

Врз основа на член 16 од Законот за податоците во електронски облик и електронски потпис (Службен весник на Република Македонија бр.34/2001), министерот за финансии донесе,

ПРАВИЛНИК

за содржината на правилата на издавачот на сертификати

Член 1

Со овој правилник се пропишува содржината на правилата на издавачот на квалификувани сертификати, (во понатамошен текст: издавач).

Член 2

Издавачот во правилата треба да ги утврди постапките и опремата кои ќе ги применува во согласност со условите и стандардите кои се општо прифатени во Европската унија.

Член 3

Со правилата се утврдуваат и просториите и опремата на издавачот кои треба да бидат обезбедени стручно, електронски и физички од неовластен пристап.

Член 4

Правилата на издавачите на квалификувани сертификати , треба да содржат два дела, јавен и таен дел.

Член 5

Сите битни одредби кои што ги регулираат и влијаат на односите помеѓу издавачот и сопствениците на издадени квалификувани сертификати од тој издавач и трети лица, а кои се однесуваат на тие сертификати, треба да бидат содржани во јавниот дел од внатрешни правила.

Член 6

Правилата во својот јавен дел треба да содржат и одредби за:

- инфраструктура на издавачот, кои ги содржат основните технички карактеристики, карактеристики на постапката и податоци за ниво то на безбедноста и сигурноста на инфраструктурата;
- бројот, состојба и стручната подготовка на вработените кај издавачот;
- правила за можните подредени издавачи, и за правила за меѓусебно признавање на издавачи;
- безбедносни барања и обврски на сопствениците на сертификати и трети лица, кои што се однесуваат на сертификати;
- основните карактеристики и содржина на сертификати кои што ги издава издавачот;
- ракување и управување со сертификати, кои што во себе содржат пред се одредби поврзани со барањето за издавање и проверка на автентичноста на лицето и одредби за издавање, продолжување на важноста и поништување на сертификати;
- одговорноста на издавачот и висината на склученото осигурување;

- податоци за автентичноста на издавачот и негова инфраструктура
- постапките за престанок на работа на издавачот.

Член 7

Правилата во свој таен дел содржат доверливи податоци за:

- просторите на издавачот;
- вработените кај издавачот, кои што во себе содржат, пред се, надлежност и задачи на поединците, посебни надлежности на поединците, потребни услови и одредби за евентуални надворешни соработници;
- физичка безбедност на инфраструктурата на издавачот, пред се поврзана со пристапот во просториите на издавачот (право за влез, автентификациски систем, и др.), или со ракување со машинската опрема и отпадокот како и со внесување и изнесување на опрема и материјал;
- електронска и програмска безбедност, пред се поврзани за безбедно програмирање на сервери, употреба на телекомуникациски средства и опрема, со пријави во системот, безбедносни копии и слично;
- внатрешната контрола, пред се, за оперативна изведба и следење на движење (контрола на физички влез, контрола на пропусници и дозволи, известување за безбедносни проблеми и слично);
- постапки и чекори во непредвидени случаи;
- водење на дневниците и содржина на записниците, заедно со одредби за можните електронски облици на записници.

Член 8

Јавниот дел на правилата на издавачот треба да биде слободно достапен во електронски облик на интернет и во трајниот медиум за чување на податоци во електронски или класичен облик.

Член 9

Издавачот со правилата треба да предвиди секој работен ден редовно да се вршат прегледи на сигурноста на опремата.

Ако издавачот својата дејност ја врши 24 часа дневно непрекинато во текот на целата година, должен е прегледите да ги врши секој ден.

Со прегледот од ствот 1 и 2 од овој член, се утврдува дали податоците и опремата се сигурни, дали сигурносните системи работат, како и дали имало пристап или обид за пристап до опремата и податоците тоа од неовластено лице, што се евидентира веднаш.

Член 10

Издавачот со правилата треба да утврди дека со податоците за електронско потпишување кај издавачот, работат најмалку двајца вработени истовремено, заради тоа издавачот треба да обезбеди никој да не може сам да ги добие сите потребни податоци или да ја користи опрема за пристап до опремата во која се чуваат податоците за електронско потпишување на издавачот.

Член 11

Издавачот со правилата треба да утврди дека на најмалку две

сигурносни копии од сите поважни податоци и другите средства за чување или пренесување на податоците, се обезбедува чување, со што ќе се спречи губењето или неовластено користење на истите.

Сигурносните копии треба да се чуваат одвоено од информациониот систем за управување со квалификуваните сертификати и на друга посебна локација просторно одалечена од информациониот систем.

Чувањето на сигурносните копии задолжително се евидентира.

Член 12

Издавачот треба да обезбеди сигурност во извршувањето на дејноста на чувањето на податоците за електронско потпишување и тоа до моментот на нивното важење или поништувањето, односно најмалку до рокот утврден со законот за нивно чување.

Издавачот треба да обезбеди и сигурност и во пристапот до податоците за електронско потпишување на лицата на кои според законот тие податоци треба да им се достапни.

Член 13

Издавачот составува записник за сите дадени почетни овластувања и употребени постапки при инсталирање на неговиот информациониот систем за управување со квалификуваните сертификати.

Издавачот составува записник и доколку дојде до промена на овластувањата или до промена во подесувањето на информациониот систем за управување со квалификуваните сертификати, издавачот составува нов записник.

Записниците од ст1 и 2 на овој член, треба да бидат потпишани од сите лица кои учествувале при инсталирањето како и лицата кои учествувале во дадените овластувања и постапки при инсталирањето или подоцнежните промени и трајно да бидат зачувани.

Член 14

При физички пристап до информациониот систем за управување со квалификувани сертификати, издавачот задолжително обезбедува присуство на најмалку двајца вработени истовремено кои имаат одобрение за пристап.

Одобрение за пристап се дава на вработените чие присуство е неопходно за нормално работење на системот.

Издавачот треба да има список на лицата кои имаат одобрение за пристап.

Лицата без одобрение можат да имаат пристап до системот само во итни случаи во придружба на лице кое има одобрение, освен ако тоа го загрозува животот и здравјето на лицето со одобрение.

Секој пристап до системот задолжително се евидентира.

Член 15

Информационо-телекомуникациона опрема која е поврзана со друга информационо-телекомуникациона мрежа, издавачот е должен да ја обезбеди со сигурносни механизми (систем за спречување и откривање на упад и огнен заштитен ѕид и слично), кои спречуваат неовластен пристап до овие мрежи и овозможуваат пристап само по протокол кој е неопходен за управување со квалификувани сертификати.

Член 16

Во информациониот систем кој е организиран на начин што постои комуникација преку друга мрежа до системот за управување со квалификувани сертификати, комуникација треба да биде шифрирана.

Член 17

Информациониот систем на издавачот на квалификувани сертификати треба да биде составен исклучиво од машинска и програмска опрема која е неопходна за управување со квалификувани сертификати.

Член 18

Во правилата издавачот треба да утврди дека, податоците за електронско потпишување кои не се потребни за проверување на други податоци, по истекот на важноста се поништуваат.

Член 19

Со правилата издавачот треба да утврди дека податоците кои влијаат на сигурноста на дејноста на издавачот, не смеат на неконтролиран начин да го напуштат неговиот систем или просторот, со кој може да се загрози вршењето на дејноста согласно со важечките прописи и правилата на издавачот и дека сите средства за чување на податоци после употребата треба да се отстранат и задолжително да се уништат.

Член 20

Во правилата издавачот утврдува дека информациониот систем на издавачот за управување со квалификуваните сертификати треба да има вградено доволно сигурносни механизми кои спречуваат злоупотреба од вработените и овозможуваат јасна поделба на задачите согласно со овој правилник.

Сигурносните механизми од став 1 на овој член, треба да обезбедуваат контролиран пристап на податоците и евиденција на пристапот до ниво на поединец и тоа за сите дејствија кои влијаат на управување со квалификуваните сертификати.

Член 21

Издавачот со опремата и постапките обезбедува единственост на податоците за проверка на електронскиот потпис, односно обезбедува недвосмислена и сигурна идентификација на носителот на сертификатот врз основа на податоците за електронско потпишување.

Додека со програмската опрема која се употребува за генерирање на податоците за електронско потпишување треба да обезбеди да се избегне злоупотребата на овие податоци во најмала можна мерка со моментално достапната технологија.

Член 22

Во правилата се утврдува дека издавачот организира приемна служба каде лично и со употреба на службени документи со слика се утврдува идентитетот на лицата кои се носители на квалификуван сертификат или бараат издавање на таков сертификат.

За правните лица службата од став 1 на овој член е должна да побара и друга потребна документација за идентификација.

Член 23

Со правилата треба да се утврди поделба на задачите на вработените кај издавачот, така што ќе се оствари јасна поделба помеѓу задачите од областа на управувањето со квалификуваните сертификати, од задачите од областа на управувањето со информационите системи и задачите од областа на сигурноста и контролата, со што ќе се спречи секаква злоупотреба.

Член 24

Овој правилник влегува во сила осмиот ден од денот на објавувањето во "Службен весник на Република Македонија".

Бр.
17.август 2001 година

МИНИСТЕР,
Никола Груевски