратори - инсталираат, конфигурираат и одржуваат доверливи системи и управување со услуги на Evrotrust. Ова вклучува обновување на системот;
  c) Системски оператори - одговорни за секојдневното работење на доверливите системи на Evrotrust. Се овластени да вршат системски резервни копии;
  d) Системски ревизори - тие се овластени да ги прегледуваат и ревидираат архивите и дневниците на доверливите системи на Evrotrust.
  e) Дополнителни улоги – Evrotrust има вработени кои извршуваат доверливи улоги за специфични услуги за доверба.
- На персоналот на Evrotrust им се доделуваат доверливи улоги од страна на повисокото раководство врз основа на „најмалата привилегија“ при пристап или конфигурирање на привилегии за пристап;
- На персоналот не му се дозволува пристап до доверливи функции додека не се завршат потребните проверки. Evrotrust бара потврда за криминално досие.

7. ЕВИДЕНЦИЈА НА НАСТАНИ И ВОДЕЊЕ НА ДНЕВНИЦИ

За ефикасно управување и функционирање на Evrotrust, се евидентираат сите настани кои имаат значително влијание врз безбедноста и доверливоста на технолошкиот систем, контролата врз персоналот и клиентите, како и влијанието врз безбедноста на дадените услуги. Evrotrust гарантира високо ниво на безбедност на личните податоци при нивната обработка и шифрирање. Во случај на несреќа, можно е брзо враќање на зачуваните записи. Информациите за е-дневникот автоматски се генерираат. Дневниците на снимените настани се чуваат во датотеки на системскиот диск најмалку 6 (шест) месеци. За тоа време, тие се достапни на интернет или во процес на пребарување од овластени вработени во Evrotrust. По овој период, евиденцијата се чува во архивата. Архивираните дневници се чуваат најмалку 10 (десет) години, по што безбедно се уништуваат. Архивата е потпишана со електронски потпис/електронски временски печат.

8. АРХИВИРАЊЕ

Evrotrust ги архивира сите податоци и датотеки поврзани со: информации за регистрација; со системска безбедност; сите барања поднесени од клиенти; сите информации за клиентите; сите клучеви што ги користат органите за сертификација и органот за регистрација; и целата кореспонденција помеѓу Evrotrust и клиентите. Сите документи и податоци што се користат во процесот на проверка на идентитетот се резервни копии.

Evrotrust ги евидентира и ги чува на располагање за соодветен период, вклучително и за случаи кога ги суспендирал своите активности, сите релевантни информации во врска со податоците издадени и примени од него, а особено со цел да обезбеди докази во правните постапки и да обезбеди континуитет во давањето на услугата. Evrotrust не ги користи собраните и зачуваните информации за други цели освен оние поврзани со неговата активност.

9. БЕЗБЕДНОСТ НА АКТИВНОСТА

Софтверските апликации што се користат во технолошкиот систем на Evrotrust се развиени и имплементирани од високо квалификувани специјалисти. Пред да воведат нови апликации, тие поминуваат низ тест период. Тестирањето се врши на посебни системи, независни од оние во редовна работа. Сите хардверски промени се следат и евидентирани. При набавка на нова техничка опрема таа се снабдува со потребните работни процедури и упатства за употреба. Тековната конфигурација на технолошкиот систем на Evrotrust, како и сите промени и ажурирања на системот, се евидентираат и се вршат на контролиран начин. Контролите овозможуваат континуирана проверка на интегритетот на технолошкиот систем и навремено ажурирање и отстранување на проблеми.

Evrotrust користи доверливи системи и производи кои се заштитени од модификации и гарантираат техничка сигурност и доверливост на процесите што ги поддржуваат. Evrotrust ги применува следниве барања:

- врши анализа на безбедносните барања при дизајнирање на нови системи и нови услуги за да се обезбеди нивната безбедност;
- ги спроведува процедурите за контрола на промените во софтверот и конфигурацијата на технолошките системи;
- процедурите за контрола на промените ја вклучуваат нивната документација;
- интегритетот на системите и информациите на Evrotrust е заштитен од вируси, малициозен и неовластен софтвер;
- средствата што се користат во системите на Evrotrust се безбедно обработени за да се заштитат записите од оштетување, кражба, неовластен пристап и застареност;
- процедурите за управување со евиденцијата се заштитени од морална застареност и влошување во периодот за кој се бара да се води евиденција;
- процедурите се применуваат од сите доверителски и административни улоги вклучени во

испораката на услуги;

- Evrotrust развива и спроведува процедури за да се осигура дека:
  a) безбедносните „закрпи“ се применуваат во разумен временски период по кој тие стануваат достапни;
  b) безбедносните „закрпи“ не се применуваат доколку постои ризик од воведување дополнителни ранливости или нестабилности кои ги надминуваат придобивките од нивната примена;
  c) документирајте ги причините зошто не се применуваат безбедносни закрпи.

9.1. ПОЛИТИКА ЗА БЕЗБЕДНОСТ НА ИНФОРМАЦИИ

Evrotrust има развиено и одобри од раководството Политика за безбедност на информации и ги применува следните барања:

- Политиката го дефинира пристапот на Evrotrust за управување со активностите за безбедност на информациите;
- Промените во политиката за безбедност на информациите се доставуваат до трети страни (корисници, засегнати страни, надзорни и други регулаторни органи, тела за оцена на сообразност) кога е применливо;
- Политиката за информациска безбедност на Evrotrust е документирана, имплементирана и ажурирана;
- Сите вработени во Evrotrust се запознаени со Политиката за безбедност на информациите;
- Evrotrust е одговорен за усогласеност со процедурите во Политиката за безбедност на информациите во случаи кога дел од своите активности ги пренесува на подизведувачи. Во присуство на подизведувачи, Evrotrust ја одредува нивната одговорност и гарантира дека тие строго ги спроведуваат сите контроли за безбедноста на информациите што ги бара Evrotrust;
- Политиката за информациска безбедност на Evrotrust и пописот на средствата за безбедност на информациите се прегледуваат во планирани интервали или доколку се случат значителни промени за да се обезбеди нивната соодветност, соодветност и ефективност;
- Сите промени кои можат да влијаат на нивото на обезбедената безбедност на информациите се одобрени од тело за управување со безбедноста на информациите;
- Конфигурацијата на системите на Evrotrust редовно се проверува за промени што може да ги прекршат правилата за безбедност на информациите. Максималниот интервал помеѓу две проверки е според внатрешните процедури на Evrotrust.
- Политиката за безбедност ги документира безбедносните контроли и приватноста на личните податоци. Личните податоци доставени до Evrotrust се складираат и обработуваат во согласност со Законот за заштита на личните податоци и РЕГУЛАТИВАТА (ЕУ) 2016/679

Општа регулатива за заштита на податоци (GDPR). Evrotrust собира количина на информации пропорционални на неговата намена и употреба. Секој корисник се согласува за обработка на неговите лични податоци. Оваа согласност се покажува со потпишување на Договор за електронска идентификација. Личните податоци се користат само во врска со обезбедувањето на конкретната услуга. Личните податоци се заштитени во согласност со правилата за приватност содржани во безбедносната политика на Evrotrust.

9.2. МРЕЖНА БЕЗБЕДНОСТ

Evrotrust ја гарантира мрежната безбедност на системите од надворешни интервенции и закани со користење на процедурите што тие ги применуваат следните барања:

- во случај на далечински пристап до системи кои складираат или обработуваат доверливи податоци, политиката е да се документираат контролите за безбедност и приватност имплементирани за заштита на личните податоци.
- во случај на далечински пристап до системи кои складираат или обработуваат доверливи податоци, преземени се мерки за заштита од ризиците од далечински пристап.

10. РАНЛИВОСТ И ПРОЦЕНКА

10.1. ПРОЦЕНКА НА РИЗИК

Со цел да се обезбеди квалитетот и доверливоста на обезбедената услуга за електронска идентификација, Evrotrust врши проценка на ризикот. Evrotrust ги класифицира и води регистрите на сите средства во согласност со барањата на ISO/IEC 27001. Според Политиката за безбедност, се врши анализа за проценка на ранливоста на сите внатрешни процедури, апликации и информациски системи. Барањата за анализа може да се утврдат и од надворешна институција овластена да врши ревизија на Evrotrust. Анализата на ризик се врши најмалку еднаш годишно. Одлука да се пристапи кон анализа носи менаџментот на Evrotrust. Evrotrust ги применува следниве барања:

- врши проценка на ризик за да се идентификуваат, анализираат и проценат ризиците поврзани со деловни и технички прашања со обезбедената услуга за сертификати;
- избира соодветни мерки за лекување на ризикот, земајќи ги предвид резултатите од проценката на ризикот. Мерките за управување со ризик обезбедуваат дека нивото на безбедност е пропорционално со степенот на ризик;
- ги дефинира сите безбедносни барања и оперативни процедури кои се неопходни за исполнување на избраните мерки за третирање на ризикот, како што е документирано во политиката за безбедност на информациите и во практиката;
- проценката на ризикот се ревидира периодично;
- раководството ја одобрува проценката на ризикот и го прифаќа идентификуваниот резидуален ризик.

10.2. УПРАВУВАЊЕ СО ИНЦИДЕНТИ

Сите системи вклучени во издавањето електронски идентитет нудат висок степен на доверливост. Технолошкиот систем се наоѓа во физички заштитена средина, што го минимизира ризикот од природни катастрофи.

За управување со инциденти, Evrotrust применува процедури кои ги исполнуваат следните барања:

- ги следи сите активности поврзани со пристап и користење на информациски системи и барања за услуги;
- како резултат на мониторингот, се известува и анализира чувствителноста на секоја собрана информација;
- абнормални системски активности кои укажуваат на потенцијално нарушување на безбедноста, вклучително и упад во системот и мрежата на Evrotrust, се откриваат и се пријавуваат како аларми;
- Evrotrust ги следи следните настани:
  a) овозможете и оневозможете карактеристики за евиденција; и
  b) достапност и користење на потребните услуги во мрежата на Evrotrust.
- Evrotrust делува навремено и координирано за брзо реагирање на инциденти и ограничување на влијанието на безбедносните прекршувања;
- назначува доверливи службеници кои ќе ги следат предупредувањата за потенцијално критични настани и ќе обезбедат дека релевантните инциденти се пријавени во согласност со воспоставените внатрешни процедури;
- Evrotrust воспостави процедури за известување на релевантните надлежни органи во согласност со важечките регулаторни правила за секое нарушување на безбедноста или губење на интегритетот што има значително влијание врз услугата за автентикација и личните податоци, во рок од 24 часа од откривањето на прекршувањето;
- Кога нарушувањето на безбедноста или губењето на интегритетот може негативно да влијае на физичко или правно лице на кое му е обезбедена услуга за автентикација, Evrotrust ќе го извести истото физичко или правно лице за повреда на безбедноста или губење на интегритетот без непотребно одлагање;
- Системите на Evrotrust редовно се следат за да се идентификуваат докази за злонамерна активност, се имплементираат механизми за автоматска обработка на дневници и вработените се предупредени за можни критични настани поврзани со безбедноста;
- Evrotrust ќе ја објави секоја критична ранливост што претходно не ја објавил во период од 48 часа по нејзиното откривање;
- За секоја ранливост, со оглед на нејзиното потенцијално влијание, Evrotrust:
  a) креира и спроведува план за ублажување на ранливоста; или
  b) документи со докази дека ранливоста не бара ублажување, на пример ако трошоците за нејзиното потенцијално влијание не ги оправдуваат трошоците за нејзино

ублажување;

- Постапките за известување и одговор за инциденти се користат на таков начин што штетата од безбедносни инциденти и дефекти на системот е минимизирана.

11. ПРЕСТАНОК НА ДЕЈНОСТА НА EVROTRUST

Обврските опишани подолу се дизајнирани да го минимизираат деловното нарушување на клиентите и засегнатите страни кои произлегуваат од одлуката на Evrotrust да го прекине работењето.

11.1. ПРЕСТАНОК НА ДЕЛОВНИ АКТИВНОСТИ

По престанокот на активноста на Evrotrust, компанијата ќе го стори следново:

- Следува ажуриран и одобрен од раководството план и сценарио за престанок на дејноста на органот за сертификација;
- известете ги клиентите,националниот надзорен орган во Република Северна Македонија - Министерство за информатичко општество и администрација (МИОА) и трети лица за престанок на дејноста на нејзиниот орган за сертификација. Информациите се обезбедуваат преку е-пошта или со објавување на веб-страницата на Evrotrust;
- го прекинува овластувањето на сите лица кои имаат договорни работи за вршење работи поврзани со давање на услугата;
- пред да ја прекине активноста, во разумен временски период, ги пренесува своите обврски за одржување на сите информации потребни за обезбедување докази на доверлива страна;
- пред да престанат да работат, приватните клучеви, вклучувајќи ги и резервните копии, се уништуваат или се повлекуваат од употреба на таков начин што приватните клучеви не можат да се повлечат;
- ако е можно, ја пренесува својата активност на друг давател на шема за електронска идентификација;
- Evrotrust спроведува мерки за покривање на трошоците во случај на стечај или поради други причини за престанок на дејноста. Во случај да не може сам да ги покрие трошоците, има предвидено мерки во рамките на важечката законска регулатива;
- престанува да издава потврди и електронска идентификација;
- прави комерцијално разумни напори да го минимизира нарушувањето на интересите на клиентите.

11.2. ПРЕНОС НА АКТИВНОСТ НА ДРУГ ДАВАТЕЛ НА ШЕМИ ЗА ЕЛЕКТРОНСКА ИДЕНТИФИКАЦИЈА

Со цел да се обезбеди континуитет на издавање на електронски идентитет на клиентите, Evrotrust може да потпише договор со друг добавувач на шеми за електронска

идентификација. Во овој случај, Evrotrust:

- го известува Надзорниот орган за својата намера најдоцна 2 месеци пред датумот на престанок и пренос на дејноста;
- писмено го известува Надзорниот орган и клиентите дека неговата дејност ја презема друг давател на шема за електронска идентификација, како и за неговото име. Известувањето е објавено на веб-страницата на Evrotrust;
- ги информира клиентите за условите за одржување на пренесените информации до давателот на услугата што прима;
- да го промени статусот на оперативните сертификати и уредно да ја пренесе целата документација поврзана со неговата дејност на добавувачот што прима, заедно со сите архиви, како и сите издадени сертификати;
- ги врши потребните дејствија за пренос на обврските за одржување на информациите на давателот на услугите што ги прима. Добавувачот што прима ги презема правата, обврските и архивата на Evrotrust.

11.3. ПОВЛЕКУВАЊЕ НА СТАТУСОТ НА EVROTRUST КАКО РЕГИСТРИРАН ДАВАТЕЛ НА ШЕМАТА ЗА ЕЛЕКТРОНСКА ИДЕНТИФИКАЦИЈА

По одземањето на статусот на Evrotrust како регистриран давател на шема за електронска идентификација, тој ќе го стори следново:

- да ги извести своите клиенти за неговиот променет статус;
- престанува да издава нови електронски потврди;
- прави комерцијално разумни напори да го минимизира нарушувањето на интересите на клиентите.

12. БЕЗБЕДНОСТ НА ИТ СИСТЕМИТЕ

Evrotrust користи само доверлив и безбеден хардвер и софтвер кои се дел од неговиот компјутерски систем. Компјутерските системи на кои работат сите критични компоненти на инфраструктурата на Evrotrust се опремени и конфигурирани со средства за локална заштита на пристапот до софтверот и информациите податоци. Evrotrust користи процедури за управување со информацискатa безбедност на целата инфраструктура во согласност со стандардите општо прифатени во меѓународната практика.

Интегритетот на системите и информациите на Evrotrust е заштитен од вируси, малициозен и неовластен софтвер. Средствата што се користат во системите на Evrotrust се безбедно обработени за да се заштитат записите од оштетување, кражба, неовластен пристап и застареност. Evrotrust развива и имплементира процедури за да се осигура дека безбедносните закрпи се применуваат во разумен временски период по кој тие стануваат достапни; безбедносните закрпи не се применуваат доколку постои ризик од воведување дополнителни пропусти или нестабилности кои ги надминуваат придобивките од нивната

примена и ги документира причините зошто безбедносните закрпи не се применуваат.
Физичката безбедност на системите за издавање и управување со сертификати е во согласност со барањата на меѓународните стандарди и препораки. Воспоставена е двофакторна контрола на пристап и 24-часовно вооружено физичко обезбедување. Пристап до кабинетот со опремата не е дозволен на повеќе од 2 (две) овластени технички лица на Evrotrust. Секој пристап до просториите со критична инфраструктура е документиран во посебни дневници. Заштитата ја обезбедува невооружено 24-часовно обезбедување. Просториите на Evrotrust имаат систем за алармна сигнализација, систем за видео надзор, систем за сигнално известување и систем за контрола на пристап. Сите системи се проверуваат периодично. Овластениот персонал на Evrotrust строго ги следи развиените внатрешни процедури за пристап до различни области со ограничен физички пристап. Пристапот до областа на операторите и администраторите е ограничен и се спроведува преку употреба на паметна картичка и систем за контрола на пристап.

12.1. БЕЗБЕДНОСТ НА ЖИВОТНИОТ ЦИКЛУС НА ТЕХНОЛОШКИОТ СИСТЕМ

Сите хардверски промени се следат и регистрираат од овластени вработени во Evrotrust. При набавка на нова техничка опрема таа се снабдува со потребните работни процедури и упатства за употреба. Ја надгледува функционалноста на процесот на системот и гарантира дека тој функционира правилно и во согласност со испорачаната производна конфигурација.

13. МРЕЖНА БЕЗБЕДНОСТ

Во инфраструктурата на Evrotrust се користат современи технички средства за размена и заштита на информации за гарантирање на мрежната безбедност на системите од надворешни интервенции и закани.

14. ТЕХНИЧКИТЕ И БЕЗБЕДНОСНИТЕ КАРАКТЕРИСТИКИ НА СРЕДСТВАТА ЗА ЕЛЕКТРОНСКА ИДЕНТИФИКАЦИЈА

14.1. EID ПРЕКУ МОБИЛНАТА АПЛИКАЦИЈА EVROTRUST

Механизмот за електронска идентификација преку мобилната апликација на Evrotrust се заснова на издаден квалификуван атрибутивен сертификат за квалификуван електронски потпис. Издадените квалификувани сертификати максимално ги штитат податоците за електронската идентификација, така тоа е многу малку веројатно напаѓач со промовиран основни потенцијал за напад Да може преку активности допаѓа нагаѓање, прислушкување, репродукција или манипулација на комуникацијата Да злоупотреби со механизмот за автентикација на автентичноста. Значењата за електронски идентификација сè дизајни така, тоа издавачот Да преземаат соодветно мерки, за Да проверки, тоа сè користи само под контрола или во поседување на лицето,на кои припаѓа Системот Evrotrust користи поседување на инсталирана апликација на личен мобилен телефон (фактор на поседување)

и внесување на Лична шифра за пристап/ПИН код (фактор на знаење). Дополнително, мобилната апликација поддржува опција за биометриско препознавање на лицето и/или отпечатокот од прст (фактор – биометрика). Се врши динамична автентикација, која користи криптографска техника која обезбедува начин да се создаде електронска потврда на барање дека субјектот ги контролира податоците за идентификација и која се менува со секоја автентикација помеѓу субјектот и системот што го потврдува идентитетот на субјектот. Средствата за електронска идентификација се заштитени од дуплирање и манипулации со користење на криптографски клучеви и алгоритми. Заштитата од напаѓачи со висок потенцијал за напад се спроведува преку сложени мерки, вклучувајќи DDoS системи за заштита, Firewalls, системи за резервација и бројни други софтверски и хардверски решенија. Мобилната апликација што се користи е дизајнирана така што лицето на кое му припаѓа може со сигурност да ја заштити од употреба од други лица преку кодови за пристап, биометрика и други безбедни средства.

14.2. EID ПРЕКУ ВЕБ ИНТЕРФЕЈС

Механизмот за електронска идентификација, преку веб-интерфејс, се заснова на креирана датотека која ги содржи личните податоци на лицето во структурирана форма, претставена преку општо прифатен стандард. Интеграцијата на веб-апликацијата ја заштитува околината од неовластени дејства како на пр нагаѓање, прислушкување, репродукција или манипулација на комуникацијата со цел злоупотреба а со механизмот за автентикација на автентичноста. Значењата за електронски идентификација сѐ дизајни така, тоа издавачот Да преземаат соодветно мерки,за Да проверки, тоа тоа сѐ користи само под контрола или во поседување на лицето, на кои припаѓа Технологијата развиена од Evrotrust се потпира на два фактори - поседување личен мобилен телефон (фактор на поседување), од кој преку независен канал се потврдува издавањето на средствата за идентификација и внесување на персоналниот код за пристап/ПИН кодот (фактор на знаење). . Дополнително, технологијата поддржува опција за биометриско препознавање на лицето (фактор - биометрика), во рамките на процесот на идентификација. Се врши динамична автентикација, која користи криптографска техника која обезбедува начин да се создаде, на барање, електронска потврда дека субјектот има контрола над процесот на идентификација. Средствата за електронска идентификација се заштитени од дуплирање и манипулации со користење на криптографски клучеви и алгоритми за временско печатење. Заштитата на веб-базирана платформа во која е интегрирано решението мора да обезбеди мерки против напаѓачите со висок потенцијал за напади и мора да обезбеди сеопфатни мерки вклучувајќи системи за заштита на DDoS, заштитен sидови, системи за резервација и мноштво други софтверски и хардверски решенија. Користената веб-базирана платформа мора да биде дизајнирана така што лицето на кое му припаѓа може веродостојно да ги заштити средствата за електронска идентификација од употреба од други лица преку кодови за пристап, биометрика и други безбедни средства.

15. ВЕРИФИКАЦИЈА И КОНТРОЛА НА АКТИВНОСТИТЕ НА EVROTRUST

15.1. ВНАТРЕШНИ РЕВИЗИИ

Внатрешните ревизии на Evrotrust имаат за цел да ја контролираат активноста на обезбедување електронска идентификација и да ја потврдат усогласеноста со барањата на важечките стандарди и одлуките и мерките за внатрешно управување. Evrotrust е предмет на најмалку една внатрешна ревизија годишно. Резултатите од ревизиите се сумирани во извештаи. Врз основа на оценките направени во извештајот, менаџментот на Evrotrust утврдува мерки и рокови за отстранување на констатираните празнини и недоследности.

15.2. НЕЗАВИСНА НАДВОРЕШНА РЕВИЗИЈА

Evrotrust се ревидира најмалку еднаш на секои 36 месеци од независен инспекциски тим според меѓународниот стандард ISO/IEC 27001.

Алатката за електронска идентификација на Evrotrust е потврдена од страна на Орган за оцена на сообразност Регулатива (ЕУ) 2015/1502. Како резултат по успешно завршената инспекција, Evrotrust доби потврда за „високо“ ниво на осигурување. Нивото на гаранција се однесува на средство за електронска идентификација во контекст на шемата за електронска идентификација на Evrotrust што обезбедува висок степен на доверба во тврдениот или тврдениот идентитет на поединецот, и се карактеризира со повикување на релевантните технички спецификации, стандарди и процедури, вклучувајќи технички проверки насочени кон спречување на злоупотреба или промена на идентитетот.

15.3. РЕВИЗИЈА ОД СТРАНА НА НАЦИОНАЛЕН НАДЗОРЕН ОРГАН

Националниот надзорен орган може во секое време да изврши ревизија.

16. ФИНАНСИСКИ ОБВРСКИ

Evrotrust е одговорен за услугата за проверка на идентитетот што им се обезбедува на лицата кои се потпираат на идентификација. Evrotrust одговара доколку штетите се по негова вина и настанати од крајно невнимание или умисла во одредена граница.

Доколку Evrotrust потврди и прифати дека настанала штета, се обврзува да плати за штетите што се директна и непосредна последица на несовесното однесување на вработените.

17. ДЕЛОВНО ОСИГУРУВАЊЕ

Evrotrust презема задолжително осигурување за својата дејност во обезбедување на услуга за електронска идентификација. Задолжителното осигурување има непрекинат рок и се обновува еднаш годишно. Предмет на осигурувањето е одговорност на Evrotrust за неговите активности, согласно барањата на важечката законска регулатива. Задолжителното осигурување ја покрива одговорноста на Evrotrust кон физичките лица, односно доверливите

страни за предизвикани имотни и неимотни штети до границите дефинирани во националното законодавство. По појавата на настан кој може да дозволи побарување покриено со осигурувањето, засегнатото лице мора писмено да го извести Evrotrust и осигурителот во рок од 7 дена откако настанот ќе му стане познат. Осигурувањето не покрива случаи на одрекување, особено за штети предизвикани од непочитување на обврските на физички лица, виша сила и други околности кои се надвор од контрола на Evrotrust.

18. ПРИВАТНОСТ НА ЛИЧНИТЕ ПОДАТОЦИ

Evrotrust строго забележува дека вработените ги исполнуваат условите за доверливост и нераспределба на личните податоци на лицата кои му станале познати при спроведување на активноста за електронска идентификација.

Evrotrust ги евидентира и одржува пристапот за соодветен временски период, вклучително и по престанокот на неговите активности, сите информации во врска со податоците издадени и примени во текот на неговите активности, со цел да обезбеди докази во правните постапки и со цел да се обезбеди континуитет на услугите. Ја одржува доверливоста и интегритетот на тековните и архивираните записи во врска со работењето на Услугите. Документите кои се однесуваат на функционирањето на услугите се архивираат целосно и доверливо во согласност со добрите деловни практики. Документите кои се однесуваат на работењето на Услугите се обезбедуваат доколку се потребни за да се обезбедат докази за правилното функционирање на Услугите за целите на правните постапки. Се запишува точното време на настаните поврзани со управувањето со активностите, како што се управувањето со клучеви и синхронизацијата на часовникот. Времето што се користи за снимање настани, како што се бара во дневникот за ревизија, се синхронизира со UTC најмалку еднаш дневно. Евиденцијата во врска со услугите се чува за временски период кој е погоден за обезбедување на потребните правни докази и како што е напишано во Општите услови и договорот. Настаните се евидентирани на начин што не може лесно да се избришат или уништат освен ако не се пренесат веродостојно во долгорочни архиви во периодот што треба да се чуваат.

18.1. ПРАВА НА ИНТЕЛЕКТУАЛНА СОПСТВЕНОСТ

Различните податоци вклучени во издадените сертификати за квалификувани атрибути, односно датотеките со податоциво машински читлива форма, се предмет на права на интелектуална сопственост и други имотни и несопственички права.

19. ОБВРСКИ, ОДГОВОРНОСТ И ГАРАНЦИИ НА EVROTRUST

19.1. ГАРАНЦИИ И ОБВРСКИ

Evrotrust гарантира да обезбеди електронска идентификација како што се:

- строго ги исполнува условите во овој документ, барањата од Регулативата (ЕУ) бр. 910/2014, Регулативата (ЕУ) 2016/679 и националното законодавство;

- обезбедената услуга не ги повредува авторските права и лиценцираните права на трети лица;
- користи техничка опрема и технологии кои обезбедуваат доверливост на системите и техничка и криптографска безбедност при спроведувањето на процесите, вклучувајќи безбеден и безбеден механизам/уред за генерирање клучеви и создавање електронски потпис;
- квалификуваните атрибутивни сертификати за електронски потписи, односно датотеките со податоци во структуриран машински читлив формат, се издаваат откако презентираните информации се потврдени со законски дозволени средства;
- информациите поврзани со обезбедениот електронски идентитет и оперативната работа на системите се чуваат и одржуваат безбедно;
- ги почитува утврдените работни процедури и правила за техничка и физичка контрола, во согласност со условите во овој документ;
- дава можност веднаш да ја прекине важноста на сертификатот за квалификуван атрибут и веднаш да ги извести заинтересираните страни по неговото раскинување;
- обезбедува услови за точно утврдување на времето на издавање и престанок на електронскиот идентитет;
- обезбедува мерки против фалсификување на атрибутивни акредитиви и доверливост на податоците до кои се пристапува во процесот на идентификација;
- користи сигурни системи за складирање и управување со податоци;
- презема итни мерки во случај на технички безбедносни проблеми;
- по истекот на периодот на важност на квалификуваниот атрибутивен сертификат, да се откаже од неговата важност;
- ги информира клиентите и засегнатите страни за нивните обврски и должна грижа за однесување при користење и доверба на обезбедената услуга за електронска идентификација;
- ги користи и чува собраните лични и други информации само за целите на својата активност за обезбедување електронска идентификација во согласност со националното законодавство;
- има имплементирано шема за електронска идентификација во согласност со Регулативата (ЕУ) бр. 910/2014 и техничките спецификации развиени во согласност со неа;
- да ги идентификува корисниците и да обезбеди средства за електронска идентификација од далечина, во согласност со ETSI TS 119 461 и сите други технички спецификации и препораки релевантни за технологијата развиена од организацијата и во согласност со барањата од Регулативата (ЕУ) бр. 2015/1501 за целите на интероперабилноста;
- има осигурување за времето на својата дејност;
- одржува доверлив персонал кој ја поседува потребната експертиза, искуство и квалификации за извршување на дејноста;

- води јавен регистар;
- обезбедува постојан пристап до јавниот регистар по електронски пат (24/7/365);
- обезбедува заштита од промена на водениот јавен регистар од нерегулиран и незаконски пристап или поради случаен настан;
- врши периодични внатрешни и надворешни ревизии на своите активности;
- користи сертифициран софтвер и хардвер, како и безбедни и сигурни технолошки системи во своите активности.

19.2. ОДГОВОРНОСТИ

Evrotrust е одговорен пред клиентите и засегнатите страни за штети предизвикани од грубо невнимание или намера:

- од неисполнување на барањата од Регулативата (ЕУ) бр. 910/2014 и легислативата што се применува во Република Северна Македонија при вршење на својата дејност за обезбедување на шема за електронска идентификација;
- од неуспехот да се утврди идентитетот/идентитетот на лицето поради грубо невнимание и неусогласеност со политиките и практиките наведени овде;
- од неточни или исчезнати податоци во сертификатот за квалификуван атрибут во моментот на неговото издавање;
- од алгоритамското несовпаѓање помеѓу приватниот клуч и јавниот клуч внесен во сертификатот.
- од неусогласеност со своите обврски за издавање и управување со квалификувани сертификати за атрибуција;
- од внесување неточни или исчезнати податоци во сертификатите;

20. ОБВРСКИ НА КЛИЕНТИТЕ

Клиентите на Услугата за верификација на идентитет ги имаат следните обврски:

- да се запознаат и да ги почитуваат условите на Општите услови, политики и практики при обезбедување на електронска идентификација, како и барањата во другите документи објавени во јавниот регистар;
- да обезбеди вистинити, точни и целосни информации кои се потребни според Условите и условите, регулаторните барања, важечките политики и практики;
- во случај на неусогласеност помеѓу презентираните информации и автентицираната содржина, клиентот мора веднаш да го извести Evrotrust;
- да ги одобри условите наведени во Општите услови помеѓу него и Evrotrust.

21. ОДГОВОРНОСТ НА КЛИЕНТИТЕ

Одговорноста на клиентот е резултат на неисполнување на неговите обврски. Условите за одговорност се регулирани со Општите одредби и услови. Клиентот е одговорен доколку:

- не ги исполнува точно барањата на овој документ;
- има дадено лажни изјави поврзани со услугата за електронска идентификација;
- кога физичко лице кое нема претставничко овластување иницира услуга за идентификација на правно лице, тоа лице одговара за штета.

22. ОДРЕКУВАЊЕ

Evrotrust не е одговорен за штети предизвикани од:

- незаконски дејствија од страна на клиентите и засегнатите страни;
- случајни настани кои имаат карактер на виша сила, вклучително и злонамерни дејствија на трети лица (хакерски напади, конфискација на мобилен уред, пристап до средства за идентификација итн.)
- барање на услугата за проверка на идентитетот од страна на лице кое не ги исполнува барањата и процедурите од Практиките и политиките на Evrotrust.

23. РЕШАВАЊЕ НА СПОРОВИ

Спорови може да бидат само недоследности или противречности меѓу лица, страни во договорот. Споровите или поплаките во врска со употребата на електронска идентификација или квалификувани сертификати за атрибуција ќе се решаваат, со посредување, врз основа на информации доставени во писмена форма до Evrotrust.

24. ВАЖЕЧКИ ЗАКОН

За сите прашања кои не се решени во овој документ, ќе се применуваат одредбите од важечката законска легислатива.