Правила и услови

за користење на услуга KIBSTrust OneID

Последна промена: 16.08.2022 (види ги архивираните верзии)

1. Општи услови

Во овој документ насловен како „Правила и услови за користење на услугата KIBSTrust OneID" (Правила и услови) се опишани правилата кои ги поставува и следи КИБС АД Скопје при давањето на услуга за електронска идентификација и создавање на средство за електронска идентификација, како и условите под кои оваа услуга се испорачува кон корисниците. КИБС АД Скопје како компанија има два главни правци на делување: од една страна како клириншка куќа на мали меѓубанкарски плаќања и носител на платен промет, а од друга страна е Давател на доверливи услуги и Давател на услуги за електронска идентификација кои организациски претставуваат дел од КИБС, но настапува под брендот со име **KIBSTrust**.

За услугата KIBSTrust OneID (OneID) правилата и условите се базираат на документот „Практика за давање на услуга за електронска идентификација" (Практика).

1.1. Со „Практика за давање на услуга за електронска идентификација" се регулира проверката на идентитетот на далечина и издавањето на средство за електронска идентификација, по претходно барање на физичко или правно лице кое е субјект на идентификацијата (Субјект) пред издавач на средства за електронска идентификација.

1.2. Субјектот мора да се запознае со Практиката и истата да ја прифати. Правилата и условите и Практиката сочинуваат правно обврзувачки договор помеѓу Субјектот и КИБС.

1.3. Субјектот аплицира за спроведување на електронска идентификација (eID) своеволно врз основа на иницирана потреба од страна на давател на online услуги или по сопствена желба, со цел добивање на средство за електронска идентификација.

1.4. За да биде издадено средство за електронска идентификација, Шемата за електронска идентификација, , предвидува:

- далечинска проверка на идентитетот на Субјектот со употреба на метод кој овозможува сигурност еднаква на физичкото присуство (член 24, став 1 g од eIDAS Регулативата и член 31 од MK-eIDAS). Оваа проверка на идентитетот на физичкото лице се спроведува со користење на биометриски податоци или физички карактеристики кои на единствен начин го поврзуваат лицето со документите за лична идентификација за што има и потврда од доверлив извор, или
- проверката на идентитетот на Субјектот за кој веќе е издаден квалификуван електронски сертификат по неговата идентификација со физичко присуство, од страна на признаен давател на квалификувани доверливи услуги кој презентирал прифатливи официјални документи за идентификација (член 24, став 1a од eIDAS Регулативата и член 11 од MK-eIDAS).

1.5. Прифатливи документи за идентификација на Субјектот се: национална лична карта за жител на Република Северна Македонија, привремена лична карта за странски државјани со привремен престој во Република Северна Македонија и патна исправа (пасош) издаден од страна на Република Северна Македонија.

1.6. KIBSTrust може целиот процес на верификација на идентитетот или негов дел да го додели на извршување на трето лице.

1.7. KIBSTrust може да одбие да издаде средство за електронска идентификација, според свое наоѓање, доколку валидацијата на идентитетот со користење на некоја од методите, наведени во став 1.5 не е успешена.

1.8. За Субјектот, чиј идентитет е потврден преку методот на далечинска електронска идентификација, дополнително ќе се применуваат условите наведени во став 5.3. Далечинската проверка на

идентитетот е достапна и изводлива, само кога околностите за време на процесот на проверка на идентитетот се доволни за да се обезбеди точен доказ за идентитетот на Субјектот.

1.9. Процесот на спроведување на електронска идентификација и издавање на средство за електронска идентификација е поврзан со поседување на паметен мобилен уред кај Субјектот, инсталирана апликација OneID Mobile на истиот уред, постоење на валида адреса за електронска пошта и број за мобилна линија придружена на паметниот мобилен уред.

1.10. Субјектот треба да биде деловно способно лице за да започне процедура на спроведување на електронска идентификација.

1.11. Субјектот се согласува квалификуваниот сертификат кој се креира за него во процесот на создавање на електронскиот идентитет да биде сместен на средство за креирање квалификуван потпис (QSCD) во облак, обезбеден од KIBSTrust. Субјектот е единствено одговорен за правилна употреба на QSCD.

1.12. Субјектот може да побара сертификатот кој е дел од средството за електронска идентификација да не се објави во Јавниот именик на издадени сертификати на KIBSTrust.

1.13. Субјектот може да не ја плаќа услугата за создавање на електронски идентитет и користење на квалификуваниот сертификат креиран во процесот на електронска идентификација само кога трета страна давател на online услуги го иницира процесот на електронска идентификација и/или користење на издадениот квалификуван сертификат.

1.14. КИБС, а следствено и KIBSTrust како QTSP гарантира почитување на принципот на еднаквост и заштита од дискриминација при остварување на човековите права и слободи[1].

1.15. KIBSTrust го задржува правото, според свое наоѓање, да ги менува и дополнува својата Практика и овие Правила и услови во секое време и без известување, доколку за тоа постои оправдана потреба, односно кога тоа е задолжително според регулаторните барања или измена на стандардите. Измените и дополнувањата се објавуваат 30 дена пред стапувањето во сила. Тековната верзија и претходната верзија се објавени на https://www.kibstrust.com/repository. За измените или дополнувањата на документите Субјектот ќе биде соодветно информиран.

2. Тип на квалификуван сертификат како дел од средството за електронска идентификација и негово прифаќање

2.1. Квалификуваниот сертификат придружен на средството за електронска идентификација како вид, намена и постапка на издавање е опишан во следната табела:

Вид на сертификат	Намена	Применета и објавена политика за сертификација
Квалификувани електронски потписи во согласност со МК-eIDAS и eIDAS. Cert Policy IDs: 1.3.6.1.4.1.16305.1.2.5.1.4 (Remote QSCD) and 0.4.0.194112.1.2 (QCP-n-qscd)	Податоци во електронска форма кои се приложени или логички поврзани кон други податоци во електронска форма и кои потписникот ги користи за потпишување.	CP/CPS на КИБС за квалификувани сертификати за електронски потписи, квалификувани електронски печати и временски жигови се објавени на: https://www.kibstrust.com/repository Во согласност со: ETSI EN 319 411-2 Certificate Policy: QCP-n-qscd Cert Policy ID: 1.3.6.1.4.1. 16305.1.1.5

Табела 1

2.2. Квалификуваните сертификати издадени во процесот на електронска идентификација и средството за електронска идентификација се со валидност од 2 години.

[1] Закон за спречување и заштита од дискриминација

2.3. Следниве постапки претставуваат прифаќање на средството за електронска идентификација:

- Преземањето на квалификуваниот сертификат како дел од средството за електронска идентификација претставува прифаќање на средството за електронска идентификација од страна на Субјектот.
- Субјектот нема да достави приговор за квалификуваниот сертификат и неговата содржина во рок од 5 дена од издавањето на средството за електронска идентификација.

3. Забрана за користење на средство за електронска идентификација

3.1. Средството за електронска идентификација кое се користи за автентикација од страна на Субјектот може да се користи и за потпишување на електронски документи, под услов употребата на овој тип потпишување да не е забранета на друг начин со закон, забранета за користење со овие Правилата и услови, Практиката, како и други договори на Субјектот со третата страна.

3.2. Квалификуваниот сертификат како дел од средството за електронска идентификација на Субјектот не може да се користи надвор од границите и контекстот наведен во делот „Применета и објавена политика за сертификација“ дадена во Табела 1 погоре за квалификувани сертификати за електронски потписи за незаконски цели, или спротивно на јавниот интерес, или на друг начин кога постои веројатност дека ќе го нарушат деловното работење или угледот на KIBSTrust односно КИБС. Индикативно, употребата на квалификуваниот сертификат е забранета за која било од следниве цели:

3.2.1. Незаконски активности (вклучувајќи сајбер-напади и обиди за злоупотреба на сертификатот).
3.2.2. Издавање нови сертификати и информации во врска со валидноста на сертификатот.
3.2.3. Овозможување на други лица да го користат приватниот клуч на Субјектот.
3.2.4. Овозможување сертификатот издаден за електронско потпишување да се користи на автоматизиран начин.
3.2.5. Користење на сертификатот издаден за електронско потпишување документи кое може да доведе до несакани последици (вклучително и потпишување на таквите документи за потреби на тестирање).

4. Валидност на квалификуваниот сертификат и ревизорски записи

4.1. Информациите во квалификуваниот сертификат се точни. Нема грешки или суштинско погрешно претставување на фактите во сертификатот што се познати или што потекнуваат од Субјектот кој го одобруваа барањето за издавање на сертификат.

4.2. Сертификатот станува валиден на датумот наведен во сертификатот. Валидноста на сертификатот истекува на датумот наведен во сертификатот, или на датумот и во времето кога е поништен сертификатот.

4.3. Ревизорските записи се чуваат локално во период од најмалку 2 (два) месеци. Физичките или дигиталните архивски записи во врска со барањата за сертификат, информациите за регистрација и поништување се чуваат во период од најмалку 10 (десет) години по истекот на соодветниот сертификат.

5. Права и обврски на Субјектот на идентификација и обештетување

5.1. Субјектот има право да поднесе барање за издавање сертификат, прифаќајќи ги сегашните Правила и услови и треба да се придржува кон барањата предвидени во CP/CPS на KIBSTrust за квалификувани сертификати за електронски потписи.

5.2. Субјектот на електронска идентификација кој поседува или треба да поседува средство за електронска идентификација е:

5.2.1. единствено одговорен за одржување на пристапот кон неговиот приватен клуч од квалификуваниот сертификат.

5.2.2. единствено и целосно е одговорен за сите последици од користењето на неговото средство за електронска идентификација за време и по истекување на важноста на сертификатот придружен на средството за електронска идентификација.

5.2.3. единствено одговорен за секоја штета предизвикана поради неизвршување или неправилно извршување на своите обврски, наведени во овие Правила и услови и/или законите на Република Северна Македонија.

5.2.4. свесен дека електронските потписи дадени врз основа на истечени или поништени сертификати се неважечки.

5.2.5. свесен дека треба да достави точни, вистинити и целосни информации кои се суштински за создавањето на средството за електронска идентификација издавањето на сертификатот.

5.2.6. свесен дека не треба да продолжува со постапката за создавање на средство за електронска идентификација, доколку не е деловно способен.

5.2.7. свесен дека приватниот клуч од неговиот квалификуван електронски потпис се користи единствено под негова контрола и да биде внимателен за да се избегне неовластена употреба на истиот.

5.2.8. одговорен за тајноста на податоците за автентикација при пристап кон приватниот клуч (корисничко име, лозинка, ПИН) што се наоѓа на далечинско QSCD (облакот на KIBSTrust).

5.2.9. одговорен за правилната употреба на мобилниот уред на кој е инсталирана апликацијата OneID Mobile за да се креира и користи квалификуван сертификат што се наоѓа на далечинско QSCD. Доколку Субјектот го загуби или го уништи мобилниот уред, или пак не е во можност да го употреби квалификуваниот сертификат поради некоја друга причина што е надвор од контролата на KIBSTrust, тој треба да го контактира директно KIBSTrust за да побара поништување на неговиот сертификат.

5.2.10. одговорен да го користи неговиот приватен клуч и сертификат во согласност со овие Правила и услови, вклучувајќи ги применливите договори, утврдени во дел 9 и законите на Република Северна Македонија.

5.2.11. одговорен да го извести KIBSTrust за точните информации во разумно време, во случај на промена на неговите лични податоци или за секоја друга неточност во содржината на сертификатот.

5.2.12. одговорен да го информира KIBSTrust за можноста на неовластено користење на неговиот приватен клуч или, доколку неговиот приватен клуч е загубен, украден, потенцијално компромитиран или, доколку ја изгубил контролата над неговиот клуч поради компромитирање на податоците за автентикација (на пример, ПИН, ПУК, корисничко име, лозинка) или други причини, и веднаш да го поништи неговиот сертификат.

5.2.13. одговорен тој или негов правен застапник или наследник да побара поништување на сертификатот, доколку претходно воспоставените односи со Субјектот прекинале или престанале да постојат.

5.2.14. одговорен ако продолжи да го користи приватниот клуч, иако сертификатот е поништен или издавачот на сертификатот е компромитиран.

5.3. Следниве правила дополнително се однесуваат на Субјектот, чиј идентитет е верификуван со користење на метод на далечинска верификација на идентитетот:

5.3.1. Субјектот треба да ги следи инструкциите точно според дадената информација во мобилната апликација OneID, документација на KIBSTrust или овластениот вработен кој го спроведува процесот на валидација.

5.3.2. Субјектот треба да презентира документ/и за идентификација во добра состојба и со добра осветленост, до онаа мера до која може да се потврди нивната автентичност.

5.3.3. На почетокот од далечинското препознавање и пред започнување со процесот на верификација, Субјектот мора да даде негова експлицитна согласност во однос на употребата, евидентирањето и складирањето на процесот на далечинска верификација на идентитетот, фотографирањето на лицето на Субјектот, методот на верификација кој овозможува сигурност еднаква на физичко присуство, документите за идентификација и евентуално друг потребен материјал.

5.3.4. Доколку во процесот на далечинска верификација на идентитетот се појави трето лице, освен Субјектот, сесијата ќе се прекине, сите снимени податоци ќе се избришат и процесот ќе се повтори, под услов да не се појават трети лица.

5.3.5. Системот за далечинска автентикација на KIBSTrust или овластениот вработен веднаш ќе го прекине процесот на далечинска верификација на идентитетот:

- Кога документот за идентификација не е соодветен или предизвикува сомнеж во врска со автентичноста и сигурноста; или
- Кога Субјектот несоодветно се однесува кон автоматскиот процес за далечинска автентикација или кон овластениот вработен на КИБС, или постојат индикации дека Субјектот е под притисок, има психолошко или ментално нарушување или злоупотребува супстанци. Во овие случаи, процесот не може да се повтори и Субјектот мора да избере еден од другите методи на верификација на идентитетот, наведен во став 1.4.
- Кога Субјектот е деловно неспособно лице.

5.3.6. Субјектот треба да достави до KIBSTrust согласност во која детално ќе ги наведе своите лични информации и неговата намера да продолжи со издавањето квалификуван сертификат.

5.4. До онаа мера до која е дозволено со применливиот закон, претплатниците треба да го обештетат КИБС за:

5.4.1. Лажно и погрешно прикажување на факт од страна на Субјектот во образецот за нарачка и договор за издавање сертификат.

5.4.2. Пропуст на Субјектот да наведе материјален факт во образецот за нарачка и договор, доколку погрешното прикажување или пропуст е направено поради небрежност или со намера да измами некоја страна.

5.4.3. Неуспех на Субјектот да го заштити својот приватен клуч, да користи сигурен систем или на друг начин да преземе мерки на претпазливост за да се спречи компромитирање, губење, откривање, модификација или неовластена употреба на приватниот клуч на Субјектот.

5.4.4. Користење име од страна на Субјектот што ги прекршува правата на интелектуална сопственост на трето лице.

6. Права на давателот на услугата OneID

6.1. Без оглед на Дел 8, KIBSTrust треба да ги обезбеди услугите во согласност со Практиката, CP/CPS за квалификувани електронски потписи и електронски печати, CP/CPS на Издавачот на временски жиг KIBSTrust, како и со соодветното законодавство.

7. Обврски на засегнатите страни

7.1. Засегнатата страна ги проучува ризиците и одговорностите поврзани со прифаќањето на средството за електронска идентификација, а со тоа и на квалификуваниот сертификат. Ризиците и одговорностите се наведени во Практиката. Засегнатата страна потврдува дека има пристап до доволно информации за да може да донесе одлука за степенот до кој ќе избере да се потпре на информациите од средството за електронска идентификација. ЗАСЕГНАТАТА СТРАНА Е ОДГОВОРНА ЗА ОДЛУКАТА ДАЛИ ДА СЕ ПОТПРЕ ИЛИ НЕ, НА ИНФОРМАЦИИТЕ СОДРЖАНИ ВО КВАЛИФИКУВАНИОТ СЕРТИФИКАТ.

7.2. Засегнатата страна потврдува и се согласува дека нејзиното користење на складиштето на KIBSTrust, достапно на https://www.kibstrust.com/repository, и нејзиното потпирање на квалификуваниот сертификат како дел од средството за електронска идентификација ќе биде регулирано со применливата Практика која може повремено да се менува.

7.3. Доколку не се приложени доволно докази кон сертификатот за електронски потпис во врска со валидноста на сертификатот, засегнатата страна ја потврдува валидноста или поништувањето на квалификуваниот сертификат со користење информации за тековниот статус за поништување, врз база на услугите за валидација на сертификатот понудени од KIBSTrust, креиран со приватен клуч којшто соодветствува на јавниот клуч содржан во квалификуваниот сертификат, врз основа на услугите за проверка на сертификати кои ги нуди KIBSTrust во периодот на користење на сертификатот или со ставање на квалификуван електронски потпис или квалификуван електронски печат. Методот со кој може да се провери статусот на сертификатот е со проверка во регистар на

поништени сертификати од Издавачот на сертификати (CRL) кој го издал сертификатот на кој засегнатата страна сака да се потпре или со користење на информации преку протоколот за електронско добивање статус на сертификатот (OCSP).

7.4. Засегнатата страна треба да ги земе предвид сите ограничувања наведени во кој било сертификат, издаден од KIBSTrust и да обезбеди дека трансакцијата што треба да се прифати е во согласност со соодветните CP/CPS.

7.4.1. Квалификувани сертификати се користат само до онаа мера до која употребата е во согласност со важечкиот закон. Квалификуваните сертификати не се дизајнирани, наменети или одобрени за употреба или препродажба како контролна опрема во опасни околности или за употреба што бара безбедно извршување, како што е работење на нуклеарни постројки, воздухопловни навигациски системи или системи за комуникација, системи за контрола на воздушниот сообраќај или системи за контрола на оружје, каде што дефект може да доведе директно до смрт, лична повреда или сериозно оштетување на животната средина.

7.4.2. KIBSTrust обезбедува достапност на услугите за статусот на сертификатот 24 часа на ден, 7 дена во неделата со севкупна достапност од минимум 99% годишно, со планиран прекин што не надминува 0,4% годишно.

7.4.3. Засегнатата страна ја потврдува валидноста на сертификатот со проверка на валидноста на истиот користејќи информации од услугите за проверка OCSP и CRL достапни преку линковите дадени во сертификатот. Услугата OCSP е достапна преку HTTP протокол и е јавно достапна на http://ocsp2.kibstrust.com/.

7.4.4. Од засегнатите страни се очекува да го користат регистарот на даватели на квалификувани доверливи услуги на Министерството за информатичко општество и администрација во Република Северна Македонија за да утврдат дали електронскиот потпис, печат или временски жиг се квалификувани (https://trusteid.mioa.gov.mk/registar_listi/).

8. Ограничена гаранција и ограничување на одговорноста

8.1. KIBSTrust е одговорен за извршувањето на својата услуга за електронска идентификација, како што е наведено во неговата Практика и овие Правила и услови.

8.2. KIBSTrust е одговорен за извршувањето на своите доверливи услуги, како што е наведено во неговите CP/CPS, за квалификувани електронски потписи.

8.3. КИБС гарантира дека има договори за задолжително осигурување што ги покриваат сите доверливи услуги и услуга на електронска идентификација на KIBSTrust за да се обезбеди надомест на штета предизвикана од прекршување на обврските на KIBSTrust.

8.4. KIBSTrust ги информира сите претплатници и Субјекти за електронска идентификација пред да престане со вршење на дејност поврзана со услугата на електронска идентификација и услуги на издавање на сертификати и ја одржува документацијата поврзана со прекинатите услуги на издавање на сертификати и потребните информации во согласност со процесот утврден во CP/CPS.

8.5. КИБС не е одговорен за:

8.5.1. тајноста на податоците за пристап до приватни клучеви (корисничко име, лозинка, биометрија) кога се наоѓаат на далечинско QSCD, за можно губење или оштетување на мобилниот уред што се користи за автентикација на корисникот.

8.5.2. неправилната употреба на сертификат од страна на Субјектот или каква било злоупотреба на сертификатот или несоодветна проверка на сертификатот или за погрешни одлуки на Субјектот или засегнатата страна или какви било последици поради грешка или пропуст од страна на Субјектот или грешка или пропуст при проверките на валидноста на сертификатот.

8.5.3. фалсификуван електронски потпис на документ, индикативно поради украден или компромитиран приватен клуч на корисникот.

8.5.4. неисполнувањето на своите обврски, доколку таквото неисполнување се должи на грешки или безбедносни проблеми на надзорниот орган, недостапност на доверливиот извор на податоци како што се Централниот регистар на население, регистарот на даватели на

квалификувани доверливи услуги и шеми за електронска идентификација на Министерството за информатичко општество и администрација во Република Северна Македонија или кој било друг приватен правен субјект или јавен орган.

8.5.5. работата на софтверот или другите апликации обезбедени од трети лица кои не се поврзани со KIBSTrust.

8.5.6. неисполнувањето на обврските, доколку таквото неисполнување се должи на настан на виша сила.

8.6. Како што е наведено во соодветните CP/CPS, КИБС дава ограничени гаранции и ги одрекува сите други гаранции, вклучително и гаранциите за соодветност за пласирање на пазарот или соодветност за одредена намена, ја ограничува одговорноста и ја исклучува целата одговорност, освен во случај на намерно несоодветно однесување или груба небрежност, за каква било загуба на добивка, загуба на податоци или други индиректни, последователни или казнени штети што произлегуваат од или во врска со користењето, испораката, лиценцирањето, извршувањето, неизвршувањето или компромитирањето на сертификати за електронски потписи, електронски печати, временски жигови или кои било други трансакции или услуги што се нудат или се разгледуваат овде, дури и ако KIBSTrust е известен за можноста од настанување на такви штети. Вкупната одговорност на КИБС кон сите страни вклучувајќи го и Субјектот, во никој случај нема да ја надмине соодветната граница на одговорност за таквиот квалификуван сертификат наведен подолу:

8.6.1. комбинираната вкупна одговорност на КИБС кон кое било и сите лица во врска со определен квалификуван сертификат е ограничена на износ што не надминува петстотини (500) евра по сертификат и вкупни максимални побарувања од педесет илјади (50.000) евра за квалификувана услуга, без оглед на природата на одговорност и видот, износот или степенот на претрпената штета. Ограничувањата на одговорноста предвидени во овој став се исти без оглед на бројот на сертификати за квалификувани потписи / печати, трансакции или побарувања во врска со таквиот сертификат.

8.6.2. ограничувањата на одговорноста, предвидени овде, ќе се применуваат до максимално дозволениот степен според важечкиот закон на важечката јурисдикција.

8.7. Субјектите и засегнатите страни се известуваат за можноста за кражба или друга форма на компромитирање на приватен клуч што соодветствува на јавен клуч, содржан во квалификуваниот сертификат, што може или не може да се открие, и за можноста за употреба на украден или компромитиран клуч за да се фалсификува квалификуван електронски потпис или квалификуван електронски печат на документ.

8.8. KIBSTrust може да го прекине процесот на валидација, доколку се утврди или се сомнева дека неточна или лажна информација е обезбедена од Субјектот или ако проверката на идентитетот на Субјектот не е успешна. Без оглед на став 8.5, КИБС не е одговорен на кој било начин за автентичноста или веродостојноста на документите за идентификација доставени од Субјектот, ниту за каква било штета што може да му биде предизвикана на Субјектот или на трети лица.

9. Применливи поврзани договори, политики и практики

Релевантни договори, политики и изјави за практики во врска со сегашните Правила и услови:

9.1. CP/CPS на КИБС за квалификувани сертификати за електронски потписи и електронски печати.

9.2. Профили на сертификати и OCSP за квалификувани електронски потписи и квалификувани електронски печати, и конкретно:

- Политика за ЕУ квалификувани сертификати издадени на физички лица (OID 0.4.0.194112.1.0), **QCP-n**.
- Политика за ЕУ квалификуван сертификат издаден на физичко лице каде приватниот клуч и поврзаниот сертификат се наоѓаат на QSCD (OID 0.4.0.194112.1.2), **QCP-n-QSCD**.

9.3. Политика за приватност (KIBSTrust).

9.4. Тековните верзии на сите горенаведени документи се јавно достапни во складиштето на КИБС https://www.kibstrust.com/repository.

10. Политика за приватност и доверливост

10.1. КИБС ги обработува личните податоци според Политиката за приватност (KIBSTrust) достапна во складиштето на https://www.kibstrust.com/repository и согласно сите законски прописи на Република Северна Македонија.

10.2. Сите информации кои станале познати при обезбедувањето на услугите и кои не се наменети за објавување (на пр. информации кои му биле познати на KIBSTrust како резултат на работењето и обезбедувањето на доверливите услуги) се доверливи. Субјектот има право да добие информации од KIBSTrust за тоа кои податоци за него се чуваат / обработуваат во согласност со закон.

10.3. KIBSTrust ги заштитува доверливите информации и информациите наменети за внатрешна употреба од нивно компромитирање и се воздржува од нивно откривање на трети страни со спроведување различни безбедносни контроли.

10.4. Во согласност со релевантните закони и законски акти, KIBSTrust има право да ги открие информациите за Субјектот или субјектот на трета страна која има право да ги добие таквите информации и под услов откривањето да е законско, во согласност со националните прописи и прописите на ЕУ за заштита на податоци.

10.5. Покрај тоа, статистичките податоци за услугите на KIBSTrust кои не се персонализирани, исто така, се сметаат за јавни информации. КИБС може да објавува статистички податоци за своите услуги кои не се персонализирани.

11. Достапност за лица со посебни потреби

11.1. Издавањето на средство за електронска идентификација вклучува процеси на правење онлајн активности вклучително идентификација на далечина.

11.2. Активностите кои се спроведат online возможно е да се спроведат и со лица со посебни потреби, доколку нивните работни станици, паметни мобилни уреди со посебно креирани алатки кои барањата кои треба да ги исполни лицето со посебни потреби ќе ги направи разбирливи за него.

11.3. Доколку извршување на нарачката онлајн не е можно, лицата со посебни потреби можат да дојдат во просториите на РК/ЛРК на KIBSTrust. Пристапот до канцеларијата на РК/ЛРК на KIBSTrust е без бариери. Информациите за непречен пристап до ЛРК се јасно прикажани на веб-страницата https://www.kibstrust.com. Покрај тоа, KIBSTrust на барање на лице со посебни потреби нуди услуга за помош од дома.

11.4. За лицата со посебни потреби кога истите ќе пристигнат во РК, процедурата за издавање на средство за електронска идентификација може да биде спроведена со помош на вработени на КИБС. Во секој случај, лицата со посебни потреби пожелно е да бидат придружени од лица кои ги разбираат потребите и стекнале доверба од лицето со посебни потреби за да го забрзаат процесот на издавање на средство за електронска идентификација .

11.5. Употребата на средството за електронска идентификација за лица со посебни потреби зависи од тоа како нивните работни станици, паметни мобилни уреди, оперативни системи и апликативен софтвер се прилагодени за нивните посебни потреби.

12. Политика за поврат на средства

12.1. KIBSTrust прави напори да обезбеди највисок степен на квалитет на своите услуги. Сепак треба да се има предвид следново:

12.1.1. Услугата за електронска идентификација може да биде наплатена од Субјектот.

12.1.2. Субјектот во рок од пет (5) дена од денот на активирањето на сертификатот, може да поднесе рекламација за услугата која ја добил во случај на невалидно функционирање, несовпаѓање на описот на услугата со дадениот опис, намената и употребата што се декларирани и објавени од страна на KIBSTrust.

12.1.3. KIBSTrust нема да прифати никакви побарувања за неправилно користење на услугата или штети предизвикани по вина или дејствија на Субјектот.

12.1.4. Субјектот има право да се повлече од онлајн подготвената процедура за создавање на средство за електронска идентификација пред активирањето на услугата. Доколку Субјектот не ја заврши процедурата на процесот на издавање средство за електронска идентификација ќе биде автоматски отфрлен од системот.

13. Применлив закон, жалби и механизам за решавање на спорови

13.1. Сите спорови во врска со доверливите услуги кои се обезбедуваат во согласност со овие Правила и услови се регулираат во секој поглед и се толкуваат во согласност со законите на Република Северна Македонија.

13.2. До онаа мера која е дозволена со закон, пред да може да се употреби било каков механизам за решавање спорови во поглед на одреден спор којшто се однесува на кој било аспект на доверливите услуги на KIBSTrust, Субјектот или која било друга страна во спорот мора да ги извести KIBSTrust и сите други страни инволвирани во спорот за сите евентуални побарувања или жалби најдоцна во рок од триесет (30) календарски дена по откривањето на основата за побарувањето, освен ако не е поинаку предвидено со закон. Доколку спорот не биде решен во рок од шеесет (60) дена по првичното известување, страната може да побара правно решавање. Сите страни се согласни дека судовите на Република Северна Македонија ќе бидат исклучиво надлежни за сослушување и решавање на кој било спор во врска со толкувањето и спроведувањето на овие Правила и обезбедувањето на услугите на KIBSTrust.

13.3. Субјектот или која било друга страна може да го поднесе своето побарување или жалба на следнава адреса за е-пошта: helpdesk@kibstrust.com.

13.4. Сите барања за спор треба да се испратат на контактот за информации наведен во овие Правила и услови.

14. Ревизија и оценување на сообразност

14.1. KIBSTrust е давател на квалификувани доверливи услуги и на шема за електронска идентификација. Претходниот статус му е доделен од страна на надзорно тело, по поднесувањето на извештај за оценување на сообразноста од страна на акредитирано тело за оценување на сообразноста согласно 14.3 и 14.4.

14.2. Доверливите услуги и шемата за електронска идентификција се регистрирани во Регистарот на даватели на доверливи услуги и шеми за електронска идентификција на Министерството за информатичко општество и администрација во Република Северна Македонија. Предуслов за таквата регистрација е усогласеност со применливите прописи и стандарди во државата, на светско и европско ниво.

14.3. Телото за оценување на сообразноста е акредитирано во согласност со Регулативата (ЕЗ) бр. 765/2008 како надлежно за оценување на сообразноста на давателот на квалификувани доверливи услуги и на квалификуваните доверливи услуги кои тој ги обезбедува.

14.4. Шема за акредитација во обем: ISO / IEC 17065 + ETSI EN 319 403 + eIDAS Art.3.18.

14.5. Заклучоците од ревизијата или извештаите кои се базираат на резултатите од ревизија на оценувањето на сообразноста, извршено во согласност со Регулативата eIDAS, како и соодветните закони и стандарди се објавени во складиштето на КИБС на страницата https://www.kibstrust.com/repository.

15. Контакт информации

15.1. Давател на квалификувани доверливи услуги:

КИБС АД (KIBSTrust)

бул. "Кузман Јосифовски Питу" 1,
+389 2 5513 444, +389 2 3297 444
https://www.kibstrust.com
helpdesk@kibstrust.com
1000 Скопје, Република Северна Македонија
(понеделник - петок 8.30 - 16.00 централно европско време)

15.2. Барањата за прашања со животниот циклус на средството за електронска идентификација се примаат од 08.30 до 16.00 (UTC +2) 8/5 лично во РК, или преку е-порака на oneid@kibstrust.com.

15.3. Информациите на веб-страницата и контакт податоците за услужниот веб-портал се достапни на https://www.oneid.mk, https://www.kibstrust.com.

16. Важност на Правилата и условите

16.1. Овие Правила и услови се утврдени во македонска и англиска верзија. Во случај на какви било несогласувања помеѓу овие верзии, македонската верзија ќе преовлада.

16.2. Се што не е наведено во овие Правила и услови или е во колизија со одредби од Практиката, важат одредбите од Практиката.

16.3. Доколку се утврди дека која било одредба од овие Правила и услови, или нејзината примена е невалидна или неприменлива поради која било причина и во која било мера, останатите одредби (како и примената на невалидната или неприменливата одредба на други лица или околности) нема да бидат засегнати од таквото откривање на невалидност или неприменливост, и ќе се толкуваат на начин на којшто разумно ќе се спроведе намерата на страните.

17. Дефиниции и кратенки

Поим/кратенка	Дефиниција
Издавач на сертификати (ИС)	Дел од компанијата КИБС одговорен за издавање и верификување сертификати и листи на поништени сертификати со својот електронски потпис.
Сертификат	Јавен клуч заедно со дополнителни информации, наведени во профилот на сертификатот, чиешто фалсификување е оневозможено преку шифрирање со користење на приватниот клуч на издавачот на сертификатот кој го издал .
Политика за сертификати (CP)	Именуван пакет правила што укажува на применливост на сертификат за одредена заедница и / или класа на примена со заеднички безбедносни барања.
Правила за издавање квалификувани сертификати (CPS)	Правила за постапките што ги користи издавачот на сертификати при издавање, управување, поништување и обновување сертификат или обновување сертификат со нов пар клучеви.
Регистар на поништени сертификати (CRL)	Потпишана листа каде е наведена групата на сертификати што се поништени од издавачот на сертификати.
eIDAS Регулатива	Регулатива (ЕУ) бр. 910/2014 на Европскиот Парламент и на Советот од 23 јули 2014 година за електронска идентификација и доверливи услуги за електронски трансакции на внатрешниот пазар и за укинување на Директивата 1999/93/ЕЗ.
Верификација / валидација на идентитет	Единствена идентификација на лице преку проверка на неговиот/нејзиниот наводен идентитет.
MK-eIDAS	Закон за електронски документи, електронска идентификација и доверливи услуги, (Службен весник на Република Северна Македонија, бр. 101/19....215/19).
КИБС	КИБС А.Д. Скопје
OCSP	Протокол за електронско добивање статус на сертификат.
OID	Идентификатор кој се користи за еднозначно именување на одреден објект.
PIN код	Активациски код за Квалификувани сертификати за електронски потписи и електронски печати.
Приватен клуч	Клуч од парот клучеви за кој се претпоставува дека се чува во тајност од страна на сопственикот на парот клучеви, а кој се користи за креирање електронски потписи и/или за дешифрирање на електронски записи или датотеки кои биле шифрирани со соодветниот јавен клуч.
Јавен клуч	Клуч од парот клучеви кој може јавно да бидат објавен од страна на сопственикот на соодветниот приватен клуч кој се користи од засегнатите страни за потврда на електронските потписи, креирани со помош на соодветниот приватен клуч на сопственикот и/или за шифрирање пораки кои можат да бидат дешифрирани само со помош на приватниот клуч на сопственикот.
Квалификуван сертификат	Квалификуван сертификат е сертификат кој го издава ИС, кој е акредитиран и надгледуван од страна на надзорно тело назначено од државата и кој ги исполнува барањата на Законот за електронски документи, електронска идентификација и доверливи услуги, и eIDAS.
Квалификуван електронски потпис	Напреден електронски потпис кој е креиран од средство за креирање квалификуван електронски потпис и кој се заснова на квалификуван сертификат за електронски потпис.
Квалификуван електронски печат	Напреден електронски печат кој е креиран од средство за креирање квалификуван електронски печат и кој се заснова на квалификуван сертификат за електронски печат.

Квалификуван електронски временски жиг	Податоци во електронска форма што поврзуваат други податоци во електронска форма со одредено време за утврдување доказ дека тие постоеле во тоа време, на начин на којшто е исклучена можноста за промена на податоците. Се базира на точен извор на време поврзан со UTC и се потпишува со користење напреден електронски потпис или напреден електронски печат на давателот на квалификувана доверлива услуга.
Средство за креирање квалификуван потпис/печат (QSCD)	Безбедно средство за креирање квалификуван електронски потпис / печат што ги исполнува барањата утврдени во делот II од eIDAS Регулативата. QSCD може да биде локално во форма на USB токен или смарт картичка или далечинско во форма на хардверски сигурносен модул.
Квалификувани доверливи услуги	Доверлива услуга, како што е дефинирана во eIDAS што ги задоволува применливите барања утврдени во оваа Регулатива.
Давател на квалификувани доверливи услуги	Давател на доверливи услуги кој обезбедува една или повеќе квалификувани доверливи услуги и има добиено квалификуван статус од страна на надзорното тело.
Засегната страна	Физичко или правно лице кое се потпира на информациите наведени во сертификатот.
Далечинска верификација на идентитет	Метод/процес со кој Субјектот е идентификуван преку видео конференција и е еквивалентен на верификацијата на идентитетот со физичко присуство.
Субјект	Субјектот може да биде: а) физичко лице. б) физичко лице за кое е утврдено дека е поврзано со правно лице. в) правно лице (кое може да биде организација или единица или оддел за кои е утврдено дека се поврзани со одредена организација).

КРАЈ НА ДОКУМЕНТОТ