Врз основа на член 30 од Законот за податоците во електронски облик и електронски потпис (“Службен весник на Република Македонија” бр.34/01 и 6/02), министерот за финансии донесе

П Р А В И Л Н И К
ЗА ПОТРЕБНАТА ОПРЕМА И СИСТЕМ ЗА ЧУВАЊЕ НА СЕРТИФИКАТИ И КВАЛИФИКУВАНИ СЕРТИФИКАТИ

Член 1

Со овој правилник се пропишуваат техничките услови и стандарди за потребната опрема и систем за чување на сертификати од страна на издавачите на сертификати.

Систем за чување на сертификати опфаќа: физичка и техничка безбедност на просториите, управување со системите, безбедноста и основните операции, континуитет на работењето, временска синхронизација, идентификација и потврдување на веродостојноста, контрола на пристапот до мрежата и системите, управување, генерирање, објавување, користење, менување, уништување, чување, резервно копирање и обновување на клучеви, евидентирање, чување, резервно копирање и обновување на податоци, генерирање и објавување на сертификати и управување со поништени сертификати.

Одредбите од овој правилник се однесуваат на издавачите на сертификати, освен доколку со овој правилник за издавачите на квалификувани сертификати не е поинаку уредено.

Член 2

Издавачот на сертификати треба да користи опрема, постапки и методи за администрирање и управување со безбедноста на користената инфраструктура, кои се во согласност со општоприфатените стандарди за управување со информатичка безбедност.

Член 3

Системот и техничката опрема што се користат за обезбедување услуги за регистрација на барателот, генерирање сертификати, објавување на информации за правилата и сертификатите, управување со поништени сертификати, како и за другите услуги коишто ги нуди издавачот на сертификати мора да бидат дизајнирани и користени исклучиво за таа намена.

Член 4

Лицата задолжени за управување кај издавачот на сертификати иницираат, а контролорите на системот спроведуваат внатрешни контроли најмалку еднаш годишно, но и во кој било случај на промена која влијае врз безбедноста на системот.

Кај издавачот на сертификати се води детална евиденција за изршената оценка на работењето, како и за условите и обемот за извршените внатрешни и надворешни контроли.

Член 5

Издавачот на сертификати треба да ја чува документацијата во врска со тековната состојба на техничката опрема и технологиите кои ги користи најмалку 5 (пет) години по престанокот на користењето на истите.

Член 6

Физички пристап до капацитетите, информациите и системите на издавачот на сертификати имаат само овластените лица определени од органот на управување.

Доколку е потребен пристап на друго лице до капацитетите, информациите и системите на издавачот на сертификати, истото треба да биде придружувано и надгледувано од овластено лице.

Издавачот на сертификати треба да обезбеди:

- Просториите кои се користат за функциите на управување со сертификати и клучеви да се под 24-часовно физичко и електронско набљудување заради спречување на неовластен пристап;
- Опремата, информациите, медиумите и програмата кои ги користи издавачот на сертификати да не можат да бидат изнесени од просториите без овластување; и
- Да се води евиденција на секој пристап во просториите и да се врши периодична контрола врз истата.

Физичкото обезбедување на просториите на издавачот на сертификати треба да има јасен опис кој вклучува:

- Безбедносни зони кои се воспоставени и нивните безбедносни карактеристики;
- Врските со заштитените добра; и
- Целосен и ажуриран список на лица вработени кај издавачот на сертификати кои имаат право на пристап до определните зони, кој е достапен на увид.

Ажурирањето на описот и списокот на лица вработени кај издавачот на сертификати кои имаат пристап до определните зони, органот на управување треба да го додели на лице вработено кај издавачот на сертификати, кое треба да врши негова периодична проверка.

Чувствителниот материјал, чиј животен век завршил, треба да се уништи на безбеден начин.

Член 7

Издавачот на сертификати треба на лицето задолжено за регистрациски работи да му обезбеди соодветен простор, кој ќе биде безбеден за складирање на информациите за барателите.

Техничката опрема за работа на лицето одговорно за регистрациски работи треба да биде заштитена од неовластен пристап.

Член 8

Капацитетите на издавачот на сертификати се заштитуваат од ризиците во опкружувањето преку примена на мерки и контроли со кои се намалува ризикот од потенцијални закани, вклучувајќи кражба, пожар, експлозии, чад, вода, прашина, вибрации, хемиски влијанија, пречки во снабдувањето со електрична енергија и електромагнетно зрачење.

Член 9

Издавачот на сертификати треба да овозможи управување со системот на безбеден начин. Издавачот на сертификати треба да осигура дека вработените лица и правилата кои ги применува ја оддржуваат и подобруваат доверливоста на пропишаните услуги.

Член 10

Издавачот на сертификати со правилата треба да овозможи системот да:

- функционира исправно и безбедно;
- се употребува на начин со кој ризикот од неисправност на системот е минимален;
- биде заштитен од вируси и други потенцијално ризични и штетни програми, за да го осигура интегритетот на податоците кои тој ги обработува.

Издавачот на сертификати треба да ги почитува инсталациските, административните и корисничките упатства на производителите на користената техничка опрема и технологии и доколку е неопходно да изработи дополнителна документација.

Член 11

Преку континуитетот на работењето се обезбедува услугите на издавачот на сертификати да се достапни и во случај на неисправност на техничката опрема или системот.

Во случај на неисправност, системот мора да обезбеди непрекинато извршување на следните услуги:

- објавување на сертификати;
- поништување на сертификати; и
- објавување на поништените сертификати.

Издавачот на квалификувани сертификати треба да обезбеди услугите од став 2 на овој член да бидат најмалку 99.9% достапни, освен во случај на виша сила или вонредна состојба кај издавачот.

Во случај на виша сила или вонредна состојба, издавачот на сертификати треба да продолжи со вршење на услугите употребувајќи алтернативен систем. Системите треба да овозможат примена на правилата на издавачот во кои се утврдува максималниот прифатлив застој при давањето на услугите.

Преминот од примарен систем на алтернативен систем и обратно не смее да предизвика ризик врз безбедносниот карактер на системите.

Член 12

Сите часовници на системите коишто издавачот на сертификати ги користи за обезбедување на услугите, кои зависат од времето, се синхронизираат до секунда според Co-ordinated Universal Time (во продолжение на текстот: UTC).

Издавачот на сертификати треба да употребува најмалку 2 (два) независни извори на UTC за да одржи стабилен временски извор, од кои едниот треба да биде хардверски извор на точно време, којшто е синхронизиран со службениот извор на UTC.

Исполнувањето на условот од став 2 од овој член е независен од кои било други временски услови кои се однесуваат на временскиот жиг.

Член 13

Идентификацијата и потврдувањето на веродостојноста треба да се користат за контрола на пристапот и да овозможат употреба на системите само од страна на овластени лица.

Одредбите од ставот 1 од овој член се применува на сите компоненти на управување кај издавачот на сертификати. Идентификацијата и потврдувањето на веродостојноста треба да се обезбедат на ниво на оперативен систем или на ниво на поединечни компоненти во системот.

Системите треба да го идентификуваат секој корисник и успешно да ја потврдат веродостојноста на истиот, пред да овозможат какво било дејствије во името на тој корисник или улогата претпоставена од истиот.

При повторното пријавување на корисник на системот, кој претходно се одјавил, системот треба да ја потврди неговата веродостојност.

Ако бројот на неуспешни обиди за потврдување на веродостојноста е еднаков на максималниот број на дозволени обиди, системот треба да ги оневозможи понатамошните обиди за потврдување на веродостојноста, освен ако лицето има улога на администратор.

Член 14

Системите треба да обезбедат можност за контрола и ограничување на пристапот преку давање на најмало ниво на привилегии на идентификуваните лица до компонентите на системот или функциите, во зависност од улогата на лицето.

Член 15

Издавачот на сертификати треба да применува контроли и огнени ѕидови за заштита на внатрешните сегменти на неговата мрежа од надворешен пристап.

Контролите и огнените ѕидови треба да бидат конфигурирани на начин што секој пристап и протокол кој не е потребен за функционирање на услугите на издавачот на сертификати ќе биде оневозможен.

Член 16

Издавачот на сертификати во рамките на својата инфраструктура употребува криптографски клучеви за да ги овозможи функциите на интегритет, доверливост и потврдување на веродостојноста. Управувањето со криптографските клучеви треба да се води на безбеден начин за да се заштитат овие клучеви од неовластена употреба, откривање, менување или замена, која би резултирала со загрозување на безбедноста.

Јавен клуч е клуч кој се користи при асиметрична енкрипција. Со секој јавен клуч во пар доаѓа и соодветен приватен клуч. Со помош на јавниот клуч може да се изврши енкрипција на податоците кои можат да бидат декритпирани само со соодветниот приватен клуч. Јавниот клуч се користи и при верификација на електронски потпишаните податоци (кои се потпишани со приватниот клуч).

Приватен клуч е клуч кој се користи при асиметрична енкрипција. Со секој приватен клуч во пар доаѓа и соодветен јавен клуч. Со помош на приватниот клуч може да се изврши декрипција на податоците кои се енкриптирани со јавниот клуч. Приватниот клуч се користи и при електронското потпишување на податоците.

Таен клуч е клуч кој се користи при симетрична енкрипција. Двете страни кои разменуваат податоци, мораат да го имаат истиот клуч како би ги декриптирале податоците. При енкрипцијата и декрипцијата се користи истиот таен клуч.

Издавачот на сертификати, во зависност од местото и начинот на употреба на клучевите, врши нивно групирање на најмалку следните категории:

- клучеви за потпишување на издавачот на сертификати, односно пар клучеви кои се користат за изработка на сертификати;
- инфраструктурни клучеви, односно клучеви користени од издавачот на сертификати за потврдување на под-системите, потпишување на контролните записи, енкрипција на пренесените или зачувани податоци и друго; и
- оперативни клучеви, кои се користат од вработените лица кои го управуваат или користат системот на издавачот, како и за потврдување, потпишување или доверливост.

Член 17

Клучевите за потпишување на издавачот на сертификати треба да бидат генерирани во безбеден криптографски модул.

Креирањето на клучеви за потпишување на издавачот треба да биде во опкружување кое е физички заштитено во согласност со членовите 6, 7 и 8 од овој правилник и под контрола на најмалку две вработени лица.

Безбедниот криптографски модул во кој се генерираат клучевите за потпишување на издавачот треба да биде евалуиран и сертифициран најмалку според еден од следните стандарди или друг соодветен стандард:

- FIPS140-1 или FIPS140-2, ниво 3 или повисоко;

- CEN CWA 14167-2, 14167-3 и 14167-4; и
- ISO/ IEC 15408 ниво EAL 4 или повисоко.

Клучевите на издавачот треба да користат SHA-1-RSA.

Ако клучевите на издавачот се со важност до 2012 година, тогаш потребната должина на клучевите треба да биде најмалку 1280 бита.

Ако клучевите на издавачот се со важност до 2022 година, тогаш потребната должина на клучевите треба да биде најмалку 2048 бита.

Клучевите на издавачот не треба да бидат со важност подолга од 20 години.

Издавачот на сертификати со правилата треба да ги пропише:

- сите значајни безбедносни операции; и
- описот на задачите (улогите) на присутните лица при постапката за генерирање на клучеви на издавачот на сертификати, во која како сведоци учествуваат надворешен експерт и нотар.

Сите присутни лица и сведоци треба да потпишат изјава со која потврдуваат дека постапката е спроведена во согласност со правилата.

Доказите дека постапката за генерирање на клучеви на издавачот на сертификати е изведена под соодветна контрола треба да бидат достапни на барање на заинтересирани лица.

Член 18

Инфраструктурните клучеви треба да бидат генерирани во безбеден криптографски модул. Безбедниот криптографски модул треба да биде евалуиран и сертифициран најмалку според FIPS140-1 или FIPS140-2 ниво 2 или друг соодветен стандард. За креирање на клучевите за електронски потпис и криптирање треба да се користат следните алгоритми:

- Електронски потпис: SHA-1 со RSA клуч, чија должина треба да биде најмалку 1024 бита;
- Енкрипција: AES 256, 3DES; и
- Хеш алгоритми: SHA-1.

Член 19

Оперативните клучеви треба да бидат генерирани во безбеден криптографски модул. Овој криптографски модул треба да биде евалуиран и сертифициран најмалку според FIPS140-1 или FIPS140-2 ниво 2 или друг соодветен стандард. За креирање на клучевите за електронски потпис и криптирање треба да се користат следните алгоритми:

- Електронски потпис: SHA-1 со RSA клуч, чија должина треба да биде најмалку 1024 бита;
- Енкрипција: AES 256, 3DES; и
- Хеш алгоритми: SHA-1.

Член 20

Приватните и тајните клучеви не може да се објавуваат во некриптирана форма.

Јавните клучеви, кои не се сертифицирани, треба да се чуваат безбедно за да се спречи каква било можност од пресретнување или манипулација.

Јавниот клуч поврзан со клучевите за потпишување на издавачот и/или Инфраструктурните клучеви може да се објавуваат до носителите на сертификати и до трети лица. Интегритетот и веродостојноста на овој јавен клуч и другите поврзани параметри треба да се одржуваат во текот на првичното и секое следно објавување.

Јавниот клуч поврзан со клучевите за потпишување на издавачот на сертификати може да се дистрибуира во сертификат потпишан од самиот издавач или издаден од друг издавач. Самопотпишаниот сертификат на издавачот треба да ги има следните карактеристики:

- потписот на кој се однесува сертификатот треба да има можност за потврдување користејќи ги податоците содржани во сертификатот;

- полињата за носителот на сертификатот и издавачот треба да бидат идентични.

Издавачот на сертификати треба да овозможи создавање отпечаток („fingerprint„) на самопотпишан сертификат користејќи SHA-1 хеш алгоритми.

Член 21

Пристапот до сите безбедни криптографски модули кои се користат за клучевите за потпишување, инфраструктурните клучеви и оперативните клучеви на издавачот на сертификати треба да се контролира.

Издавачот на сертификати треба да воспостави контрола од најмалку две лица врз административните функции при генерирање сертификати за оперативните клучеви.

Клучевите за потпишување на издавачот на сертификати треба да бидат користени исклучиво за потпишување на сертификати и за листите на поништени сертификати.

Инфраструктурните клучеви треба да бидат користени исклучиво за заштита на: системите на издавачот, инфраструктурните услуги и податоците.

Оперативните клучеви и сертификатите треба да бидат користени исклучиво за администрирање на системот на издавачот.

Издавачот на сертификати треба да обезбеди екстензијата (атрибутот) на X.509, која ја определува намената на јавниот клуч да биде присутна во сите издадени сертификати. Ако полето на екстензијата (атрибутот) за намена на клучот содржи непорекнување, тогаш истиот не смее да има друга намена.

Екстензијата (атрибутот) на X.509, која ја определува намената на јавниот клуч во сертификатите, треба да соодветствува со RFC 3280 Internet X.509 public key infrastructure certificate и Certificate Revocation List (листа на поништени сертификати) профил или понов.

Екстензијата (атрибутот) на X.509, која ја определува намената на јавниот клуч во квалификуваните сертификати, покрај условите од претходниот став, треба да соодветствува и со ETSI TS 102 280 V1.1.1 (2004-03), X.509 V.3 профил на сертификат – за сертификати издадени на физички лица.

Член 22

Инфраструктурните клучеви и оперативните клучеви се менуваат најмалку еднаш годишно.

Ако кој било од алгоритмите кои се користат се смета дека повеќе не е безбеден, тогаш клучевите кои се засноваат на тој алгоритам мора веднаш да се променат.

Менувањето на клучот треба да се изведе на безбеден начин.

Член 23

Кога на клучевите за потпишување на издавачот на сертификати им истекува важноста, тие се уништуваат на начин што ќе оневозможи нивно обновување.

Системите на издавачот на сертификати ќе овозможат анулирање на приватните и тајните клучеви, кои се зачувани во хардверот или софтверот во некриптирана форма.

Софтверското уништување на клучот треба да се изведе користејќи безбедни постапки за бришење што целосно ги презапишуваат клучевите, односно вршат повеќекратно презапишување, демагнетизирање или го распарчуваат медиумот за магнетно чување.

Член 24

Сите приватни и тајни клучеви треба да се чуваат безбедно.

Клучот за потпишување на издавачот треба да се чува во безбеден криптографски модул, којшто ги исполнува условите за евалуација и сертификација наведени во член 17 од овој правилник.

Приватните и тајните инфраструктурни клучеви треба да се чуваат во безбеден криптографски модул, коишто ги исполнуваат условите за сертификација наведени во член 18 од овој правилник.

Приватните и тајните оперативни клучеви треба да бидат зачувани во безбеден криптографски модул, кој што ги исполнува условите за сертификација наведени во член 19 од овој правилник.

Ако кој било приватен или таен клуч во безбеден криптографски модул се извезува од тој модул, треба претходно да се заштити во самиот модул за да се обезбеди неговата доверливост. Извезените приватни или тајни клучеви треба да се заштитат со AES 256, 3DES или со друг алгоритам за енкрипција со слична јачина. Кој и да било друг чувствителен материјал не смее да се чува незаштитен.

Издавачот на сертификати треба да обезбеди обновувањето на приватните или тајни клучеви за потпишување, клучевите за инфраструктура и оперативните клучеви од резервната копија исклучиво да се извршува од овластени лица, односно од страна на лицето одговорно за безбедност.

Издавачот на сертификати треба да обезбеди обновувањето од резервната копија на приватните клучеви за потпишување на издавачот на сертификати исклучиво да се изведе под контрола на најмалку две лица.

Член 25

Издавачот на серитификати не треба да ги чува податоците за електронско потпишување во согласност со член 30 од Законот за податоците во електронски облик и електронски потпис, односно не треба да прави резервни копии и да не дозволи депонирање на приватните клучеви за потпишување на носителот на сертификатот.

Член 26

Во системот се евидентираат следните настани:

- управување со клучевите на издавачот;
- барања од носителите на сертификати;
- договори со носителите на сертификати;
- управување со сертификати (издавање, поништување, суспендирање, ажурирање);
- издадени сертификати;
- приватни клучеви за декрипција на носителот на сертификатот, доколку оваа услуга ја обезбедува издавачот;
- извештаи и кореспонденција за неусогласеност и компромитација; и
- сите обиди за влез во системите и безбедносните средства.

Член 27

Издавачот на квалификувани сертификати ги чува податоците и информациите утврдени во член 26 од овој правилник и другата евиденција на начин утврден во неговите правила за работа, на медиуми соодветни за зачувување и обезбедување на потребни правни докази како поддршка на електронскиот потпис.

Издавачот на квалификувани сертификати треба да ги чува сите дејствија поврзани со управувањето на клучевите на издавачот на квалификуваните сертификати, информацијата за управување со квалификуваните сертификати, како и сите други релевантни податоци утврдени во член 32 од Законот за податоци во електронски облик и електронски потпис најмалку 30 (триесет) години.

Издавачот на сертификати треба да ги чува барањата, договорите и кореспонденцијата помеѓу носителот и издавачот на сертификати, како и другите документи утврдени со член 23 од Законот за податоци во електронски облик и електронски потпис најмалку 5 (пет) години.

Доколку издавачот на сертификати нуди услуга на чување на приватни клучеви за декрипција на носителот на сертификатот, тогаш треба да ги чува најмалку 30 (триесет) години.

Доверливите приватни клучеви од кои издавачот на сертификати направил резервна копија треба да се заштитат на ниво на физичка и криптографска заштита, која е еднаква или поголема од постојната кај издавачот.

Втората копија на целиот сочуван материјал треба да се чува во просторија која се наоѓа надвор од просториите на издавачот и која треба да биде физички и криптографски заштитена. Издавачот на сертификати треба за таквата просторија да обезбеди соодветни физички и технички контроли утврдени во членовите 6, 7 и 8 од овој правилник.

Издавачот на сертификати треба да обезбеди електронски потпис, хеш или код за потврда на веродостојноста за секој сочуван запис или пресметан за целокупната евиденција. Издавачот на сертификати треба да обезбеди потврда на интегритетот на архивираните податоци.

Издавачот на сертификати треба да го проверува и потврдува интегритетот на резервните копии зачувани во главната локација најмалку еднаш годишно и да врши периодична проверка на интегритетот на материјалот зачуван надвор од главната просторија.

Член 28

Резервното копирање и обновување ги опфаќа податоците за системот, носителите на сертификати и други податоци, кои се потребни за да се обнови системот во случај на техничка неисправност или непогода, но не ги опфаќа клучевите за резервно копирање и обновување, како и условите за безбедност кои се утврдени во член 24 од овој правилник.

При генерирање на резервна копија издавачот на сертификати треба да обезбеди:

- редовно генерирање на резервни копии;
- зачуваните резервни податоци да бидат доволни за да се обнови системот;
- вработеното лице со доволно привилегии да биде во можност по потреба да генерира резервни копии.

Издавачот на сертификати треба да обезбеди интегритет и доверливост на резервните копии и притоа:

- резервните копии треба да се заштитат од модификации преку користење на електронски потписи, хешови или кодови за потврдување на веродостојноста;
- клучните безбедносни параметри и други доверливи податоци треба да се чуваат исклучиво во енкриптирана форма. Енкрипцијата треба да ги исполни криптографските услови за инфраструктурни клучеви, наведени во член 18 од овој правилник.

Издавачот на сертификати треба да обезбеди:

- системот да има функција за обновување, која ќе овозможи негово обновување преку резервните копии; и
- вработеното лице со доволно привилегии да биде во можност да ги употреби резервните копии по потреба.

Член 29

Која било порака создадена преку која било услуга треба да биде заштитена користејќи ги инфраструктурните клучеви, доколку се пренесуваат преку мрежа која не е безбедна содржи време на пораката, кое ќе го посочи времето кога испраќачот ја составил пораката.

Член 30

Издавачот на сертификати генерира сертификат користејќи го јавниот клуч на носителот на сертификатот и на тој начин го поврзува јавниот клуч со идентитетот на носителот на сертификатот.

Издавачот на сертификати треба да обезбеди сите постапки и услови кои се однесуваат на барањето, генерирањето и објавувањето да се наведат во јавниот дел од правилата на издавачот или во друг документ, кој е јавно достапен.

Издавачот на сертификати треба во своите правила да го одреди начинот на потврдување на приемот и адекватноста на сертификатот од страна на носителот.

Издавачот на сертификати применува соодветни мерки кои овозможуваат доверливо и безбедно издавање на сертификати, а особено:

- применува соодветен механизам кој ќе обезбеди доказ за идентитетот на носителот кој бара издавање сертификат за да се осигура дека тој е вистинскиот носител на приватниот клуч, кој е поврзан со јавниот клуч за кој се бара сертификација;
- исклучиво генерирање сертификати кои се конзистентни со профилите, кои се наведени во јавниот дел од правилата на издавачот на сертификати.

Повторната сертификација и/или повторното издавање на клуч на носителот на сертификатот треба да биде безбедно изведена како и при првото генерирање на сертификатот.

Секој квалификуван сертификат треба да ги содржи карактеристиките наведени во член 25 од Законот за податоци во електронски облик и електронски потпис.

Сите издадени сертификати треба да бидат во согласност со RFC 3280 Internet X.509 public key infrastructure certificate и Certificate Revocation List (листа на поништени сертификати) профил или понов.

Сите издадени квалификувани сертификати треба бидат во согласност со:

- RFC 3039 Internet X.509 public key infrastructure qualified certificates профил или понов;
- TS 101 862 v1.3.1 профил на квалификуван сертификат или понов; и
- TS 102 280, X.509 V.3 профил на сертификат за сертификати издадени на физички лица или понов.

Член 31

Лицето задолжено за регистрациски работи го потврдува идентитетот и доколку е потребно и други карактеристики кои се однесуваат на лицето на кое му е издаден сертификатот или квалификуваниот сертификат. Лицето одговорно за регистрациски работи треба да применува соодветни безбедносни мерки, а особено:

- Ако барањето за сертификат содржи чувствителни информации за барателот, истото треба да биде заштитено пред да биде испратено од лицето одговорно за регистрација до лицата одговорни за генерирање сертификати, притоа обезбедувајќи доверливост на пораката, доколку се пренесува преку мрежа која не е безбедна;
- Издавачот на квалификувани сертификати треба да применува постапка за регистрација која овозможува собирање на доволно податоци за барателот за да ги задоволи барањата за квалификуван сертификат кои се наведени во член 25 од Законот за податоци во електронски облик и електронски потпис;
- Издавачот на квалификувани сертификати треба да обезбеди барањето да содржи време на поднесување на барањето; и
- можност за избор на барателот за објавување или необјавување на сертификатот и други јавни информации.

Барањата за квалификувани сертификати, кои лицето одговорно за регистрација ги испраќа во електронска форма до лицето одговорно за генерирање сертификат, треба да бидат електронски потпишани;

Издавачот на сертификати применува механизми и безбедносни контроли за да ги заштити приватноста и доверливоста на податоците за барателот и носителот.

Член 32

Објавувањето на квалификуван сертификат треба да биде ограничено на носителот на сертификатот и на определени трети лица, во согласност со ограничувањата побарани од носителот.

Правилата за контрола на пристапот до складираните сертификати треба да бидат дефинирани на начин што ќе овозможи безбедно управување со зачуваните податоци и притоа:

-пристап за читање треба да им биде дозволен на носителите на сертификати и на овластените лица, во согласност со јавниот дел од правилата на издавачот; и

- пристап за пишување треба да биде единствено достапен на овластените лица вработени кај издавачот, во согласност со правилата на издавачот.

Член 33

Издавачот на сертификати треба да воспостави систем на давање услуги и применување на постапки со кој се овозможува навремено поништување или суспендирање на сертификатите врз основа на овластени и проверени барања. Постапките треба да се утврдат во јавниот дел од правилата на издавачот на сертификати, а особено:

- лица кои и начини на кои можат да поднесат барање за поништување или суспендирање;

- условите за дополнителна проверка на барањата за поништување во случај трета страна да пријави компромитирање на клучевите на носителот на сертификатот;

- можноста сертификатите да се суспендираат и од кои причини;

- механизмот кој се користи за објавување на информациите за поништени сертификати; и

- максималното дозволено време што може да измине од приемот на барањето за поништување до објавувањето на информацијата за извршено поништување.

Сертификатот се поништува во случаите утврдени во член 18 од Законот за податоци во електронски облик и електронски потпис, како и во другите случаи утврдени во јавниот дел од правилата на издавачот.

Суспендирањето на сертификатот не е задолжителна услуга.

Издавачот на сертификати треба да применува соодветни мерки за да обезбеди барањата за поништување или суспендирање на сертификатот да се управувани на безбеден и одговорен начин, а особено:

- секое барање за суспендирање, престанок на суспензија и поништување треба да биде соодветно проверено и потврдено;

- еднаш поништен сертификат не може да биде повторно активиран;

- барањата поврзани со поништувањето или суспендирањето треба навремено да се процесираат. Максималното дозволено време што може да измине од приемот на барањето за поништување или суспендирање на квалификуван сертификат до објавувањето на информација за извршено поништување или суспендирање не смее да биде подолго од 24 часа;

- поништувањето на сертификатите поврзани со клучевите за потпишување на издавачот на сертификати исклучиво може да се врши под контрола на најмалку две вработени лица;

- базата на податоци за состојбата на квалификуваните сертификати треба да биде ажурирана веднаш штом се изврши промена на состојбата; и

- услугата на објавување на поништени квалификувани сертификати треба да е достапна 24 часа на ден и 7 дена во неделата.

Издавачот на квалификувани сертификати треба да ги исполнува условите наведени во член 27 од Законот за податоци во електронски облик и електронски потпис.

Издавачот на сертификати применува соодветни постапки и услуги за објавување на состојбата на сертификатите. Објавувањето се остварува со користење на:

- регистар на поништени сертификати усогласен со RFC 3280 Internet X.509 public key infrastructure certificate или понов; или

- On-Line Certificate Status Protocol (онлајн протокол за проверка на состојбата на сертификатот).

Издавачот на сертификати треба да применува соодветни мерки со кои обезбедува безбедно и одговорно објавување на состојбата на поништени сертификати, а особено:

- да се заштити интегритетот и веродостојноста на информациите за состојбата;

- информациите за состојбата со поништени сертификати да се јавно достапни;

- информациите за состојбата со поништени сертификати да вклучат информации за состојбата на сертификатите најмалку до моментот на истекување на важноста на сертификатот;

- услугата на поништување на сертификати треба да биде достапна 24 часа на ден и 7 дена во неделата; и

- издавачот на сертификати треба да биде во можност да поништи кој било сертификат кој го издал, дури и во случај на непогоди.

Член 34

Издавачот на сертификати треба да го следи развојот на технологиите и светските стандарди и да ги ажурира своите правила и системи во согласност со најновите светски стандарди.

Правилата на издавачот на сертификати треба детално да ги регулираат правилата утврдени со Законот за податоци во електронски облик и електронски потпис и со подзаконските акти и применливите светски стандарди. Правилата на издавачот на сертификати треба јавно да се објават и постојано да се усогласуваат со следните сегашни или понови стандарди и препораки:

- RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy и Certification Practices Framework (Рамка за издавање сертификати); и/или

- ETSI TS 102 042 V1.2.2 (2005-06) Policy requirements for certification authorities issuing public key certificates (Правила за издавачите кои издаваат сертификати за јавни клучеви).

Правилата на издавачот на квалификувани сертификати:

- треба да бидат во согласност со Правилникот за содржината на правилата на издавачот на сертификати;

- треба да бидат во согласност со ETSI TS 101 456 V1.3.1 (2005-05) Policy requirements for certification authorities issuing qualified certificates (Правила за издавачите кои издаваат квалификувани сертификати).

Издавачот на сертификати треба да користи алгоритми за клучевите за потпишување, инфраструктирните клучеви, оперативните клучеви и другите криптографски операции утврдени во членовите 17, 18 и 19 или алгоритам којшто е општоприфатен како соодветен за таа намена според ETSI SR 002 176 V1.1.1 (2003-03) „Special Report: Algorithms and Parameters for Secure Electronic Signatures„ („Специјален извештај: Алгоритми и параметри за безбедни електронски потписи„) или поновите верзии на овој документ кои ќе бидат објавени:

- ETSI TS 102 176-1 Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms (Алгоритми и параметри за безбедни електронски потписи; Дел 1: Функции на хешовите и асиметричните алгоритми); и

- ETSI TS 102 176-2 Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices (Алгоритми и параметри за безбедни електронски потписи; Дел 2: Безбедни канали за протоколи и алгоритми за средствата за електронско потпишување).

Издавачот на сертификати треба да воспостави внатрешни правила и да презема мерки кои ќе овозможат повисок степен на безбедност на системите во согласност со стандардот BS7799 / ISO17799.

Член 35

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

Бр. 16-10104/1
22 март 2006 година
Скопје

Министер за финансии,
м-р **Никола Поповски**, с.р.