Политика за доверлива услуга
за создавање на електронски потписи

Верзија: 1.0

Датум на стапување во сила: 09.11.2021

Ознака: 111.15

КИБС АД Скопје

https://www.kibstrust.com/

Белешка за трговската марка

КИБС, KIBSTrust, SignPlus и Momentum се регистрирани марки на КИБС АД Скопје. Другите имиња кои се спомнуваат во документот, може да бидат трговски марки на други сопственици. Давателот на доверливи услуги организациски претставува дел од КИБС, но настапува под брендот со име **KIBSTrust**, па терминот „Давател на доверливи услуги КИБС“ се поистоветува со „KIBSTrust“.

Содржина

1. ВОВЕД

Неколку аспекти се важни за да се обезбеди доверба во електронските потписи. Нивната успешна имплементација во електронските процеси бара примена на стандарди за применетите услуги, процеси, системи и производи, како и проценка за усогласеност на таквите услуги, процеси, системи и производи.

Законот за електронски документи, електронска идентификација и доверливи услуги[1] (во понатамошниот текст МК-eIDAS) ги дефинира поимите електронски потпис, напреден електронски потпис, квалификуван електронски потпис, електронски печат, напреден електронски печат и квалификуван електронски печат, коишто се во согласност со ЕУ Регулативата бр. 910/2014[2] (во понатамошниот текст eIDAS).

Овие електронски потписи и печати може да се креираат со употреба на технологија за дигитален потпис.

Кога не е поинаку наведено во овој документ, „потпис“ означува „дигитален потпис[3]“.

1.1. Преглед

Овој документ (во понатамошниот текст: Политика) се концентрира на барањата за политики и безбедност што треба да се земат предвид при создавањето на потписот на доверлив начин, особено во контекст на апликациите за создавање на потпис, валидација на потпис и зголемување на потписот. Дефиниција за употребените термини може да се види во точка 1.6.

Документот опфаќа:

- општи барања,
- правна политика,
- безбедност на информации (систем за управување),
- процес на создавање потпис и зголемување на потписот,
- политика за развој и кодирање.

Овој документ ги дефинира општите барања за безбедност и политики за апликации за создавање и валидација на потпис, согласно стандардот ETSI TS 119 101: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation".

Процедурите за создавање и валидација на напредни дигитални потписи се согласно стандардот ETSI TS 119 102-1: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

Барања за даватели на доверливи услуги при обезбедување на компонентите за создавање напредни потписи се дефинираат во стандардот ETSI TS 119 431-2: „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation".

Сигурносните барања за компонентите за далечинско создавање потпис се дефинирани во стандардот ETSI TS 119 431-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev".

Барања за даватели на доверливи услуги кои обезбедуваат услуги за валидација на потпис се дефинирани во стандардот ETSI TS 119 441: "Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services".

---

[1] Закон за електронски документи, електронска идентификација и доверливи услуги (Службен весник на Република Северна Македонија 101/19, 215/19)

2 Регулатива (ЕУ) 910/2014 на Европскиот парламент и на Советот од 23 јули 2014 за електронска идентификација и доверливи услуги за електронски трансакции на внатрешниот пазар и укинување на Директивата 1999/93/ЕЗ (eIDAS)

[3] Иако со МК-eIDAS се дефинира електронски потпис, терминот дигитален потпис, како вид на електронски потпис, е глобално прифатен кога станува збор за потпис креиран со електронски сертификат издаден во PKI инфраструктура.

Општите барања за системите кои поддржуваат серверско потпишување се дефинирани со стандардот CEN EN 419 241-1: "Trustworthy Systems Supporting Server Signing; Part 1: General System Security Requirements".

Општите барања за даватели на доверливи услуги се дадени во стандардот ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers ".

Општи барања за политика и сигурност за давателите на доверливи услуги кои издаваат сертификати се дефинирани во стандардот ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

1.2. Домен на деловна активност и примена

1.2.1. Опсег и граници

Различните учесници и различниот контекст на создавање, валидација и зголемување на потписите следат одредени правилата коишто овозможуваат учесниците меѓусебно си веруваат.

Овој документ е првенствено релевантен за следниве учесници:

- Корисници на апликацијата за создавање потпис, валидација на потпис и/или зголемување на потпис, кои треба да се сигурни дека се покриени сите релевантни барања.
- Учесници кои ги интегрираат апликациите, односно компонентите за создавање потпис, валидација на потпис и/или зголемување на потписот со нивниот софтвер за деловни процеси (или користат самостоен софтвер), кои сакаат да обезбедат правилно функционирање на целокупниот процес на создавање/валидација/зголемување на потписот и дека создавањето/валидацијата на потписот се прави во доволно безбедна средина.
- Оценувачи (самоевалуација или евалуација од трета страна) за да имаат листа на критериуми според кои ќе се провери проверката.

Корисници на апликацијата можат да бидат физички или правни лица кои за своите активности/деловно работење имаат потреба од електронско потпишување на документи и нивно комуницирање со засегнатите страни (клиенти, партнери, добавувачи и т.н.).

Учесници кои ги интегрираат апликациите за создавање потпис во своите решенија за електронски услуги се правни лица кои имаат договорна обврска со КИБС за употреба на апликативните интерфејси за создавање потписи.

Корисниците на апликацијата може да бидат регистрирани корисници со своја/свои кориснички сметки и не-регистрирани корисници кои добиваат можност електронски да потпишат документи испратени од регистриран корисник.

1.2.2. Домен на примени

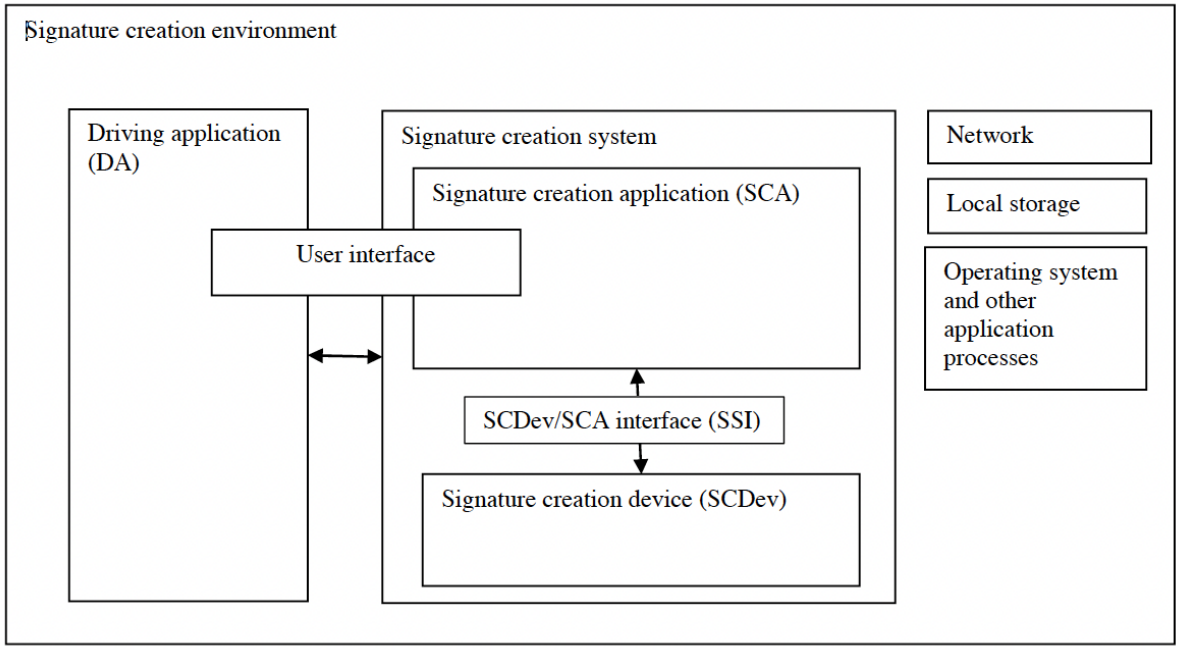
Примената се однесува на апликации за создавање потпис, валидација на потпис и/или зголемување на потпис, односно имплементација и обезбедување на модулите за:

- апликација за создавање потпис (SCA - signature creation application),
- апликација за валидација на потпис (SVA – signature validation application),
- апликација за зголемување потпис (SAA - signature augmentation application),
- движечка апликација (DA - driving application),
- комуникацијата помеѓу SCA и уредот за создавање потпис (SCDev - signature creation device) и околината во која се користат SCA/SVA/SAA.

Исто така, се специфицираат барањата за корисничкиот интерфејс кој може да биде дел од SCA/SVA/SAA или од DA која ги повикува SCA/SVA/SAA. Секој ентитет којшто ги користи SCA/SVA/SAA компонентите во неговиот деловен процес делува како DA движечка апликација.

KIBSTrust како давател на доверливи услуги ја има регистрирано услугата за создавање на електронски потписи во Регистарот на доверливи услуги при МИОа и за таа намена има поставено апликации за создавање потписи и за зголемување на потписи коишто се достапни за регистрираните корисници преку апликативни програмски интерфејси (API) и движечка апликација достапна преку интернет прелистувач на https://www.signplus.mk. Исто така во рамки на доверливата услуга за издавање на временски печати, достапна е независна движечка апликација за зголемување на потписи како дел од www.momentum.mk. Третите страни со кои KIBSTrust има договорни аранжмани поставуваат за своите клиенти движечки апликации кои се поврзани со SCA и SAA на KIBSTrust.

Околината за функционирање на услугата за создавање на електронски потписи се состои од неколку поврзани дела како што е претставено на сликата.



Слика 1. Основен модел на околина за создавање на потписи

Околината за создавање потпис опфаќа користење на DA, SCA и SCDev, мрежа, простор за складирање податоци и други информациони системи. Движечката апликација (DA) обезбедува влез во апликацијата за создавање потпис и го прима излезот. Корисничкиот интерфејс може да биде (делумно) дел од DA и/или (делумно) дел од SCA. Апликацијата за создавање потпис (SCA) го подготвува документот што треба да се потпише и го создава потпишаниот податочен објект од вредноста на дигиталниот потпис добиен од уредот за создавање потпис (SCDev). Вредноста на дигиталниот потпис се креира со помош на податоците за создавање потпис на корисникот. SCA комуницира со SCDev користејќи интерфејс (SSI).

Овој модел му овозможува на корисникот да комуницира и со движечката апликација и со апликацијата за создавање потписи.

1.2.3. Трансакциски контекст

Примената на SCA или DA може да биде во контекст на различни деловни барања, како на пример:

- Договори, нацрт договори, договори за необјавување;

- Понуди, предлози за соработка
- Потврди (на пр. за прием, испорака, испраќање итн.);
- Овластувања, одобренија и друго.

1.3. Дистрибутивни точки на политиката

Овиа Политика и придружните документи на KIBSTrust се објавени во складиштето за јавно информирање на: https://pki.kibstrust.com/repository. Документите на KIBSTrust се објавуваат заедно со датумите на применување не порано од 10 дена пред нивно стапување во сила.

1.4. Издавач на Политиката

Оваа Политика ја издава давател на доверливи услуги KIBSTrust, којшто функционира како организациски дел во рамките на организацијата КИБС АД Скопје.

Политиката се донесува и потпишува од страна на генералниот директор на КИБС АД со квалификуван дигитален сертификат за електронски потпис.

1.5. Администрација на Политиката

1.5.1. Организација која го управува документот

Оваа Политика и релевантните документи што се наведени овде ги изготвува, регистрира, одржува и ажурира Одбор за управување со политиките (ОУП[4]) на KIBSTrust, којшто може да се контактира на:

КИБС АД Скопје
Кузман Јосифовски Питу 1
1000, Скопје, Република Северна Македонија
е-пошта: pma@kibstrust.com

1.5.2. Лице за контакт

За сите прашања поврзани со оваа Политика може да биде контактиран ОУП преку:
Менаџер за PKI политики на KIBSTrust
е-пошта: pma@kibstrust.com
тел. +389 2 5513401, +389 2 3297401

1.6. Дефиниции и акроними

1.6.1. Дефиниции

За дефиниции на некои користени термин во оваа Политика видете во прилогот на крајот на документот.

1.6.2. Акроними

Кратенка	Опис
CA (ИС)	Certificate Authority (Издавач на сертификати)
CP	Certificate Policy (Политика за сертификати)
CPS	Certification Practice Statement (Постапки/Практика за издавање на сертификати)
CRL	Certificate Revocation List (Регистар на поништени сертификати)
DA	Driver Application
OCSP	Online Certificate Status Protocol (Протокол за електронско добивање на статусот на сертификат)

[4] Анг. Policy Management Authority (PMA)

OID	Object Identifier (Предметен идентификатор, единствен код на предметен идентификатор)
OTP	One Time Password (Еднократна лозинка)
PIN (ПИН)	Персонален идентификациски број
PKI	Public Key Infrastructure (Инфраструктура на јавен клуч)
PMA	Policy Management Authority
QSCD	Qualified Signature Creation Device (Средство за создавање квалификуван електронски потпис/печат)
RA (РК)	Registration Authority (Регистрациона канцеларија)
RFC	Request for Comment (Барање за забелешка)
SSL	Протокол Secure Socket Layer
TSP	Trusted Services Provider
SCA	Signature Creation Application (Апликација за создавање на потпис)
SVA	Signature Validation Application (Апликација аз валидирање на потпис)
SAA	Signature Augmentation Application (Апликација за зголемување на потпис)
SCDev	Signature Creation Device (Уред за создавање на потпис)
TSA	Time-Stamp Authority (Издавач на временски печати)
ДДУ	Давател на доверливи услуги
ОУП	Одбор за управување со политики

2. Создавање на електронски потпис

2.1. Општи барања

2.1.1. Кориснички интерфејс

Корисничкиот интерфејс може да биде дел од SCA/SVA/SAA или DA што го повикува SCA/SVA/SAA.

Со цел да се обезбеди доверба кај корисникот и да се избегнат какви било проблеми и недоразбирања во интеракција со апликацијата едно од предусловите е добро дизајниран и лесен за употреба кориснички интерфејс.

Корисничкиот интерфејс му обезбедува на корисникот:

- недвосмислени упатства за тоа како да се користи SCA/SVA/SAA и, доколку е применливо, да се инсталираат и конфигурираат компонентите на системот;
- Опис на секој чекор од дијалогот, лесно разбирлив и со повратни информации од системот;
- толерантност кон грешки ако, и покрај очигледните грешки во внесувањето, посакуваниот резултат може да се постигне со минимална корекција;
- информативно известување за грешки за да го води корисникот напред кон следната акција;
- повратна информација за да потврди дека дејството извршено од корисникот е точно (или неточно);

- можност во секое време да ја откаже тековната операција и да се врати на главното мени; или да излезе од системот целосно;
- заштита на приватноста за податоците на поединецот; и
- давање на потврда за клучните одлуки и избори на корисникот.

SCA/SVA/SAA обезбедува детален кориснички водич (wiki help) што ги води корисниците низ процесот на создавање и валидација на потпис.

Целта е на корисникот да му се обезбеди доволно информации за да го разбере процесот на создавање и валидација на потпис.

2.1.2. Општи безбедносни мерки

Системите на кои е развиена апликацијата применуваат соодветни безбедносни мерки и се прилагодуваат на специфичните апликациски околини.

Применети се следните општи безбедносни мерки (ОБМ):

ОБМ 1: Соодветни безбедносни мерки:

ОБМ 1.1: Мерките за безбедност за системите на кои се развива апликацијата се согласно применетиот стандард за управување со сигурност на информации во КИБС, ISO/IEC 27002 или врз основа на детална анализа на ризик.

ОБМ 1.2: Се користи најновата околина за апликации (управувани софтверски средини), вклучително и најнови безбедносни поправки и закрпи.

ОБМ 1.3: Се имплементираат добро тестирани и прегледани стандардизирани протоколи и библиотеки.

ОБМ 1.4: Се користат криптографски библиотеки тестирани според соодветниот стандард.

ОБМ 1.5: ОБМ 1.5: Доколку е применливо, се имплементира анти-вирусна и заштита од малициозен софтвер (вклучително и за деловите на апликацијата што може да се преземат).

ОБМ 1.6: Доколку е можно или потребно ќе се користи и лична мрежна бариера (personal firewall).

ОБМ 2: Специфични апликативни околини:

ОБМ 2.1: Кога SCA, SVA или SAA се испорачуваат како софтверски пакет, тој треба да биде дигитално потпишан.

ОБМ 2.2: Кога доставениот код или дел од него е дигитално потпишан, ова се прави со сертификат за потпишување на код обезбеден од признат издавач на сертификати и потписот содржи временски печат од признат издавач на временски печати.

ОБМ 2.3: DA треба да одржува интегритет и доверливост на сите информации доставени од корисникот и на сите податоци што течат помеѓу апликацијата и корисникот, дури и во случај на апликација поставена во јавна околина.

ОБМ 2.4: SCA/SVA/SAA го одржува интегритетот и доверливоста на сите информации доставени од корисникот и сите податоци што течат помеѓу апликацијата и корисникот, дури и во случај на јавна околина за апликација.

ОБМ 2.5: Податоците за автентикација на потписникот ќе бидат безбедно избришани на крајот на сесијата од страна на апликацијата за да се избегне каков било напад со повторување од други корисници.

ОБМ 2.6: Доколку апликацијата ја користат различни корисници, тогаш апликацијата ќе се погрижи сите податоци поврзани со процесот на потпис да бидат избришани од јавните достапни области (вклучувајќи чување во меморија (cash), или меморирање на сертификати) откако го заврши потпишувањето. Апликацијата нема да ги копира овие елементи на која било страна без овластување од корисникот.

ОБМ 3: Информирање на корисникот за препорачаните сигурносни мерки

ОБМ 3.1: SCA/SVA/SAA го информира корисникот за најдобрите практики за заштитата на персоналните компјутери (анти-вирус, личен заштитен sид, итн.). Соодветните информации може да бидат дел од документацијата за SCA/SVA/SAA.

2.1.3. Комплетност на системот

Системот во целост ги спроведува сите задолжителни барања, вклучително и оние што можат да се имплементираат или од DA или од SVA/SCA/SAA.

КС 1: Во комплетен систем ќе се имплементираат сите задолжителни барања наведени во овој документ.

2.2. Правни барања за политиката

Кога се анализира контекстот на деловната примена на потписите, се земаат предвид неколку правни аспекти. Во следните клаузули, се дефинирани целите за контролните мерки (во понатамошниот текст: контроли) во врска со обработката на личните податоци и пристапност за лицата со попреченост.

2.2.1. Обработка на лични податоци

Со цел да се обезбеди дека личните податоци се обработуваат правично и законски во согласност со применливата легислатива за заштита на личните податоци се применуваат следните контроли (ЛП):

ЛП 1: Ќе се обезбедат докази за тоа како се исполнети барањата на важечката регулатива за приватност и заштита на податоци согласно Закон за заштита на лични податоци (ЗЗЛП) и согласно Европската општа регулатива за заштита на податоци (GDPR).

ЛП 2: Ќе се преземат соодветни технички мерки против неовластена или незаконска обработка на лични податоци и против случајно губење или уништување или оштетување на личните податоци.

2.2.2. Пристапност за лица со попреченост

Со цел да се осигури дека SCA/SVA/SAA се достапни за лицата со попреченост преземена е контрола за пристапност за лица со попреченост (ПЛП).

ПЛП 1: KIBSTrust ќе се направи SCA/SVA/SAA да бидат достапни за лицата со попреченост, каде што е изводливо, согласно барањата на Законот за спречување и заштита од дискриминација (Службен весник на РСМ 258/20). Применливи стандарди како што се ETSI EN 301 549[5] може да се земат предвид.

Регулативата eIDAS наведува дека онаму каде што е изводливо, пристапност за лица со попреченост потребно е да се земе предвид.

2.3. Барања за безбедност на информации

Оваа точка од Политиката ги содржи најважните барања за безбедноста на информациите и системите за управувањето со безбедноста на информациите. Контролите дефинирани во оваа клаузула ја покриваат околината во која се применуваат SCA/SVA/SAA и движечките апликации (DA).

ISMS 1: Контролите идентификувани во оваа Политика ќе се применат во контекст на системот за управување со безбедноста информациите на КИБС за којшто поседува и меѓународен сертификат за усогласеност со барањата на стандардот ISO 27001.

ISMS 2: За организација која интегрира процеси на создавање и валидација на потпис, треба да биде безбедност на информациите имплементиран врз основа на ISO/IEC 27001 [i.5], соодветно интегриран со следните одредби.

[5] ETSI EN 301 549: "Accessibility requirements suitable for public procurement of ICT products and services in Europe".

2.3.1. Мрежна заштита

Ако SCA/SVA/SAA прима или испраќа доверливи податоци преку мрежа, гарантирана е заштитата на овие податоци во преносот, како и заштита од мрежни закани на инфраструктурата што ја поддржува обработката и складирањето на доверливи податоци, преку примената на наведените контроли за мрежна заштита (МЗ).

МЗ 1: Ако SCA/SVA/SAA се имплементирани во опкружување кое содржи компоненти од различни нивоа на безбедност кои комуницираат преку мрежи, тогаш мрежите што пренесуваат доверливи податоци до или од SCA/SVA/SAA треба да бидат соодветно сегментирани за да се забрани директен пристап од помалку доверливи системи на повисоки доверливи системи кои содржат или обработуваат доверливи податоци. Доверливи податоци не треба да бидат пренесувани преку неконтролирани или незаштитени мрежи.

МЗ 2: Мрежниот пристап до информатичките системи што складираат или обработуваат доверливи податоци е соодветно ограничен користејќи уреди за филтрирање како што се заштитни ѕидови. Поставените правилата ги штитат информационите системи од неовластени влезен и појдовен сообраќај.

2.3.2. Заштита на информациски системи

Информациските системи што ракуваат со податоците за создавање потпис и околината на SCA/SVA/SAA се обезбедени против неовластен пристап и злоупотреба, активирани се соодветни безбедносни аларми и, кога е применливо, безбедносните настани се снимаат.

Се применуваат следните контроли на заштита на информативниот систем (ЗИС):

ЗИС 1: Информациските системи се заштитени од злонамерна употреба со механизми како што се антивирусни и анти-шпионски софтвер или други превентивни механизми.

ЗИС 2: Ако SCA/SVA/SAA работи на информациски систем за неколку корисници, тогаш соодветна контрола на пристапот ќе спречи каков било неовластен пристап до доверливи податоци.

ЗИС 3: Безбедносните закрпи и поправки се следат на континуирана основа.

ЗИС 4: Инсталациите на закрпи треба да се приоритетизираат, така што безбедносни закрпи за критични или ризични системи ќе се инсталираат што е можно поскоро и во рок од 30 дена од достапноста на закрпите, а други закрпи со помал ризик се инсталираат во рок од 90 дена.

ЗИС 5: Безбедносната закрпа не се применува доколку би можела да воведе дополнителни ранливости или нестабилности што ги надминуваат придобивките од примената на закрпата. Причините за непримена на никакви безбедносни закрпи треба бидат документирани.

2.3.3. Софтверски интегритет на апликацијата

Целта на подолу наведените контроли е да се осигури дека интегритетот на SCA, SVA, SAA и DA е соодветно заштитен.

Контроли за интегритет на софтверот (ИС):

ИС 1: Компонентите SCA/SVA/SAA/DA ќе бидат заштитени од вируси и малициозен софтвер за да се обезбеди нивниот интегритет.

ИС 2: Применети се механизам за откривање промени (алатки за следење на интегритетот на датотеката) за детектирање на неовластена модификација (вклучувајќи промени, дополнувања и бришења) на критичните SCA/SVA/SAA/DA компоненти, како на пример конфигурациски датотеки.

ИС 3: SCA/SVA/SAA/DA компонентите кои биле предмет на вируси или напад на злонамерен софтвер ќе бидат поправени или оневозможени додека не е можна поправка.

ИС 4: Ако софтверските компоненти на SCA, SVA, SAA или DA се наменети да бидат објавени или испорачани, овие компоненти безбедно се испорачуваат, инсталираат и конфигурираат.

2.3.4. Безбедност на складирани податоци

За SCA/SVA/SAA имплементирани се соодветни безбедносни мерки за складирање податоци како и во околината на апликациите со цел заштита на какви било доверливи податоци.

Применети се следните контроли за безбедност на складирани податоци (БСП):

БСП 1: Информациските системи што складираат доверливи податоци се конфигурираат според однапред дефинирано основно ниво на безбедност врз основа на проценка на ризик.

БСП 2: Доверливите податоци ќе бидат заштитени од неовластен пристап и неовластени или ненамерни промени и загуба.

БСП 3: SCA/SVA/SAA и нивната околина поддржуваат соодветни мерки за безбедност на складирани податоци.

БСП 4: Безбедносните мерки за складираните податоци од БСП 3 се во согласност со дефинираното во ISO/IEC 27002 или се базирани на детална анализа на ризик.

2.3.5. Дневници на настани

За да има доказ за активностите поврзани со создавање и валидација на потпис, се користат дневници за настани во SCA/SVA/SAA/DA, или околината на апликацијата за да се соберат информации кои би можеле да бидат потребни за подоцнежни докази.

Применети контроли за дневници на настани (ДН):

ДН 1: Информациските системи што складираат или обработуваат дневници на настани се конфигурираат според однапред дефинирано основно ниво на безбедност врз основа на проценка на ризик.

ДН 2: Дневниците на настани се заштитени од неовластен пристап, и неовластено или ненамерно манипулирање или бришење.

ДН 3: SCA/SVA/SAA треба:

- да ги евидентира потребните настани; или
- ги обезбеди потребните податоци за движечката апликацијата (DA).

ДН 4: Ако SCA/SVA/SAA не ги евидентира потребните настани, DA ќе ги евидентира.

ДН 5: Секое создавање на потпис се евидентира.

ДН 6: Секоја валидација на потписот може да се евидентира.

ДН 7: Дневниците на настаните се означуваат со времето на настанот.

ДН 8: Дневниците на настани треба да го вклучат видот на настанот, успехот или неуспехот на настанот и идентификатор на личноста и/или компонента одговорна за настанот.

2.4. Процеси на создавање на потпис

2.4.1. Главни функционалности на системите за создавање на потпис

Целта е да се обезбеди дека главните функционалности на SCA се добро документирани.

Контроли за процесот на создавање потпис (ПСП):

ПСП 1: Документацијата за SCA вклучува:

- сите поддржани формати на потпис (CAdES, XAdES, PAdES, ASiC) и нивоа на потпис.
- опционални елементи и карактеристики што се поддржани и како може да се изберат и контролираат.

ПРИМЕР: Примери за такви опционални елементи и карактеристики се дали потписите можат да бидат одвоени/обвиткани/обвивачки потписи, паралелни потписи или контра-потписи.

ПСП 2: SCA се контролира за поддршка на функционалностите, како што е документирано.

2.4.2. Тип на содржина на податоци

Целта е да се осигура дека форматот на потписот е соодветен за типот на податочната содржина на документот што треба да се потпише и дека е во согласност со сите законски или деловни барања кои се применуваат.

Контроли за процесот на создавање потпис (ПСП):

ПСП 3: Документацијата за SCA ги специфицира типовите на податочна содржина што SCA ги поддржува и може правилно да ги прикаже (на пр. .pdf, .docx, .xlsx, jpg и т.н.).

ПСП 4: SCA се контролира дали ги поддржува типовите на податочна содржина коишто се документирани во документацијата од ПСП 3.

Цел на следните контроли е да се обезбеди дека проверувачот не може погрешно да го протолкува документот на потписникот поради на пр. недостаток на информации за типот на податоците, погрешна синтакса или неточна презентација или затоа што корисничкиот интерфејс не може правилно да го претстави документот на потписникот.

ПСП 5: SCA ќе дозволи вклучување на типот на податочна содржина на документот или имплицитно во документот или експлицитно како експлицитен атрибут на потписот.

ПСП 6: Доколку типот на податочна содржина на документот е вклучен во потписот, SCA ќе може да му го обезбеди на потписникот.

ПСП 7: Корисничкиот интерфејс треба да го предупреди потписникот ако документот не е во согласност со синтаксата наведена со типот на податочна содржина на документот и треба да му овозможи на потписникот да го прекине процесот на потпишување.

ПСП 8: Корисничкиот интерфејс треба да го предупреди потписникот да не создава потпис на кој било документ што покажува дека е на тип на податочна содржина што не може да му се претстави на корисникот од корисничкиот интерфејс.

ЗАБЕЛЕШКА: Може да има деловни процеси во кои потписникот нема детално да го прегледа документот пред потписот, на пр. во случај на масовно потпишување на фактури.

ПСП 9: Корисничкиот интерфејс треба да го предупреди потписникот ако не може точно да ги прикаже сите делови на документот според типот на содржина на податоци.

Контроли на процес на создавање потпис (ПСП) чија цел е дека потписот се применува на точниот документ:

ПСП 10: SCA ќе му овозможи на потписникот да идентификува што точно ќе се опфати со потписот.

ЗАБЕЛЕШКА: Ова е особено релевантно кога потписот опфаќа само дел од даден документ.

ПСП 11: DA ќе му дозволи на потписникот да го избере документот меѓу достапните документи.

ПСП 12: Во случај процесот да вклучува човечка интеракција, корисничкиот интерфејс треба да го претстави документот на потписникот.

ПСП 13: Кога документот му бил претставен на потписникот, SCA ќе се погрижи дека документот претставен на потписникот е ист како и оној што ќе биде потпишан во процесот на потпишување.

ПСП 14: DA треба да осигура дека документот избран од потписникот за потпишување е ист со оној што е даден на SCA за потпис.

Следните контроли на процесот на создавање потпис (ПСП) имаат за цел да се осигури дека потписникот не-свесно не потпишува други вградени потпишани податочни објекти што се создадени со неважечки потписи од други и дека потписникот може да знае кои потписи се валидирани или оставени невалидирани.

ПСП 15: Ако документот што треба да се потпише содржи потпишани податочни објекти и ако е достапна апликација за валидација на потпис, тогаш пред создавање на потписот, DA или SCA ги валидираат потпишаните податочни објекти користејќи SVA.

ПСП 16: Ако е направена валидација на потпишаните објекти на податоци, тогаш:

(1) DA или SCA ќе го информираат потписникот за секоја политика за валидација на потпис што ја користела SVA да ја изврши валидацијата;
(2) DA или SCA ќе го известат корисникот за резултатите од валидацијата; и
(3) DA или SCA ќе го известат корисникот за тоа кои потписи се потврдени или оставени непотврдени.

ПСП 17: Ако документот за потпишување содржи потпишани објекти на податоци и ако не е достапна или користена SVA, SCA треба да го информира потписник дека други потпишани податочни објекти се вградени во документот, и дека тој треба екстерно да го потврди вградениот потпис пред потпишување на документот.

Следната контрола на процесот на создавање потпис (ПСП) е со цел да осигури дека потписникот не може случајно да го менува документот.

ПСП 18: SCA ќе го спречи потписникот да менува било кој дел од документот за време на процесот на презентирање на содржината на документот.

Контролите во продолжение имаат за цел да обезбедат дека на SCA и се дадени доволно информации за да може точно да го претстави документот на потписникот преку корисничкиот интерфејс. Онаму каде што претставувањето на документот е важно (т.е. презентацијата е едно од средствата за пренесување на семантика), документот може да биде двосмислен ако не е обезбеден, а потписникот може да извлече значење од документот што не е наменето од потписникот.

ЗАБЕЛЕШКА: Вклучувањето на типот на содржина на податоци, (на пр. ,pdf, .docx, .xlsx, jpg, итн.) како потпишан атрибут може да спречи напади врз основа на вметнување html инструкции во податоците што треба да се потпишат, така што кога типот на податоци ќе се замени со "html" води до сосема поинаква презентација.

ПСП 19: DA треба да го вклучи атрибутот тип на содржина на податоци во изборот на атрибути што треба да се потпишат.

ПСП 20: SCA ќе овозможи вклучување на атрибутот за тип на содржина на податоци во податоци што треба да се потпишат, за да се осигура дека типот на податоци на документот е недвосмислен.

ПСП 21: Ако документот може да биде двосмислен поради недоволни информации што ја опишуваат структурата и интерпретацијата на нејзината семантика, DA треба да го вклучи атрибутот тип на содржина на податоци во изборот на атрибути на кои треба да се потпише, за да осигура дека може да се направи само едно толкување на семантиката на документот.

ПСП 22: Ако DA бара вклучување на типот на содржина на податоци, SCA ќе го енкодира типот на податоци на документот и ќе го заштити со потпис.

За да се осигури дека документот што содржи скриен код, којшто може да ја измени презентацијата на потпишаниот документ без да влијае на нејзината криптографската валидност нема да ги измами верификаторот и/или потписникот, се преземаат следните контроли во процесот на создавање потпис (ПСП 23 и 24).

ПСП 23: ПСП 23: Ако типот на податоци на документот е подложен на малициозен софтвер или скриен код што може да ја промени презентацијата на документот без да влијае на потписот, DA или SCA ќе го информираат потписникот за слабоста на овој тип на податоци.

ПСП 24: ПСП 24: DA или SCA треба јасно да му пријават на потписникот ако податоците што треба да се потпишат не можат да се претстават на потписник воопшто или не може да се претстави на сигурен начин.

ЗАБЕЛЕШКА: Можен начин да се избегнат какви било проблеми со скриен код или малициозен софтвер е трансформацијата на документ до тип кој го нема овој проблем.

Контролите во процесот на создавање потпис (ПСП 25 и 26) имаат за цел да се обезбеди потписникот да не потпише несакајќи содржина или обврска.

ПСП 25: SCA ќе дозволи потписникот да биде информиран за содржината што се потпишува.

ПСП 26: SCA ќе му дозволи на потписникот да биде информиран за кој било тип на обврска што ќе се користи во потписот.

2.4.3. Атрибутите на потписот

Целта е да се обезбеди дека потписот е применет на вистинските атрибути на потпис и дека атрибутите не се променети случајно или злонамерно.

ПСП 27: Корисничкиот интерфејс ќе му овозможи на потписникот да ги види атрибутите на потписот. Особено, потписникот треба да може да ја провери содржината на следново:

- сертификатот на потписникот, особено карактеристичното име (DN) на субјектот и DN на издавачот;
- типот на податочна содржина на документот што се потпишува (доколку е присутен);
- политиката на потпис (доколку е присутна),

ЗАБЕЛЕШКА: Политиката за потпис генерално е претставена во атрибутите за потпис со помош на идентификатор на полиса за потпис и вредноста на хашот на политиката за потпис; и видот на обврската (доколку е присутен).

ПСП 28: SCA ќе осигури дека атрибутите на потписот презентирани на потписникот се исти како и оние што ќе бидат потпишан во процесот на потпишување.

ПСП 29: DA ќе осигура дека атрибутите на потпис (ако ги има) избрани од потписникот за потпишување се исти како оние кои ќе бидат дадени на SCA.

ПСП 30: Корисничкиот интерфејс ќе го предупреди потписникот ако типот на атрибутот дозволува присуство на кој било скриен текст, макроа или активен код во атрибутот или на кои било скриени елементи.

Цел на следните контроли е да се осигури дека вистинскиот сертификат се користи за создавање на потпис, дека не се создава потпис со користење на истечен сертификат и дека сертификатот не е отповикан во моментот на потписот.

ПСП 31: Кога повеќе од еден сертификат за потпишување е достапен за употреба од страна на потписникот, DA ќе му дозволи на потписникот да го избере сертификатот што ќе се користи за создавање на потпис. Во одредени случаи DA може да обезбеди предефиниран избор за потписникот.

ПСП 32: SCA ќе го добие идентификаторот од DA потребен за користење на податоците за создавање потпис поврзани со избран сертификат за потпишување.

ПСП 33: Корисничкиот интерфејс ќе му овозможи на потписникот да ги прегледа барем следните компоненти на сертификатот избрани за да бидат вклучени во потпишувањето:

- карактеристичноиме (DN) на субјектот;
- серискиот број; и
- DN на издавачот.

ПСП 34: SCA ќе го потврди периодот на важност на сертификатот за потпишување, и ако тековното време се најде надвор од тој период, SCA ќе го спречи потписникот да ги користи соодветните податоци за создавање потпис.

ПСП 35: ПСП 35: SCA треба за сите сертификати во синџирот на сертификати почнувајќи од сертификатот за потпишување до, но не вклучувајќи го и сидрото за доверба, да го провери периодот на важност и ако времето на потпишување се најде надвор од тој период, SCA треба да го спречи потписникот да ги користи податоците за создавање потпис што одговараат на овој синџир.

ЗАБЕЛЕШКА: Поради директна доверба во коренскиот сертификат (т.н. сидро за доверба), не е потребно да се потврди неговиот статус.

ПСП 36: Ако SCA има (on-line) пристап до информациите за поништување на сертификатот, може да ги потврди статусот на информациите за поништување на сертификатите во синџирот на сертификати почнувајќи од сертификатот за потпишување до, но не вклучувајќи, сидрото за доверба. Доколку се утврди дека сертификатот за потпишување е отповикан, потписникот ќе биде спречен да ги користи соодветните податоци за создавање потпис. Доколку се потврди дека е отповикан друг сертификат за синџирот, корисникот е предупреден и SCA ќе да го спречи потписникот да ги користи податоците за создавање потпис што одговара на овој синџир.

Цел на контрола ПСП 37 е да се осигури дека точниот потписнички сертификат и другите атрибути се означени во потписот и дека тие информациите се заштитени од напади со супституција.

ПСП 37: SCA ќе го заштити посочениот сертификат или копијата од сертификат за потпишување во рамките на потписот од неоткривање на замена откако ќе се создаде потписот.

ЗАБЕЛЕШКА: Ова обично се реализира со потпишување на овие податоци заедно со документот и со нивно ставање во на пр. секцијата за автентикациски атрибути, дел од форматот на потпис.

Цел на контролите ПСП 38 и 39 е да се осигури дека потписот ги содржи сите атрибути неопходни за целта на потписот во согласност со деловните барања, ако тоа не е веќе јасно од контекстот и содржината на документот и дека потписникот е свесен за целта на неговиот потпис (тип на обврска).

ПСП 38: SCA ќе обезбеди дека целта на потпишувањето е соодветно кодирана во потписот, доколку одредена цел била избрана од страна на DA, SCA или корисникот.

ПСП 39: Ако типот на обврска биде вклучен во потписот, корисничкиот интерфејс го прикажува типот на обврската на корисникот.

Цел на следните 3 контроли е корисникот да знае која политика за создавање потпис се користи во процесот на потпишување. Во случај кога деловниот процес предвидува потписникот да избере од различни политики за создавање потпис, тој треба да знае кои политики за создавање потпис се поддржани.

ПСП 40: Кога има повеќе од една политика за создавање потпис, потписникот може да избере политика меѓу достапните. Во овој случај, SVA или DA треба:

- да му обезбеди на корисникот список на можни политики за создавање потписи;
- да го информира корисникот за содржината на политиките за создавање потписи; и
- да побара од корисникот да избере една.

ПСП 41: Ако корисникот не избере одредена политика или ако не постои експлицитна политика за создавање потпис, може да се примени стандардна (предефинирана) политика за создавање потпис.

ПСП 42: Потписникот треба да може да ја побара применета политика за потпис што се користи.

Понатаму, се осигурува дека експлицитната политика за создавање потпис користена за создавање на потписот и/или политика за потпис препорачана да се користи за валидација на потписот се доставува до засегнатите страни, доколку тоа им е потребно на деловните или правните барања.

ЗАБЕЛЕШКА: Експлицитна политика за потпис вклучена во потписот, може да биде поширока од само политика за создавање потпис, на пр. може да вклучува политика за валидација на потпис или политика за зголемување на потписот.

ПСП 43: Доколку е потребна експлицитна политика за потпис од деловните или правните барања, DA ќе обезбеди таква политика за потпис на SCA.

ПСП 44: Доколку е обезбедена експлицитна политика за потпис од страна на DA, SCA ќе вклучи недвосмислена идентификација на точната обезбедена политика во рамките на потписот.

ЗАБЕЛЕШКА: Ова може да се направи со помош на хаш на полисата.

ПСП 45: Ако потписникот избира политика за создавање потпис, DA ќе ја достави до SCA без промена.

2.4.4. Време и редослед

Целта на овие контроли е дека процесот на создавање потпис го следи предвидениот редослед на настани.

ПСП 46: SCA ќе го пресмета потписот само откако потписникот ќе даде согласност за пресметување на потписот.

ПСП 47: SCA го пресметува потписот само откако на потписникот му биле презентирани податоците што треба да се потпишат или целиот документ.

ЗАБЕЛЕШКА: Во случај на масовно потпишување, на потписникот може да не му бидат презентирани сите податоци што треба да се потпишат/документи.

ПСП 48: Ако политиката за создавање потпис бара употреба на еден или повеќе временски печати за потпис, SCA ќе побара токен за временски печат по создавањето на потписот. Ако токен со временски печат не може да се стекне во временскиот рок одреден со политиката, процесот на создавање потпис ќе биде прекинат.

2.4.5. Повикување за потпис

Цел на следните контроли е дека секој генериран потпис е резултат на експлицитно повикување за потпис. Корисничкиот интерфејс може да биде дел од SCA и/или на DA.

ПСП 49: Корисничкиот интерфејс треба да го ограничи случајното повикување на процесот на потпис од страна на потписникот.

ПСП 50: SCA ќе осигури дека потписот се применува со намера на потписникот.

ПСП 51: Доколку изразувањето волја е цел на потписот, пред да започне процесот на потпис, корисникот интерфејсот ќе побара од потписникот да изврши нетривијална интеракција на повикување потпис со SCA што најверојатно нема да се случи случајно.

ПРИМЕР: Пример за нетривијално дејство е лизгањето надолу до крајот на документот што треба да се потпише пред да го прифатите потписот, а не само да изберете „следно“.

ПСП 52: Корисничкиот интерфејс ќе пренесе јасни информации дека ќе се креира потпис.

ПСП 53: Корисничкиот интерфејс може да дава совети и информации за сите аспекти на потписот, на пр. процес и правен статус, доколку таквите информации се достапни.

Потребно е да се спречат ситуации кога SCA и SCDev се во состојба каде што се обезбедени податоци за автентикација на потписникот, а потписникот останува неактивен долг временски период, на пр. кога потписникот бил одвлечен од процесот на потпишување и друго неовластено лице можеби ќе може да го заврши процесот на потпишување на изменет или заменет документ и потпис.

ПСП 54: Во SCA, се дефинира ограничување на времето на мирување кога SCA ниту комуницира со потписникот, ниту е обработка на потпишувањето. Доколку истече овој временски рок, тогаш потписникот повторно ќе се автентицира на SCDev.

Целта е да се спречат ситуации кога погрешно насочен потписник може да изврши операции на погрешен начин така што напаѓач може да здобие доверливи податоци (на пр. ПИН или лозинка што би довело до лажно претставување на потписникот).

ПСП 55: Корисничкиот интерфејс треба да биде толку едноставен колку што може да се спроведе, за да го спречи потписникот од создавање безбедносни дупки.

ПРИМЕР: Ако дијалогот не е јасен, корисникот може да внесе доверливи податоци во полињата што не се обезбедени.

ПСП 56: Корисничкиот интерфејс ќе биде исчистен од доверливите податоци на потписникот по временски рок доволен за извршување на нормални операции. Полињата каде што беа презентирани доверливите податоци ќе бидат заменети со други „неутрални“ податоци, за спречување на латентни слики.

2.4.6. Избор на криптографски алгоритам

Алгоритмите вклучени во пресметувањето на кој било елемент на потписот се базирани на алгоритми и должини на клучеви кои се соодветни за деловните барања.

ПСП 57: Ако политиката за имплицитно или експлицитно создавање потпис бара специфичен пакет за создавање потпис, вклучувајќи должина на клучот, SCA ќе го користи наведениот алгоритам.

ПСП 58: Ако се користи политика за создавање потпис, SCA ќе провери дали политиката означува кој криптографски алгоритам може да се користи. Ако политиката не содржи такви информации, SCA ќе го предупреди корисникот за овој факт и кој алгоритам ќе се користи.

ПСП 59: Ако не се користи политика за создавање потпис или политиката не содржи никакви барања за криптографските алгоритми, тогаш треба да се користат , алгоритми и должина на клучот што одговараат на стандардот ETSI TS 119 312.

ЗАБЕЛЕШКА: Во ETSI TS 119 312 може да се најдат информации за соодветни алгоритми и времето за кое се смета дека се безбедни.

2.4.7. Автентикација на потписникот

Само легитимниот корисник на SCDev може да побара создавање на дигитален потпис.

Следните контроли на процесот на создавање потпис ги претставуваат општите барања за автентикација на корисникот.

ПСП 60: За автентикација на потписник базирана на знаење, податоците за автентикација (на пр. PIN или лозинка) треба да издржат практично погодување и напади со брутална сила.

ПСП 61: Кога податоците за автентикација на потписникот транзитираат низ SCA, SCA ќе ја одржува доверливоста и интегритетот на податоците за автентикација и безбедно ќе ги избришат веднаш штом повеќе не се потребни.

ПСП 62: Каде што податоците за автентикација (како PIN или лозинка) се испраќаат од надворешен влезен уред (како PIN pad или тастатура), преносот на податоци помеѓу влезниот уред и SCDev ќе се врши преку доверлив пат.

ПСП 63: Доколку е дозволено од SCDev, треба да се обезбеди сигурно менување на податоците за автентикација на потписник базирани на знаење.

ПСП 64: При внесување податоци за автентикација засновани на знаење, како лозинка или PIN, повратните информации нема да ја откријат нивната вредност. Ова може да се направи со замена за внесена цифра или знак од потписникот со соодветен симбол или метод кој не открива повеќе од една цифра или знак истовремено и само за краток временски период. Ова треба да се направи со повратна информација (приказ) што воопшто не ја открива внесената цифра или знак.

ЗАБЕЛЕШКА: Ова маскирање не е потребно за внесување OTP, бидејќи се користи само еднаш.

ПСП 65: Ниту SCA ниту компонентата за автентикација на потписникот нема да го спречат управувањето со PIN/лозинка од страна на SCDev. Затоа тие:

- ќе се справат со PIN/лозинка со максимална должина дозволена од SCDev; и
- нема да ги спречат потписниците да го менуваат својот PIN/лозинка по желба.

ПСП 66: При промена на PIN/лозинка, SCA ќе бара двапати презентација на нов PIN/лозинка и ќе провери дали и двете презентации се идентични пред да се достави новиот PIN/лозинка до SCDev. Кога е можно, SCA треба да избегне корисникот повторно да ги користи последните користени лозинка или PIN-кодови.

ПСП 67: SCDev ќе биде конфигуриран со максимален број на дозволени последователни погрешни внесови на податоци за автентикација.

ПСП 68: Кога потписникот дава погрешен податок за автентикација и максимумот што е дефиниран не е постигнат, треба да се даде одговор за грешка и на потписникот да му се дозволи да направи нов обид. Не се обезбедува информација за видот на грешката на корисникот.

ПСП 69: Кога потписникот дава погрешен податок за автентикација и максималниот број последователни погрешни обиди е достигнат, SCDev ќе го блокира методот на автентикација на потписникот и го известува потписникот.

ПСП 70: Бројот на неуспешни споредби со податоците за автентикација на потписникот се евидентира со број на повторни обиди. SCDev може исто така да обезбеди средство за ресетирање на бројачот за повторни обид на неговата почетна вредност (на пр. со претставување код за ресетирање, исто така познат како персонален клуч за одблокирање (PUK)).

Следните контроли на процесот на создавање потпис осигуруваат дека не е можно да се набудуваат податоците за автентикација на потписникот (на пример, PIN/лозинка или биометриски податоци).

ПСП 71: Корисникот ќе биде информиран со документацијата за чекорите што треба да се преземат за да се чуваат безбедни податоците за автентикацијата на потписникот, вклучително и обезбедување дека корисникот нема да биде надгледуван од лица или камери.

ПСП 72: Не е можно да се копираат внесените податоците за автентикација на потписникот на SCA.

ПСП 73: Во случај кога апликацијата се користи во јавна област, тастатурата што се користи за внесување на информациите во SCA:

- да биде заштитена од шпионирање и sиркање преку рамо, и
- да не испуштаат различни звуци за секое копче.

2.4.7.1. Методи за биометриска автентикација

Целта е да се осигури дека е тешко или практично невозможно да се изврши напад на имитирање со фалсификат на биометриските податоци.

ПСП 74: Доколку се користи биометриска автентикација од корисниците, поставени се методи погодни за спречување напади, како што е поднесување на „лажни“ биометриските елементи (како силиконски прсти, употреба на латентни слики, итн.).

Поставени се контроли со цел да се спротивстави на нападите со повторување, ако биометриските методи се засноваат на потенцијално јавно познати податоци (лице, око или отпечаток од прст), тогаш податоците за автентикација на потписникот се заштитени за да се обезбеди автентичност, на пример, напаѓач може да добие јавни биометриски карактеристики како што се слики од лица и отпечатоци од прст и од нив да ги изведе податоците за автентикација на потписникот, со цел злоупотреба на SCDev.

ПСП 75: Доколку се користат биометриски уреди, ќе биде обезбеден интегритет, автентичност и доверливост за патот предвиден за пренос на биометриските податоци помеѓу биометриската сензорска единица и SCDev.

ПСП 76: Доколку се користат биометриски уреди, биометриските сензори ги штитат биометриските податоци за идентификација на корисникот да не може да се користат при повторни напади.

Потребно е во времето на регистрација на корисникот да биде практично невозможно да се поврзе лицето со туѓи биометриски шаблони. На пример, злонамерен код може да ги пресретне податоците на лицето што треба да се запишат и да ги поврзе со биометриски податоци што припаѓаат на различно лице, за подоцна се автентицира неавторизиран корисник (измамник) за да го имитира автентичниот корисник.

ПСП 77: Доколку се користат биометриски уреди, асоцијацијата на биометриските податоци со корисникот не треба да се јавува надвор од доверлива патека или SCDev.

Треба да биде практично невозможно во времето на автентикација да се измени резултатот на верификација од податоците за автентикација на потписникот. На пр., напаѓачот може да го пресретне одговорот на процесот на автентикација, со цел или да даде лажен позитивен одговор (да се потврди автентичност на неовластено лице) или да се даде негативен одговор (напад за одбивање на услугата).

ПСП 78: Ако се користат биометриски уреди, спарувањето на биометриските податоци не треба да се случува во SCA.

2.4.8. Подготовка на податоци што се потпишуваат

При презентирање на податоците за потпишување, потребно е да се осигури се дека напаѓачот не може да и подметне на SCA фалсификуван потпис и да спречи SCA да примени компоненти од целиот потпис специфични за избраниот формат за да се постигне дадена цел.

ПСП 79: SCA ќе ја провери валидноста, автентичноста и комплетноста на сите добиени компоненти со цел да произведе точен формат на податоци што се потпишуваат избран од потписникот.

ПСП 80: SCA треба да користи само хаш алгоритми наведени во ETSI TS 119 312 .

ПСП 81: SCA треба да користи само пакети со потписи наведени во ETSI TS 119 312.

2.4.9. Претставување на податоците што се потпишуваат

Цел на контролите е да се осигура дека претставувањето на податоците што треба да се потпишат се правилно составени.

ПСП 82: SCA ги избира атрибутите за потпис според важечките правила или избрани имплицитни или експлицитни политика за создавање потпис.

ПСП 83: SCA ќе ги произведе точните податоци за потпис.

ПСП 84: SCA ќе ја пресмета презентацијата на податоците што се потпишуваат според важечките правила за форматирање, кодирање и хаширање на податоци што се потпишуваат со избраната имплицитна или експлицитна политика за создавање потпис. Хеширањето може да се направи во SCDev, форматирањето и кодирањето секогаш ќе ги врши SCA.

ПСП 85: SCA треба да го одржува интегритетот на податоци што се потпишуваат при пресметување на презентацијата на податоците што се потпишуваат.

2.4.10. Управување со уредите за создавање потпис

Цел на контрола

Осигурете се дека уредот за создавање потпис што се користи за создавање потпис има соодветно правно и техничко ниво според деловните барања.

ЗАБЕЛЕШКА: Можен начин да се пренесе оваа информација до SCA е политиката за создавање потпис.

ПСП 86: Ако политиката за имплицитно или експлицитно создавање потпис бара специфичен тип на уред за создавање потпис, и овој тип може да се провери автоматски, SCA ќе провери дали уредот за создавање потпис одговара на дадените барања.

ПРИМЕР: Ако е потребен квалификуван уред за создавање потпис според политиката за создавање потпис, SCA може проверете ја поврзаната QCS-изјава (ETSI EN 319 412-5 [i.26]) во сертификатот за потписник.

Цел на контрола

Осигурете се дека SCDev се користи како што е наменето.

ПСП 87: Доколку документацијата на SCDev содржи оперативен водич или еквивалентни информации за тоа како да се користи уред, употребата на SCDev ќе ги земе предвид сите применливи упатства.

2.4.11. Барања за интерфејс меѓу SCDev и SCA (SSI компонента).

Интерфејсот помеѓу уредот за создавање потпис (SCDev) и SCA е одговорен за безбедно поврзување помеѓу SCDev и SCA.

Цел на контролните барања е да се осигури дека комуникацијата помеѓу SCA и SCDev е заштитена.

ПСП 88: Компонентата SSI е да спречи набљудување или менување на податоците доставени преку интерфејсот.

ПСП 89: За типовите на SCDev за кои SSI компонентата тврди дека ги поддржува, SSI компонентата ќе ги поддржува сите ставки релевантни за физичкиот интерфејс во наведениот опсег или со неговите специфицирани карактеристики за да се обезбеди правилно операција.

ПСП 90: Компонентата SSI ќе ја избере точната функционалност на SCDev, ако платформата, на која SCDev функционалноста е имплементирана бара избор.

ПСП 91: Компонентата SSI го избира сертификатот за потпишување, а потоа и податоците за создавање потпис.

2.4.12. Масовно потпишување

Целта на контролите е да се обезбеди дека процесот на масовно потпишување не е помалку безбеден од процесот кога секој документ би бил потпишан посебно и дека не се потпишани документи што не се наменети да ги потпише потписникот.

ПСП 92: Кога е поддржано масовното потпишување, SCA ќе му дозволи на потписникот индивидуално да прикаже било кој од документите што е дел од најголемиот процес на потпис.

ПСП 93: Кога е поддржано масовното потпишување, SCA ќе обезбеди документ што не бил избран од потписникот не може да биде дел од процесот на масовно потпишување.

ПСП 94: Кога е поддржано масовно потпишување, SCA ќе обезбеди извештај за процес на масовно потпишување, вклучувајќи список од секој документ вклучен во масовното потпишување.

2.5. Процес на валидација на потпис

Не е применливо.

2.6. Процес на зголемување на потписот

2.6.1. Вовед

Зголемувањето на потписите е процес со кој одреден материјал (на пр. временски жигови, податоци за валидација, архивски материјал) се вградува во потписите за да ги направи поотпорни на промени или за зголемување нивната долготрајност.

Апликацијата за зголемување на потпис (SAA) прима потписи, како и други влезови од движечката апликација (DA) и ги зголемува добиените потписи според збир на ограничувања и опционално, придружува извештај за зголемувањето кон потписот.

Извештајот за зголемувањето ќе покаже еден од следните три резултати врз основа на политиката за зголемување на потписот:

- **Успешно:** потписот е успешно зголемен.
- **Неуспешно:** потписот не може да се зголеми.
- **Непотребно зголемување:** потписот не е зголемен бидејќи влезниот потпис е веќе усогласен со барањата на политиката за зголемување на потписот.

  ПРИМЕР: Политиката за имплицитно или експлицитно зголемување бара потпис со временски жиг, а потписот веќе содржи временски жиг.

Извештајот за зголемување се состои од главен резултат за зголемувањето придружен со дополнителни податоци, особено кога се враќа неуспешен резултат. Форматот на извештајот за зголемување е надвор од опсегот на овој документ.

Процесот на зголемување на потписот може да се користи како додаток на процесот на создавање потпис, како додаток на процес на валидација на потпис или независно од двата процеса. Трите случаи дополнително се обработуваат во следната клаузула.

2.6.2. Трите случаи на употреба

2.6.2.1. Процес за зголемување на потписот што го користи SCA

Апликацијата за создавање на потпис (SCA) им обезбедува на проверувачите барем основен потпис како што е дефинирано во ETSI TS 119 102, којшто може да се валидира согласно политиката за валидација на потпис.

Меѓутоа, во случај на SCA со on-line пристап, може да се обезбеди повеќе од овој минимален формат.

Така, SCA може да примени, покрај политиката за создавање потпис, и политика за зголемување на потписот.

ПРИМЕР 1: Може да обезбеди, во согласност со политиката за зголемување на потписот, токен за временски печат кој ќе се приложи кон потписот. Ова овозможува да се одржи валидноста на потписот во случај сертификатот за потпишување да биде поништен по UTC времето кое е означено во тој токен со временскиот печат.

ПРИМЕР 2: Може да вклучува податоци за валидација (на пр. издавачки сертификати, CRL или OCSP одговори), според политика за валидација, со што се избегнува потврдувачот (засегнатата страна) да ги презема овие податоци.

2.6.2.2. Процес на зголемување на потписот што го користи SVA

Апликацијата за валидација на потпис (SVA) ги потврдува потписите согласно политиката за валидација на потпис и им покажува на засегнатите страни (верификатор) дали потписот е валиден, неважечки или не може да се утврди неговиот статус.

Меѓутоа, генерално SVA има on-line пристап и на тој начин може да го зголеми применетиот потпис со податоци за валидација, доколку тоа го бара верификаторот и ако потписот е успешно проверен како валиден. Ако има on-line врска со издавачот на временски жигови (TSA), тогаш може да се вклучи и нов токен за временски печат во рамките на потписот.

Така, SVA може да примени, покрај политиката за валидација на потписот, и политика за зголемување на потписот.

2.6.2.3. Независен процес на зголемување на потписот

Во овој случај, апликација за зголемување на потпис (SAA) се користи независно од SCA или од SVA и на потписот ги додава податочните елементи што ги бара политиката за зголемување на потпис.

Овој независен процес е корисен за потписи кои веќе се успешно проверени и кои се архивирани. Ова значи дека независната SAA нема потреба да ги потврдува потписите. Сепак, SAA може да провери кои

криптографски алгоритми и хаш функции се користат во потписот што ги исполнува условите за зголемување, како и валидност на последниот применет токен за временски печат за да се утврди кога потписот треба повторно да се зголеми.

2.6.3. Главни функционалности

Главните функционалности на апликацијата за зголемување на потпис (SAA) се добро документирани.

Контроли (процес на зголемување на потписот)

ПЗП 1: Документацијата за SAA ги наведува:

- сите поддржани нивоа на потпис/контејнер до кои може да го зголеми потписот/контејнерот;
- какви било ограничувања што се применуваат за зголемувањето.

ПРИМЕР: Примери за такви ограничувања се поддржани hash алгоритми или поддржани одвоени (паралелни) потписи во зголемувањето.

ПЗП 2: SAA се контролира дали ги поддржува функционалностите, како што е документирано.

2.6.4. Процедури за зголемување

Контролите на процесот за зголемување на потпис (ПЗП) имаат за цел да осигурат дека се дефинирани и се следат здрави процедури за зголемување на потписот.

ПЗП 3: Спроведените процедури за зголемување на потписот ќе бидат опишани во документацијата за SAA (барем со посочување на релевантен документ).

ПЗП 4: Се користат процедури за зголемување опишани во стандардот ETSI TS 119 102.

ПЗП 5: Спроведувањето на SAA ќе се контролира во однос на дефинираните процедури за зголемување на потписот.

2.6.5. Вклучување податоци

Цел на следните две контроли е да се обезбеди дека потписот ги содржи сите потребни податоци по зголемувањето на потписот.

ПЗП 6: Ако времето на создавање на потписот е потребно до нивото на зголемување, тогаш SAA ќе опфати потврдување на време (на пр. временски печат, временска ознака или запис за доказ) што е можно поскоро по започнување на процесот на зголемување за да се обезбеди временска точка што може да се искористи за споредба со датумите на можни настани (на пр. компромитирање на клуч, поништување, истекување).

ПЗП 7: Доколку тоа го бара избраното ниво до кое се зголемува потписот, информации за сертификатите и нивниот статус на поништување за целата сертификациска патека, почнувајќи од сертификатот на потписникот до доверливиот сертификат на издавачот, ќе бидат вклучени од SAA во потписот и, кога е релевантно, заштитени со доверливо време.

Кога верификацијата на целата патека на сертификатот не е можна, SAA може да продолжи со криптографска верификација и да ги вклучи овие информации во резултатот доставен до DA.

2.6.6. Валидација на влезниот потпис во процесот на зголемување

Потребно е да се осигури дека влезниот потпис е валидиран пред зголемувањето, доколку тоа го бара политиката за зголемување на потпис.

ПЗП 8: Доколку тоа го бара политиката за зголемување на потпис, влезниот потпис се валидира.

ПЗП 9: Ако потписите се валидирани, извештајот за зголемување го вклучува резултатот од валидацијата.

2.7. Политика за развој и кодирање

Оваа клаузула ќе содржи барања, контролни цели и контроли во врска со политики за развојот и кодирањето, особено со:

1) безбедни методи за развој (како што е наведено во клаузула 9.1); и

2) тестирање на сообразност (како што е наведено во клаузула 9 .2) .

2.7.1. Методи за безбеден развој и сигурност на апликации

КИБС обезбедува употреба на соодветна методологија за развој на софтвер, алатки и имплементација на соодветни безбедносни мерки.

Применети се следните методи за безбеден развој (МБР):

МБР 1: Употреба на методологија за развој на софтвер што ги вклучува следните барања:

МБР 1.1: Документиран опис на користената и имплементирана методологија за развој на софтвер.

МБР 1.2: Имплементираната методологија следи формални процеси.

МБР 1.3: Достапни и документирани контролни процедури.

МБР 1.4: Контрола на имплементацијата на методологијата според документираните процедури.

МБР 2: Функционални и технички спецификации:

МБР 2.1: Кодот се проверува според неговите функционални и технички спецификации.

МБР 2.2: Постапките за контрола на кодот се достапни и документирани.

МБР 2.3: Кодот што ги имплементира функционалните и техничките спецификации треба да се контролира во однос на постоечките и документирани процедури.

МБР 3: Се користат најнови безбедносни поправки во околината за развој на софтвер.

МБР 4: Безбедносните мерки за околината за развој на софтвер се согласно ISO/IEC 27002 или врз основа на детална анализа на ризик.

2.7.2. Тестирање на усогласеност

Целта е да се обезбеди дека имплементациите се во согласност со применетите стандарди.

Барања за тестирање на усогласеноста (ТУ):

ТУ 1: **ТУ 1:** Ако е наведена усогласеност со стандард, тогаш усогласеноста на апликацијата ќе се тестира како што е опишано во спецификациите за тестирање на усогласеност, доколку постојат такви спецификации.

ЗАБЕЛЕШКА: Општ преглед и барања за тестирање на усогласеност и интероперабилност, се дефинирани во стандардот ETSI TS 119 104. За имплементација на специфични формати на потпис важат соодветните стандарди: ETSI TS 119 124 за CAdES, ETSI TS 119 134 за XAdES, ETSI TS 119 144 за PAdES и ETSI TS 119 164 за ASiC. За тестирање на усогласеност и интероперабилност на политиките за потпис важи ETSI TS 119 174.

ТУ 2: Применетите тестови за усогласеност се евидентираат и контролираат.

ТУ 2.1: Достапен е опис на користената методологија за тестирање на усогласеност.

ТУ 2.2: Постапките за тестирање на усогласеност треба да бидат достапни и документирани.

ТУ 2.3: Имплементацијата на методологијата треба да се контролира во однос на постоечките и документирани процедури.

ТУ 2.4: Изјава за усогласеност на имплементацијата е достапна за секоја имплементација која бара усогласеност со збир на стандарди.

ТУ 2.5: Изјавата за усогласеност ги содржи следните информации:

- административни информации кои го идентификуваат производителот и имплементацијата (на пр. име на производот и број на верзија);

- идентификација на стандардите според кои се бара усогласеност, вклучувајќи ги и броевите на верзијата (и сите профили, доколку е применливо);
- кои опционални карактеристики на стандардите се поддржани, доколку ги има;
- сите ограничувања зависни од имплементација (опсези, големини, итн.).

ТУ 2.6: Секогаш кога се издава нова верзија на производ, се извршуваат барем регресивни тестови, кои обезбедуваат дека таа компатибилност се одржува.

3. НАДЗОР ВО ВРСКА СО УСОГЛАСЕНОСТА И ДРУГИ ПРОЦЕНКИ

Сообразноста на информатичкиот систем, политиките и практиките, објектите, персоналот и средствата на КИБС се проценува од тело за проценка на сообразност, согласно законот МК-eIDAS и eIDAS регулативата, соодветните закони и стандарди или секогаш кога е направена голема промена во работата на доверлива услуга, врз база на ETSI стандардите наведени во дел 4.15.

Покрај ревизиите за усогласеност, КИБС има право да изврши други прегледи и истражувања за да се обезбеди доверливост на услугите на KIBSTrust. КИБС има право да го делегира извршувањето на овие ревизии, прегледи и истраги на ревизорска фирма на трета страна.

КИБС има право да изврши надворешни ревизии на договарачи кои се поврзани со KIBSTrust за да работат како агенти за автентикација.

3.1. Интервали и околности на проценките

Ревизијата за усогласеност на KIBSTrust се изведува најмалку еднаш годишно. Ревизиите се вршат во непрекинати низи на ревизорски периоди, и секој период е со траење не подолго од една година.

3.2. Идентитет и квалификации на ревизијата

Ревизијата за усогласеност на KIBSTrust се изведува од страна на:

- Интерни ревизори,
- Тело за проценка на усогласеност кое е акредитирано во согласност со Регулативата ЕЗ бр. 765/2008, ETSI стандардите (т.е. ETSI EN 319 403),
- Надзорно тело.

3.3. Однос на проценителот со проценуваниот субјект

Ревизорот на телото за проценка на усогласеност е независен од КИБС и од системите на КИБС кои се проценуваат. Внатрешниот ревизор не врши ревизија на сопствените области на одговорност.

3.4. Прашања опфатени со проценката

Проценката на сообразност опфаќа усогласеност на информатичкиот систем, политиките и практиките, објектите, персоналот и средствата на КИБС со МК-eIDAS и eIDAS регулативите, соодветните закони и стандарди. Телото за проценка на сообразноста врши ревизија на деловите на информатичкиот систем користен за давање доверливи услуги.

Областите на активност, предмет на внатрешна ревизија се следниве:

- Квалитет на услугата;
- Сигурност на услугата;
- Сигурност на работењето и процедурите;
- Заштита на податоците на субјектите и безбедносната политика, извршување на работните процедури и договорните обврски, како и усогласеност со CP/CPS засновани на услугите.

Телото за проценка на сообразноста и внатрешниот ревизор, исто така, ги ревидираат овие делови од информатичкиот систем, политиките и практиките, објектите, персоналот и средствата на поддоговарачите кои се поврзани со обезбедување доверливи услуги на КИБС.

3.5. Дејствија што се преземаат како резултат на пропусти

Во однос на ревизиите за усогласеност на работењето на КИБС, значајните исклучоци или недостатоци утврдени за време на ревизијата за усогласеност ќе резултираат со утврдување на активности што треба да се преземат. Оваа определба ја утврдува менаџментот на КИБС врз основа на добиените податоци од ревизорот. Менаџментот на КИБС е одговорен за развој и спроведување на корективен акциски план. Ако KIBSTrust утврди дека ваквите исклучоци или недостатоци претставуваат непосредна закана за сигурноста или интегритетот на доверливите услуги, корективниот акциски план ќе се развие во рок од 30 дена и ќе се спроведе во разумен временски период. За помалку сериозни исклучоци или недостатоци, менаџментот на КИБС ќе го процени значењето на ваквите проблеми и ќе го одреди соодветниот тек на дејствување.

Дополнително, во случај на резултат на проценка од телото за проценка на сообразноста, кој покажува дека има недостаток, Надзорниот орган бара КИБС да отстрани какво било неисполнување на барањата во временски рок (доколку е применливо) утврден од Надзорниот орган. КИБС прави напори да остане усогласен и навреме да ги исполни сите барања за недостаток. Менаџментот на КИБС е одговорен за спроведување на корективниот акциски план. КИБС го проценува значењето на недостатоците и дава приоритет на соодветните активности што треба да се преземат барем во временскиот рок што е определен од Надзорното тело или во разумен временски период.

Кога се чини дека се повредени правилата за заштита на личните податоци, Надзорниот орган го известува органот за заштита на податоците за резултатите од ревизијата за усогласеност.

3.6. Соопштување на резултатите

Заклучоците од ревизијата или сертификатот (-ите) за доверливи услуги, кои се засноваат на резултатите од ревизијата на телото за проценка на сообразност, спроведено во согласност со законот МК- eIDAS и eIDAS регулативата, соодветните закони и стандарди, може да бидат објавени на веб-страницата на КИБС https://pki.kibstrust.com/repository.

Покрај тоа, КИБС го доставува добиениот извештај за проценка на сообразноста до Надзорното тело во рок од три (3) работни дена од приемот на истиот.

Резултатите од ревизијата на усогласеност на работењето на КИБС ИС може да бидат објавени според дискреционото право на менаџментот на КИБС.

3.7. Самопроценки

КИБС врши редовни внатрешни ревизии за да утврди усогласеност согласно дел 3.4.

4. ОСТАНАТИ ДЕЛОВНИ И ПРАВНИ РАБОТИ

4.1. Надоместоци

4.1.1. Надоместоци за создавање на потписи

KIBSTrust наплатува за своите услуги за создавање на електронски потписи од своите клиенти. Клиенти се првенствено правни лица но зависно од потребите клиенти може да бидат и физички лица. Надоместокот вклучува но не се ограничува на број на електронски потписи, број на временски жигови, закупен диск простор за чување на потпишаните документи и т.н..

4.1.2. Надоместоци за пристап до сертификатите

KIBSTrust може да наплатува надоместок како услов за да ги стави на располагање сертификатите во складиште или на друг начин да ги направи сертификатите достапни на засегнатите страни. KIBSTrust не дозволува пристап до сертификатите во своите складишта на трети лица, кои при обезбедување на свои услуги користат информации за сертификатите, без претходно јасно изразена согласност од страна на субјектот.

4.1.3. Надоместоци за пристап до информациите за поништување или за статусот на сертификатот

KIBSTrust не наплатува надоместок за пристап до информациите за поништување или за статус на сертификатот. Информации за статусот на сертификатот е преку OCSP и CRL коишто се достапни преку складиштето или на друг начин достапни на засегнатите страни. KIBSTrust не дозволува пристап до информациите за статусот на сертификатите во своите складишта на трети лица, кои при обезбедување на производи или услуги користат вакви информации за статусот на сертификатите, без претходно јасно изразена согласност од страна на субјектот.

4.1.4. Надоместоци за други услуги

KIBSTrust не наплатува надоместоци за пристап до овој документ. Секое друго користење, освен едноставно разгледување на документот, како репродуцирање, редистрибуирање, изменување или создавање на текстови што ќе произлезат од нив се предмет на договор за лиценца со КИБС.

4.1.5. Политика на рефундирање (повраток на средства)

4.1.5.1. Продажба од далечина

КИБС не прифаќа какви било рекламации за недостатоци и оштетувања на сертификатот настанати по вина или активности преземени од субјектот.

4.2. Финансиска одговорност

4.2.1. Покритие на осигурување

КИБС одржува комерцијално разумно ниво на покритие со осигурување од професионална одговорност за грешки и пропусти преку програма за осигурување од грешки и пропусти кај Друштво за осигурување. Потврда за полиса за осигурување е достапна во јавното складиште KIBSTrust на http://www.kibstrust.com/repository.

Правилата за обештетување во согласност со осигурувањето од професионална одговорност на KIBSTrust (во натамошниот текст: Правила) го следат законот МК-eIDAS. Следејќи го подзаконскиот акт[6] на МК-eIDAS, КИБС е целосно прилагоден на утврдените барања за износот на покривање на ризик од одговорност за штета. За секоја доверлива услуга, KIBSTrust јавно издава „Правила и услови“ за користење на услугата. Овие правила и услови вклучуваат соодветни информации за осигурување од професионална одговорност на давателот на доверливи услуги.

4.2.2. Други средства

КИБС има доволно финансиски средства да ги одржува своите операции и да ги извршува своите должности, како и разумна можност да го понесе ризикот од одговорност кон субјектите и засегнатите страни. Доказите за финансиските средства не се јавно достапни.

4.2.3. Осигурување или гарантно покритие за крајните субјекти

Види дел 4.2.1 од овие Практики.

4.3. Доверливост на деловните информации

[6] Правилник за определување на најнискиот износ на осигурување за можна штета предизвикана од издавачот и минималниот износ или тип на покривање со осигурување од ризик од одговорност за штети предизвикани од давателот на квалификувани доверливи услуги.

4.3.1. Опсег на доверливи информации

Сите информации што станале познати при обезбедување услуги, а кои не се наменети за објавување (на пр. информации што биле познати на KIBSTrust заради функционирање и обезбедување на своите услуги) се доверливи. Субјектот има право да добие информации за себе од KIBSTrust, според важечките закони.

4.3.2. Информации што не се во доменот на доверливи информации

Секоја информација која не е означена како доверлива или за интерна употреба е јавна информација.

Покрај тоа, статистички податоци за услугите на KIBSTrust кои не се персонализирани се сметаат за јавни информации. КИБС може да објави статистички податоци за своите услуги кои не се персонализирани.

4.3.3. Одговорност за заштитата на доверливите информации

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

Откривањето или доставувањето доверливи информации на трета страна е дозволено само со писмена согласност од правниот сопственик на информацијата, врз основа на судски налог или во други случаи предвидени со закон.

4.4. Приватност на личните информации

4.4.1. План за лични податоци

KIBSTrust применува Политика за приватност, која е поставена на: http://pki.kibstrust.com/repository во согласност со важечките закони.

4.4.2. Информации што се третираат како приватни

Каков било податок за субјектот кој не е јавно достапен преку содржината на издадениот сертификат, именикот на сертификати и онлајн CRL, се третира како приватен.

4.4.3. Информации што не се сметаат за приватни

Во зависност од важечките закони, сите информации објавени во сертификатот не се сметаат како приватни.

4.4.4. Одговорност за заштита на приватните податоци

KIBSTrust ќе ги обезбеди личните податоци од компромитирање и од откривање на трети лица и ќе се придржува кон важечките закони за заштита на личните податоци.

4.4.5. Известување и согласност за користење на личните податоци

Согласно важечкиот закон за заштита на личните податоци, применливата Политиката за приватност и прифатените услови и правила за користење, личните податоци не се користат без согласност на страната на која се однесува информацијата.

4.4.6. Откривање што произлегува од судски или административен процес

КИБС има право да открие доверливи информации ако, со добра намера, верува дека:

- откривањето е неопходно како одговор на судска покана и налог за претрес;
- откривањето е неопходно како одговор на судски, административни и други правни процедури за време на истражни процеси во граѓански или административни дејствија, како на пример судска покана, распит, барање за прифаќање и барање за продуцирање на документи.

Овој дел подлежи на применливите закони на територијата на државата.

4.4.7. Откривање по барање на сопственикот

Политиката за приватност содржи одредби поврзани со откривање на лични податоци на лицето кое му ги доставило тие податоци на KIBSTrust. Овој дел е во согласност со важечкиот закон за заштита на лични податоци.

4.4.8. Други околности на откривање информации

Не се применува.

4.5. Права на интелектуална сопственост

Распределбата на правата на интелектуална сопственост помеѓу партнерите на КИБС, освен субјектите и засегнатите страни, е регулирана со важечките договори, склучени помеѓу тие учесници и КИБС. Следниве потточки се однесуваат на правата на интелектуална сопственост поврзани со субјектите и засегнатите страни.

Документите кои се стават на располагање на апликацијата за создавање потпис се сопственост на иницијаторот на потпишувањето, како договорна страна за користење на доверливата услуга за создавање на електронски потписи.

4.5.1. Права на сопственост на информациите во сертификатите и информациите за поништување

КИБС ги задржува сите права на интелектуална сопственост во и на сертификатите и на информациите за поништување што ги издава. КИБС дава дозвола за репродуцирање и дистрибуирање на сертификатите на неекслузивна основа без плаќање на авторски права, под услов тие да бидат репродуцирани во целост и користењето на сертификатите да биде регулирано со Правилата и условите наведени во сертификатот. КИБС дава дозвола за користење на информациите за поништување заради извршување на функциите на засегнатите страни, што е регулирано во соодветните Правила и услови или некои други важечки договори.

4.5.2. Права на сопственост на информациите во оваа Политика

Субјектите прифаќаат дека KIBSTrust ги задржува сите права на интелектуална сопственост на оваа Политика и релевантните CP/CPS.

4.5.3. Права на сопственост на имиња

Подносителот на барањето за сертификат ги задржува сите права што ги има (доколку ги има) на трговската марка, сервисната марка или трговското име содржани во барањето за сертификат и карактеристичното име во сертификатот, издаден на таквиот барател на сертификат.

4.5.4. Права на сопственост на клучевите и материјалот со клучеви

Паровите клучеви што соодветствуваат со сертификатите на ИС и на субјектите - крајни корисници се сопственост на ИС и на субјектите - крајни корисници кои се субјекти на тие сертификати, без оглед на физичкиот медиум во кој тие се складираат и заштитуваат, и тие лица ги задржуваат сите права на интелектуална сопственост во и на овие парови клучеви. Без да се ограничува воопштеноста на претходното, коренските јавни клучеви на KIBSTrust и коренските сертификати кои ги содржат нив, клучеви и самопотпишаните сертификати, се сопственост на KIBSTrust. Конечно, тајните удели на приватните клучеви на ИС се сопственост на ИС и ИС ги задржува сите права на интелектуална сопственост на тие тајни удели, иако не може да стекне физичка сопственост врз тие удели или ИС од KIBSTrust.

4.5.5. Прекршување на правата на сопственост

КИБС свесно не ги крши правата на интелектуална сопственост на која било трета страна.

4.6. Изјави и гаранции

4.6.1. Изјави и гаранции на давателот на услугата

KIBSTrust гарантира дека:

- ги обезбедува своите услуги во согласност со барањата и процедурите дефинирани во овие Политика и поврзаните документи;
- е во согласност со MK-eIDAS, eIDAS и поврзаните правни акти;
- ги објавува своите Политики и поврзаните документи и ја гарантира нивната достапност во мрежата за комуникација со јавни податоци;
- ги објавува и исполнува барањата на правилата и условите за субјекти и гарантира нивна достапност и пристап во мрежата за комуникација со јавни податоци;
- ја одржува доверливоста на информациите што ги добива во текот на снабдувањето со услугата и што не подлежат на објавување;
- води сметка за сертификатите, издадени од него и нивната валидност, и обезбедува можност за проверка на важноста на сертификатите;
- обезбедува пристап до приватните клучеви на далечинското QSCD на овластениот субјект на клучевите;
- обезбедува правилно управување и усогласеност на далечинското QSCD;
- го известува Надзорното тело за какви било промени во јавниот клуч што се користи за давање доверливи услуги;
- без непотребно одложување, но во секој случај во рок од 24 часа откако ќе дознае за какво било нарушување на сигурноста или загубата на интегритетот што има значајно влијание врз пружената услуга или врз личните податоци што се содржат во неа, ќе го извести Надзорниот орган и, кога е соодветно, другите релевантни тела како националниот CERT или Агенцијата за заштита на лични податоци на РСМ.
- кога постои можност прекршувањето на сигурноста или загубата на интегритетот да влијае негативно на физичко или правно лице на кое му е обезбедена услуга, без одложување ќе го извести физичкото или правното лице за повредата на сигурноста или за губењето на интегритетот;
- ја чува целата документација, евиденција и записи поврзани со услугите;
- обезбедува проценка на усогласеноста според барањата и го презентира заклучокот на телото за проценка на усогласеноста на Надзорното тело за да обезбеди континуиран статус на услуги регистрирани во Регистарот при МИОа;
- има финансиска стабилност и ресурси потребни за да работи во согласност со оваа Политика;
- ги објавува условите на политиката за задолжително осигурување и заклучокот на телото за проценка на усогласеноста во мрежата за комуникација со јавни податоци;
- овозможува пристап до своите услуги за лица со посебни потреби, доколку тоа е можно;
- нема материјално погрешно претставување на факт во сертификатите, познат или што потекнува од ентитетите преку кои се одобрува барањето за издавање сертификат.

Правилата и условите за користење на услуги на КИБС може да вклучат дополнителни изјави и гаранции.

4.6.2. Изјави и гаранции на корисникот

Корисниците гарантираат дека:

- Сите изјави направени од корисникот се вистинити, а корисникот е свесен за тоа дека KIBSTrust може да одбие да ја обезбеди услугата ако корисникот намерно претставил лажни, неточни или нецелосни информации за услугата;
- Корисникот ги почитува барањата дадени од KIBSTrust во оваа Политика и поврзаните документи;
- Сите информации доставени од корисникот се вистинити и во случај на промена на доставените податоци, корисникот треба да ги извести точните податоци во согласност со правилата утврдени со овие Практики и поврзаните документи;

- Услугата се користи исклучиво за овластени и правни цели, во согласност со оваа Политика и склучениот Договор за услугата;
- Секој потпис креиран со употреба на приватниот клуч кој одговара на јавниот клуч, наведен во сертификатот е напреден/квалификуван потпис на субјектот и соодветниот сертификат е прифатен и оперативен (не е истечен или поништен) во моментот кога се креира потпис,
- Податоците како ПИН, корисничко име, лозинка, OTP и т.н. со кои се пристапува до приватниот клуч се заштитени и дека ниту едно неовластено лице досега немало пристап до нив,
- Квалификуваност потпис се креира само со QSCD.

Правилата и условите на KIBSTrust за користење на доверливи услуги може да вклучат дополнителни изјави и гаранции.

4.6.3. Изјави и гаранции на засегнатата страна

Според Правилата и условите на KIBSTrust за користење на услуга се предвидува засегнатата страна да потврди дека поседува доволно информации за да донесе одлука за обемот до кој таа ќе одбере да се потпре на информациите во сертификатот, дека единствено таа е одговорна за одлуката дали ќе се потпре или не на таквата информација, и дека таа ќе ги поднесе законските последици од неуспевањето да ги изврши обврските на засегната страна согласно овие Практики.

Правилата и условите на KIBSTrust за користење на квалификувани доверливи услуги може да вклучат дополнителни изјави и гаранции на засегнатите страни.

4.6.4. Изјави и гаранции на други учесници

Не се применува.

4.7. Одрекување на гаранциите

До онаа мера која е дозволена со важечкиот закон, Правилата и условите за користење на услугата ги одрекуваат можните гаранции на KIBSTrust, вклучително и каква било гаранција за пласирање на пазарот или соодветност за одредена намена.

КИБС не е одговорен за:

- Тајноста на податоците (ПИН, корисничко име, лозинка, OTP) со кои се има пристап до приватните клучеви на субјектите, можната злоупотреба на сертификати или несоодветните проверки на сертификати или за погрешни одлуки на засегнатата страна, или какви било последици поради грешки или пропусти во проверките за валидација на доверлива услуга;
- Неизвршување на своите обврски, доколку таквото неизвршување се должи на грешки или безбедносни проблеми на Надзорното тело, органот за супервизија на заштитата на податоци, доверливиот список или кој било друг јавен орган;
- Неизвршување на своите обврски или крирање на дополнителни трошоци за своите корисници на услуги како последица на промена на технички стандарди;
- Неизвршување на обврските што произлегуваат од оваа Политика и поврзаните документи, доколку таквото неизвршување е предизвикано од Виша сила.

4.8. Ограничувања на одговорност

Правилата и условите на KIBSTrust за користење на доверливи услуги ја ограничуваат одговорноста на KIBSTrust. Ограничувањата на одговорноста вклучуваат изземање на индиректни, посебни, случајни и последователни штети.

Одговорноста (и/или нејзиното ограничување) на корисниците и засегнатите страни е наведена во релевантните договори за користење на доверливи услуги.

4.9. Обесштетувања

4.9.1. Обесштетување од страна на корисниците

До мера до која е пропишано со применливиот закон, од корисниците се очекува да го обесштетат КИБС за:

- Фалсификување или погрешно интерпретирање на факти од страна на корисникот,
- Неприкажување на материјален факт, од страна на корисникот, ако погрешната интерпретација или пропустот се направени од небрежност или со намера да се измами некоја од страните,
- Неуспехот на субјектот да го заштити својот приватен клуч, да го користи доверливиот систем или неуспевањето на друг начин да спречи компромитирање, губење, откривање, изменување или неовластено користење на приватен клуч, или
- Користењето на име (вклучително и без ограничувања во рамките на општото име, името на доменот, или електронската адреса) од страна на субјектот кое ги прекршува правата на интелектуална сопственост на трето лице.

Договорот може да вклучи дополнителни обврски за обесштетувања.

4.9.2. Обесштетување од страна на засегнатите страни

До мера до која е пропишано со применливиот закон, Правилата и условите на KIBSTrust за користење на квалификувани доверливи услуги бараат засегнатата страна да го обесштети KIBSTrust во случај кога:

- Засегнатата страна не ги исполнила обврските на засегната страна,
- Засегнатата страна се потпира на сертификат за кој во дадени околности, тоа не е разумно, или
- Засегнатата страна не го проверила статусот на сертификатот за да утврди дали сертификатот е истечен или поништен.

Правилата и условите за користење на квалификуваните доверливи услуги може да вклучат дополнителни обврски за обесштетување.

4.10. Период и прекин на важност

4.10.1. Период на важност

Оваа Политика стапуваат во сила по објавувањето во складиштето на KIBSTrust. Измените и дополнувањата на оваа Политика стапуваат во сила по објавувањето во складиштето на KIBSTrust.

4.10.2. Прекин на важност

Оваа Политика со промените кои се прават одвреме навреме остануваат во сила сè додека не се заменат со нова верзија.

4.10.3. Ефекти од прекинот на важност и продолжување

Без оглед на прекинувањето на важноста на оваа Политика, КИБС и корисниците, се обврзани со сите услови наведени во договорот за користење на доверливата услуга.

4.11. Индивидуални известувања и комуникација

Доколку не е специфицирано поинаку со договор помеѓу страните, KIBSTrust и корисниците ќе користат комерцијално разумни методи за да комуницираат помеѓу себе, имајќи ги предвид критичноста и темата на комуникацијата.

Делот 1.5.2 ги дава сите достапни средства за комуникација.

4.12. Измени и дополнувања

4.12.1. Процедура на измени и дополнувања

Измените и дополнувањата на оваа Политика прави Одборот за управување со политики (ОУП) на KIBSTrust. Измените и дополнувањата се во форма на документ кој содржи изменета и дополнета форма

на документот или ажурирање. Верзиите со измените и дополнувањата или ажурирањата поврзани со складиштето на КИБС се објавени на https://pki.kibstrust.com/repository/.

Ажурирањата ги заменуваат сите наведени или спротивставени одредби на наведената верзија на документот.

4.12.2. Механизам и период на известување

ОУП на KIBSTrust го задржува правото да ги измени и дополни овие Политика и/или соодветните CP/CPS без известување за измените и дополнувањата што не се материјални, вклучително и без ограничување корекција на типографски грешки, измени во URL адреси и промени во информации за контакт. Одлуката на ОУП да ги означи измените како материјални или нематеријални е според дискреционото право на ОУП.

Предложените измени и дополнувања на оваа Политика и поврзаните CP/CPS се објавени со складиштето на КИБС лоцирано на: https://pki.kibstrust.com/repository/.

Без оглед на сè спротивно во оваа Политика и CP/CPS, доколку ОУП верува дека материјалните измени и дополнувања во оваа Политика и CP/CPS се неопходни веднаш да се запре или да се спречи нарушување на сигурноста на КИБС како давател на доверливи услуги (TSP) или на кој било дел од тоа, КИБС и ОУП имаат право да ги направат ваквите измени и дополнувања преку објавување во складиштето на КИБС. Ваквите измени и дополнувања ќе стапат во сила веднаш по објавувањето. Во разумно време по објавувањето, КИБС ќе ги извести корисниците за ваквите измени и дополнувања.

КИБС и ОУП, ќе ја ажурираат оваа Политика минимум на годишно ниво.

Измените и дополнувањата што не го менуваат значењето на оваа Политика, како што се правописни корекции, превод и ажурирања за деталите за контакт, се документирани во делот историја на верзии на овој документ. Во овој случај, вториот дел од бројот на верзијата на документот е зголемен.

Во случај на значителни промени, новата верзија на документот јасно се разликува од претходните и првиот дел од број на верзија е зголемен за еден.

4.12.3. Околности под кои мора да се промени предметниот идентификатор (OID)

Ако ОУП одреди дека е неопходна промена во некој предметен идентификатор што соодветствува на политиката за сертификати, измените и дополнувањата ќе содржат нов предметен идентификатор за политиките за сертификати. Инаку, измените и дополнувањата не бараат промена во предметниот идентификатор на политиките за сертификати.

4.13. Одредби за решавање на спорови

4.13.1. Спорови помеѓу KIBSTrust, претставништва и клиенти

Споровите меѓу учесниците во KIBSTrust се решаваат во согласност со одредбите на важечките договори меѓу страните.

4.13.2. Спорови со субјекти - крајни корисници или засегнати страни

Правилата и условите на KIBSTrust содржат клаузула за решавање на спорови. За споровите во кои е инволвиран KIBSTrust, предвиден е почетен период на преговори од шеесет (60) дена, после кој ќе следи судски спор во надлежниот судот во Скопје.

4.14. Меродавно право

Законите на Република Северна Македонија ќе бидат надлежни за извршувањето, составувањето, интерпретирањето и важноста на оваа Политика, без оглед на договорот или изборот на други законски одредби и без барање да се воспостави комерцијална врска во земјата. Овој избор на закон е направен

за да се обезбедат униформни процедури и толкување за сите учесници на KIBSTrust, без оглед каде се наоѓаат.

Одредбата за меродавно право важи само за оваа Политика. Договорите кои ја вклучуваат оваа Политика само како референца може да имаат свои сопствени одредби за меродавно право, под услов делот 4.14 да го регулира извршувањето, составувањето, интерпретирањето и важноста на условите од оваа Политика, одделно и раздвоено од останатите одредби на кој било таков договор, предмет на какви било ограничувања што се појавуваат во применливиот закон.

4.15. Усогласеност со меродавното право

КИБС обезбедува усогласеност со законските услови за исполнување на сите применливи законски барања за заштита на евиденцијата од губење, уништување и фалсификување и барањата на следново:

- MK-eIDAS - Закон за електронски документи, електронска идентификација и доверливи услуги (Службен весник на Република Северна Македонија 101/19...215/19);
- eIDAS - Регулатива (ЕУ) бр. 910/2014 на Европскиот парламент и на Советот од 23 јули 2014 година за електронски услуги за идентификација и доверливи услуги за електронски трансакции на внатрешниот пазар и укинување на Директивата 1999/93 / ЕЗ;
- Закон за заштита на лични податоци во Република Северна Македонија и поврзаната ЕУ регулатива (GDPR).

4.16. Останати одредби

4.16.1. Целосност на договорот

Не се применува.

4.16.2. Доделување

Сите субјекти кои работат според овие Практики не можат да ги доделат своите права или обврски без претходна писмена согласност од KIBSTrust. Освен ако не е поинаку определено во договор со страна, КИБС не дава известување за доделување.

4.16.3. Одвоивост на одредби

Во случај ако некој член или клаузула од овие Практики се прогласат за неспроведливи од соодветен суд или од друг надлежен авторитет, останатиот дел од овие Практики ќе остане во сила.

4.16.4. Спроведување (надоместок за адвокат и откажување од правата)

КИБС може да бара надомест на штета и адвокатски такси од страната за штети, загуби и трошоци поврзани со однесувањето на таа страна. Неуспехот на КИБС да спроведе одредба од овие Практики не го одрекува правото на КИБС да ја спроведе истата одредба подоцна или правото да спроведе друга одредба од овие Практики. За да бидат во сила, одрекувањата мора да бидат во писмена форма и потпишани од КИБС.

4.16.5. Виша сила

Неисполнувањето на обврските што произлегуваат од CP/CPS и / или поврзаните документи не се смета за прекршување, доколку таквото неисполнување е предизвикано од Виша сила. Ниту една од страните нема да бара оштета или друг надомест од другите страни за доцнење или неисполнување на овие Практики и / или поврзаните документи, предизвикани од Виша сила.

4.17. Други одредби

Не се применува.

Додаток А. Табела со дефиниции

Термин	Дефиниција
Напреден електронски потпис	Електронски потпис што ги исполнува следниве услови: • на единствен начин е поврзан со потписникот; • овозможува идентификација на потписникот; • да е создаден со употреба на податоци за создавање на електронски потпис кои потписникот, со високо ниво на доверба, може да ги користи единствено под сопствена контрола; и • да е поврзан со податоците кои се потпишани, на таков начин што секоја подоцнежна измена на истите е воочлива.
Сертификат за електронски потпис	електронска потврда која ги поврзува податоците за валидација на електронскиот потпис со физичко лице и која го потврдува најмалку името или псевдонимот на тоа лице. Технички тоа е јавен клуч на корисник, заедно со некои други информации, кој е шифриран со приватниот клуч на издавачот на сертификати што го издал, за да не може да се фалсификува.
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.
Издавач на сертификати (ИС)	Овластен давател на доверлива услуга за издавање на сертификати
Компромитирање	Прекршување (или претпоставено прекршување) на безбедносната политика, при кое може да се случи неовластено откривање или губење на контролата врз чувствителни информации. Во однос на приватните клучеви, компромитирање претставува губење, кражба, откривање, изменување, неовластено користење или друг вид на компромитирање на сигурноста на тој приватен клуч.
Електронски потпис	Податоци во електронска форма кои се приложени или логички се поврзани со други електронски податоци, и кој потписникот го користи за потпишување.
Правила и услови за користење на услуги	Обврзувачки документ во кој се наведени правилата и условите според кои физичко или правно лице дејствува како корисник или како засегната страна за соодветните доверливи услуги кои ги обезбедува КИБС.
Права на интелектуална сопственост	Права кои потпаѓаат под некое од следново: авторски права, патент, трговска тајна, заштитена марка и кои било други права на интелектуална сопственост.
Складиште (Repository)	Веб-базирано место за јавно информирање за политики и практики за издавање сертификати и средства за електронска идентификација и други релевантни информации на КИБС, достапни онлајн.
Сертификат со долготрајна важност	Квалификуван сертификат кој е валиден 1 до 3 години.
Еднократен сертификат	Сертификат за еднократна употреба издаден согласно политика за сертификати Lightweight Certificate Policy (LCP профил на сертификат)
Протокол за онлајн статус на сертификат (OCSP)	Протокол со кој им се обезбедува на засегнатите страни информација за статусот на сертификатот во реално време.
Одбор за управување со политиките на KIBSTrust (ОУП)	Група во рамките на КИБС одговорна за објавување на оваа Практика и поврзаните документи.
Приватен клуч	Клучот од парот клучеви што безбедно се чува од страна на носителот на клучот, и тој се користи за креирање квалификуван сертификат или за дешифрирање на електронски записи или датотеки што биле шифрирани со соодветниот јавен клуч.

Термин	Дефиниција
Јавен клуч	Клучот од парот на клучеви што може да биде јавно обелоденет од носителот на соодветниот приватен клуч и кој се користи од страна на засегнатата страна за да потврди квалификуван сертификат, односно електронскиот потпис креиран со соодветниот приватен клуч на носителот.
Инфраструктура на јавен клуч (PKI)	Архитектура, организација, техники, практики и процедури кои заеднички ги поддржуваат имплементацијата и функционирањето на криптографскиот систем на јавни клучеви базирани на сертификат. КИБС PKI се состои од системи кои соработуваат за обезбедување и имплементирање на криптиграфски систем за јавен клуч врз основа на сертификат.
Квалификуван електронски потпис	Напреден електронски потпис што е креиран од квалификуван уред за создавање електронски потпис и се заснова на квалификуван сертификат за електронски потпис.
Квалификуван сертификат	Квалификуван сертификат е сертификат издаден од издаден од давател на квалификувана доверлива услуга и кој ги исполнува условите утврдени во овој закон, а кои се однесуваат на квалификуван сертификат за електронски потпис.
Квалификуван сертификат за електронски потпис	Сертификат за електронски потписи, издаден од квалификуван давател на доверливи услуги кој ги исполнува условите утврдени во Анекс I на eIDAS.
Средство за создавање квалификуван потпис/печат (QSCD)	Уред кој е одговорен за квалификување на дигитални потписи со употреба на специфичен хардвер и софтвер со што се гарантира дека единствено потписникот има контрола врз неговиот приватен клуч.
Засегната страна	Поединец или организација која делува потпирајќи се на сертификат и / или електронски потпис.
Далечинско QSCD	Серверски базиран HSM што се користи за централно генерирање и употреба на претплатнички приватни клучеви.
Коренски ИС	Орган за сертификација кој е на највисоко ниво во доменот на TSP и кој се користи за потпишување подредени ИС.
Тајни удели	Делови од приватен клуч на ИС или дел од податоци за активирање што се потребни за да функционира приватниот клуч на ИС во рамките на аранжманот на тајни удели.
Субјект на сертификатот	Како носител на сертификат може да биде: - физичко лице; - физичко лице идентификувано дека е поврзано со правно лице; - правно лице (тоа може да биде организација или единица или оддел идентификуван дека е поврзана со организација);
Субјект на електронска идентификација	Физичко или правно лице кое поведува постапката за барање за издавање на средство електронска идентификација пред издавач на средства за електронска идентификација.
Надзорно тело	Органот што е назначен од страна на земја-членка за извршување на надзорни активности на доверливите услуги и давателите на услуги според eIDAS. Според МК-eIDAS тое е Министерството за информатичко општество и администрација.
Давател на доверливи услуги	Правно лице кое обезбедува една или повеќе доверливи услуги.

Термин	Дефиниција
Доверлива услуга	Електронска услуга при електронски трансакции, која се состои од: - создавање, валидација и верификација на електронски потписи, електронски печати или електронски временски жигови, услуги за електронска препорачана достава, како и сертификати поврзани со овие услуги или - создавање, валидација и верификација на сертификати за автентичност на веб страници или - зачувување на електронски потписи, печати или сертификати поврзани со овие услуги. Доверливите услуги може да бидат неквалификувани и квалификувани.
Движечка апликација (анг. driving application)	апликација која ја користи апликацијата за создавање потпис за да создаде потпис или апликацијата за валидација на потпис за да валидира дигитален потпис или апликацијата за зголемување на потпис за да зголеми дигитален потпис.
Апликација за создавање потпис (signature creation application**)**	Апликација во рамките на системот за потпишување која го надополнува уредот за создавање на потписи, која создава податочен објект.
Податоци за создавање на потпис	уникатни податоци, како што се шифри или приватни криптографски клучеви, кои ги користи потписникот за да создаде вредност на дигитален потпис.
Уред за создавање на потпис	конфигуриран софтвер или хардвер што се користи за имплементација на податоците за создавање потпис и за создавање вредност на дигитален потпис.
Систем за создавање потпис	целокупниот систем, којшто се состои од апликација за создавање потпис и уред за создавање потпис, со којшто се создава дигитален потпис.
Зголемување на потпис	процес на инкорпорирање на дополнителни информации на дигитален потпис со цел да се одржи валидноста на тој потпис на долг рок. Апликацијата за зголемување на потписот може да се имплементира како дел од апликацијата за создавање потпис или како дел од апликацијата за валидација на потпис или како самостојна апликација.
Валидација на потпис	процес на проверка и потврдување дека потписот е валиден.
Верификација на потпис	процес на проверка на криптографската вредност на потписот користејќи податоци за верификација на потписот.
Податоци за верификација на потпис	податоци, како што се шифри или јавни криптографски клучеви, кои се користат за да се потврди потписот.

Крај на документот