20200530947

МИНИСТЕРСТВО ЗА ИНФОРМАТИЧКО ОПШТЕСТВО И АДМИНИСТРАЦИЈА

Врз основа на член 18 став (3) од Законот за електронски документи, електронска идентификација и доверливи услуги (*) („Службен весник на Република Северна Македонија“ бр. 101/19 и 275/19), министерот за информатичко општество и администрација донесе

ПРАВИЛНИК ЗА ПРОЦЕДУРИТЕ И СТАНДАРДИТЕ ЗА ИСПОЛНЕТОСТ НА ТЕХНИЧКИТЕ, ФИЗИЧКИТЕ И ОРГАНИЗАЦИСКИТЕ МЕРКИ ЗА СИГУРНОСТ НА ШЕМИ ЗА ЕЛЕКТРОНСКА ИДЕНТИФИКАЦИЈА

Член 1

Со овој правилник се пропишуваат процедурите и стандардите за исполнетост на техничките, физичките и организациските мерки за сигурност на шеми за електронска идентификација.

Член 2

Во рамки на регистрираната шема за електронска идентификација, нивото на сигурност на средствата за електронска идентификација издадени во истата, се обезедува преку:

а) процедури за управување со средства за електронска идентификација;

б) процедури за автентикација на средствата за електронска идентификација;

в) процедури и стандарди за исполнетост на техничките, физичките и организациски мерки за сигурност на шеми за електронска идентификација.

Средствата за електронска идентификација издадени во рамките на регистрираната шема за електронска идентификација кои обезбедуваат повисоко ниво на сигурност, се смета дека го обезбедуваат и пониското ниво на сигурност.

Член 3

Одделни изрази употребени во овој правилник го имаат следното значење:

- „доверлив извор“ е вид на извор на потребни податоци на кој може да му се верува дека обезбедува точни податоци или докази што можат да се користат за докажување на идентитетот на лицето кое употребува средство за електронска идентификација;

- „фактор на автентикација“ е одреден фактор наведен во електронска форма кој се смета за суштински во процесот на автентикација, а за кој постои потврда дека е поврзан со лицето кое се повикува на тој фактор. Факторот за автентикација може да биде еден од следните категории:

(а) „фактор за автентикација што се поседува“ е фактор за автентикација за кој се бара субјектот на електронска идентификација да докаже дека го поседува како дел од средството за идентификација;

(б) „фактор за автентикација што се знае“ е фактор за автентикација за кој се бара субјектот на електронска идентификација да докаже дека знае одредени информации кои се поврзани со средството за електронска идентификација;

(в) „фактор за автентикација што е својствен“ е фактор за автентикација кој се заснова на физички атрибути на лицето кое е субјект на електронска идентификација, а кој фактор субјектот на електронска идентификација е должен да докаже дека го има;

- „динамична автентикација“ е електронски процес со употреба на криптографски или други техники преку кои се обезбедува создавањето на средства за електронска идентификација во форма на електронска потврда или доказ дека субјектот на електронска идентификација ги поседува или ги има податоците за идентификација и истата се менува во системот што го потврдува идентитетот на субјектот на електронска идентификација и е различен за секоја поединечна автентикација на субјектот;

- „управување со безбедност на мрежи и информациски системи“ е способност на мрежните и информациските системи, на одредено ниво на доверба, да се спротивстават на какво било дејство кое ја компромитира достапноста, автентичноста, интегритетот или доверливоста на складираните или пренесените или обработените податоци или поврзаните услуги што ги нудат или се достапни преку тие мрежи и информациски системи;

- „јазол“ е точка на поврзување што е дел од архитектурата за интероперабилност за електронска идентификација и е вклучена во прекугранична автентикација на лица и има можност да ги препознае и обработува или да изврши пренос во други јазли преку користење на национална инфраструктура за електронска идентификација до интерфејс на национална инфраструктура за електронска идентификација на друга држава;

- „оператор на јазол“ е правно лице одговорно за одржување на јазолот и кое ги извршува правилно и сигурно своите функции како точка за поврзување.

Член 4

Процедурите и стандардите кои се однесуваат на техничките мерки за сигурност на шемата за електронска идентификација се применуваат и за средствата за електронска идентификација кои се издадени во рамки на самата шема за електронска идентификација.

Шемите за електронска идентификација може да бидат со ниско, значително и високо ниво, во однос на процедурите кои ги користат за:

- пријавување и регистрација на субјект на електронска идентификација,
- проверка на идентитет и верификација на физички лица или
- проверка на идентитет и верификација на правни лица.

Во зависност од нивото во кое спаѓа шемата за електронска идентификација, во истото ниво за електронска идентификација се и средствата за електронска идентификација издадени во рамки на таа шема.

Јазлите треба да се разликуваат помеѓу телата на јавниот и приватниот сектор преку техничките средства што се употребуваат.

Член 5

Нивото на сигурност на шемата за електронска идентификација во фаза на пријавување и регистрација може да биде:

- ниско ниво на сигурност,
- значително ниво на сигурност и
- високо ниво на сигурност.

При употребата на шемите за електронска идентификација за ниско, значително и високо ниво на сигурност во фазата на пријавување и регистрација треба:

- субјектот на електронска идентификација да биде запознаен со условите поврзани со користењето на средствата за електронска идентификација,
- субјектот на електронска идентификација да биде запознаен со препораките за мерките за безбедност поврзани со средството за електронска идентификација и

- да се обезбедат сите релевантни податоци за идентитетот на субјектот на електронска идентификација кои се потребни за докажување на поврзаноста на средството за електронска идентификација со субјектот на електронска идентификација и верификација на неговиот идентитет.

Член 6

Нивото на сигурност на шемата за електронска идентификација во фаза на проверка на идентитет и верификација на физички лица може да биде:

- ниско ниво на сигурност,
- значително ниво на сигурност и
- високо ниво на сигурност.

Член 7

При употребата на шемата за електронска идентификација на ниско ниво на сигурност во фазата на проверка на идентитет и верификација на физичкото лице треба:

- да се смета дека физичкото лице го поседува доказот кој се бара за издавање на средството за електронска идентификација;
- да се смета дека физичкото лице го поседува доказот кој се бара за издавање на средството за електронска идентификација во оригинал или според податоците добиени од доверлив извор упатуваат на тоа дека доказот е валиден;
- според податоците кои се добиени од доверлив извор, да може да се потврди дека физичкото лице постои и дека истото физичко лице е поврзано со идентитетот кој го прикажува.

Член 8

При употребата на шемата за електронска идентификација на значително ниво на сигурност, покрај стандардите кои се однесуваат на шемата за електронска идентификација на ниско ниво на сигурност во фазата на проверка на идентитет и верификација на физички лица, треба:

- со сигурност да се утврди дека физичкото лице го поседува доказот кој се бара за издавање на средството за електронска идентификација во оригинал или според доверлив извор е потврдено дека физичкото лице постои и преземените мерки за проверка на идентитет да упатуваат на истото физичко лице, земајќи го предвид ризикот од изгубен, украден, суспендиран, одземен или истечен доказ со кој располага доверливиот извор или
- физичко лице да има приложено доказ за негова лична идентификација заради издавање на средство за електронска идентификација и се преземени мерки за намалување на ризикот дека доказот за лична идентификација е изгубен, украден, суспендиран, одземен или истечен или
- процедурата за проверка на идентитетот на физичкото лице кое бара издавање на средство за електронска идентификација да биде веќе спроведена од страна на регистриран или признаен давател на доверливи услуги за издавање на напреден електронски потпис и таа процедура да има еквивалентна важност според извештаите на телото за оцена на сообразност или
- на физичкото лице за кое се врши проверката веќе да му е издадено еквивалентно валидно средство, односно напреден електронски потпис кој е издаден од страна на регистриран или признаен давател на доверливи услуги.

Член 9

При употребата на шемата за електронска идентификација на високо ниво на сигурност, освен стандардите кои се однесуваат на шемата за електронска идентификација на значително ниво на сигурност во фазата на проверка на идентитет и верификација на физички лица, треба:

- проверката на идентитетот на физичкото лице да биде спроведена со користење на биометриски податоци или физички карактеристики кои на единствен начин го поврзуваат лицето со документот за лична идентификација за што има и потврда од доверлив извор или

- претходно да биде веќе извршена проверка на идентитетот на физичкото лице заради издавање на друго еквивалентно средство, односно квалификуван електронски потпис од страна на друг давател на квалификувана доверлива услуга и се преземени мерки за потврда на валидноста на претходно извршената проверка или

- на физичкото лице за кое се врши проверката веќе му да му е издадено еквивалентно валидно средство, односно квалификуван електронски потпис кој е издаден од страна на регистриран или признаен давател на квалификувани доверливи услуги.

Член 10

При употребата на шемата за електронска идентификација на ниско ниво на сигурност во фазата на проверка на идентитет и верификација на правното лице треба:

- за идентитетот на правното лице кон барањето за издавање на средство за електронска идентификација да се приложат релевантни докази кои го потврдуваат уписот на правното лице во соодветен регистар за уписи на правни лица,

- за доказите кои го потврдуваат уписот на правното лице во соодветен регистар за уписи на правни лица да се претпостави дека се оригинални или според податоците добиени од доверлив извор упатуваат на тоа дека доказот е валиден.

Член 11

При употребата на шемата за електронска идентификација на значително ниво на сигурност, покрај процедурите кои се однесуваат на шемата за електронска идентификација на ниско ниво на сигурност во фазата на проверка на идентитет и верификација на правни лица, треба:

- со сигурност да може да се утврди дека правното лице го поседува доказот кој го потврдува уписот на правното лице во соодветен регистар за уписи на правни лица кој содржи и податоци за името и формата на правното лице, како и податоци за извршената регистрација во оригинал и според доверлив извор да биде потврдено дека правното лице постои и преземените мерки за проверка на идентитетот упатуваат на истото правно лице, земајќи го предвид ризикот од изгубен, украден, суспендиран, одземен или истечен доказ со кој располага доверливиот изворот или

- процедурата за проверка на идентитетот на правното лице кое бара издавање на средство за електронска идентификација да биде веќе спроведена од страна на давател на доверливи услуги за издавање на друго средство, односно напреден електронски печат и таа процедура да има еквивалентна важност според извештаите на телото за оцена на сообразност или

- правното лице веќе да има друго валидно средство, односно напреден електронски печат издаден од страна на регистриран или признаен давател на доверливи услуги.

Член 12

При употребата на шемата за електронска идентификација на високо ниво на сигурност, покрај стандардите кои се однесуваат на шемата за електронска идентификација на значително ниво на сигурност во фазата на проверка на идентитет и верификација на правни лица, треба:

- правното лице да го поседува во оригинал доказот кој го потврдува уписот на правното лице во соодветен регистар за уписи на правни лица кој содржи и податоци за името и формата на правното лице и според доверлив извор е потврдено дека правното лице постои во правниот промет или

- процедурата за проверка на идентитетот на правното лице кое бара издавање на средство за електронска идентификација да биде веќе спроведена од страна на давател на квалификувани доверливи услуги за издавање на друго средство, односно квалификуван електронски печат и таа процедура има еквивалнентна важност според извештаите на телото за оцена на сообразност, за што се преземени и соодветни мерки за да се утврди дека резултатите од другата процедура се сеуште валидни или

- правното лице веќе да има друго валидно средство, односно квалификуван електронски печат издаден од страна на регистриран или признаен давател на квалификувани доверливи услуги, за што се преземени и соодветни мерки за да се утврди дека квалификуваниот електронски печат е сеуште валиден.

Член 13

Средството за електронска идентификација на физичкото лице кое е овластено лице на правно лице се поврзува со средството за електронска идентификација на правното лице, ако:

- може да се прекине врската помеѓу двете средства преку активирање, суспензија, обновување или одземање на едното средство за електронска идентификација независно од другото средство за електронска идентификација, согласно прописите од областа на дејноста што ја врши правното лице, како и прописите што се однесуваат на физичкото лице како овластено лице на правното лице,

- физичкото лице кое е овластено лице на правното лице чие средство за електронска идентификација е поврзано со средството за електронска идентификација на правното лице може да делегира вршење на одредени задачи на друго физичко лице во име на правното лице, при што одговорноста останува на страна на физичкото лице кое е овластено лице на правното лице.

Нивоата на сигурност за поврзување на средството за електронска идентификација на физичкото лице кое е овластено лице на правно лице со средството за електронска идентификација на правното лице може да биде:

- ниско ниво на сигурност,
- значително ниво на сигурност и
- високо ниво на сигурност.

Член 14

Средството за електронска идентификација на физичкото лице кое е овластено лице на правно лице се поврзува со средството за електронска идентификација на правното лице на ниско ниво на сигурност, ако:

- проверката и верификацијата на идентитетот на физичкото лице кое е овластено лице на правно лице е извршена на ниско ниво на сигурност,

- поврзаноста на физичкото лице со правното лице е согласно прописите кои се однесуваат на овластувањата на физичките лица како овластени лица на правни лица и
- физичкото лице ги исполнило условите определени со закон кои се однесуваат на физичките лица како овластени лица на правни лица.

Член 15

Средството за електронска идентификација на физичкото лице кое е овластено лице на правно лице се поврзува со средството за електронска идентификација на правното лице на значително ниво на сигурност, ако:

- физичкото лице ги исполнило условите определени со закон кои се однесуваат на физичките лица како овластени лица на правни лица,
- проверката и верификацијата на идентитетот на физичкото лице кое е овластено лице на правно лице е извршена на значително или високо ниво на сигурност,
- физичкото лице е евидентирано како овластено лице на правното лице врз основа на соодветен доказ, односно врз основа на уписот на правното лице во соодветен регистар за упис на правни лица и
- поврзаноста на физичкото лице со правното лице е верификувана со информации добиени од надлежен орган.

Член 16

Средството за електронска идентификација на физичкото лице кое е овластено лице на правно лице се поврзува со средството за електронска идентификација на правното лице на високо ниво на сигурност, ако:

- физичкото лице ги исполнило условите определени со закон кои се однесуваат на физичките лица како овластени лица на правни лица,
- физичкото лице е евидентирано како овластено лице на правното лице врз основа на соодветен доказ, односно врз основа на уписот на правното лице во соодветен регистар за упис на правни лица,
- проверката и верификацијата на идентитетот на физичкото лице кое е овластено лице на правно лице е извршена на високо ниво на сигурност и
- поврзувањето е потврдено од страна на правното лице со квалификуван електронски печат или со средство за електронска идентификација од високо ниво на сигурност.

Член 17

Стандардите за исполнетост на техничките мерки за сигурност на шемите за електронска идентификација на ниско ниво кои се однесуваат на карактеристиките и дизајнот на средствата за електронска идентификација на ниско ниво се:

- средството за електронска идентификација користи најмалку еден фактор за автентикација.
- средството за електронска идентификација е дизајнирано така што се смета дека издавачот на средството презел разумни мерки за да провери дали се користи само под контрола или владение на лицето на кое му е издадено.

Стандардите за исполнетост на техничките мерки за сигурност на шемите за електронска идентификација на значително ниво кои се однесуваат на карактеристиките и дизајнот на средствата за електронска идентификација на значително ниво се:

- средството за електронска идентификација користи најмалку два фактори на автентикација од различни категории и

- средство за електронска идентификација е дизајнирано така што може да се претпостави дека се користи само ако е под контрола или во владение на лицето на кое му е издадено.

Стандардите за исполнетост на техничките мерки за сигурност на шемите за електронска идентификација на високо ниво кои се однесуваат на карактеристиките и дизајнот на средствата за електронска идентификација на високо ниво се:

- средството за електронска идентификација користи најмалку два фактори на автентикација од различни категории,
- средство за електронска идентификација е дизајнирано така што може да се претпостави дека се користи само ако е под контрола или во владение на лицето на кое му е издадено,
- средството за електронска идентификација е заштитено од умножување и упад во истото, како и од напад со висок потенцијал за нарушување на неговата безбедност и
- средството за електронска идентификација е дизајнирано така што може да биде со сигурност заштитено од страна на лицето на кое му припаѓа против употреба од други страни.

Процедурите за издавање, достава и активирање на средствата за електронска идентификација на ниско ниво опфаќаат издавање на средството за електронска идентификација и доставување на истото преку механизам со кој може да се претпостави дека субјектот кој го побарува тоа средство за електронска идентификација ќе го добие средството.

Процедурите за издавање, достава и активирање на средствата за електронска идентификација на значително ниво опфаќаат издавање на средството за електронска идентификација и доставување на истото преку механизам со кој може да се смета дека му се предава во сопственост на субјектот на средството за електронска идентификација.

Процедурите за издавање, достава и активирање на средствата за електронска идентификација на високо ниво со процесот на активирање на средството за електронска идентификација потврдуваат дека истото му се предава во сопственост на лицето кое е сопственик на средството за електронска идентификација.

Процедурите за суспензија, отповикување и повторно активирање на средствата за електронска идентификација на ниско, на значително и на високо ниво треба да потврдат дека:

- постои можност за навремена и ефикасна суспензија или отповикување на средство за електронска идентификација идентификација,
- постојат утврдени мерки кои ќе бидат преземени за да се спречи неовластена суспензија, отповикување и повторно активирање на средството за електронска идентификација идентификација и
- повторна активација може да се изврши само доколку се исполнети условите кои важеле пред да биде извршена суспензијата или отповикувањето.

Процедурите за обнова и замена на средствата за електронска идентификација на ниско и значително ниво на сигурност, земајќи ги предвид ризиците од промена во податоците за идентификација на лицето, за обновување или замена треба да потврдат дека:

- се исполнети истите стандарди како за првата проверка на идентитет и верификација на лицето или
- процедурата за обнова и замена е спроведена со употреба на валидно средство за електронско идентификација кое е на исто или повисоко ниво на сигурност.

Кога обновата или замената на средствата за електронска идентификација на високо ниво на сигурност се спроведува со употреба на валидно средство за електронска идентификација, процедурите за обнова и замена на средствата треба, покрај стандардите од ставовите 1, 2 и 3 на овој член, да ги потврдат и податоците за идентитетот од доверлив извор.

Член 18

Автентикација на средствата за електронска идентификација на ниско ниво на сигурност треба:

1. пред објавувањето на податоците за идентификација на лицето да е обезбедена верификација на средствата за електронска идентификација и да се потврди нејзината валидност,

2. податоците за идентификација на лицата да се чуваат како дел од механизмот за автентикација, на тој начин што информациите се заштитени од губење или нивно компромитирање, вклучително и нивна обработка надвор од мрежни системи.

3. да се спроведе на тој начин што вклучува безбедносни контроли за верификација на средствата за електронска идентификација, како и мерки за заштита од потенцијално погодување, прислушување, реприза или манипулација при комуникацијата по електронски пат од закани за потенцијален напад на механизмите за автентикација.

Автентикација на средствата за електронска идентификација на значително ниво на сигурност, покрај стандардите од став 1 на овој член треба:

1. пред објавувањето на податоците за идентификација на лицето да е обезбедена верификација на средствата за електронска идентификација преку динамичка автентикација,

2. автентикацијата да се спроведува на тој начин што се имплементирани безбедносни контроли за верификација на средствата за електронска идентификација, како и мерки за заштита од погодување, прислушување, реприза или манипулација при комуникацијата по електронски пат од закани за потенцијален напад на механизмите за автентикација.

Автентикација на средствата за електронска идентификација на високо ниво на сигурност, покрај критериумите од став 2 на овој член треба во самиот механизам за автентикација да содржи безбедносни контроли за верификација на средствата за електронска идентификација, како и мерки за заштита и спречување на погодување, прислушување, реприза или манипулација при комуникацијата по електронски пат од закани за напад на механизмите за автентикација.

Член 19

Издавачот на шеми за електронска идентификација треба да користи опрема, процедури и мерки за администрирање и управување со безбедноста на користената инфраструктура кои ги исполнуваат стандардите за управување со информатичка безбедност, односно стандардите од серијата ISO 27000.

Системот и техничката опрема што се користат за издавање на шеми за електронска идентификација, како и за другите услуги коишто ги нуди издавачот на шеми за електронска идентификација треба да бидат дизајнирани и користени единствено за таа намена.

Физички пристап до капацитетите, информациите и системите на издавачот на шемите за електронска идентификација имаат само овластените лица во правното лице.

Ако е потребен пристап на друго лице до капацитетите, информациите и системите на издавачот на шемите за електронска идентификација, истото треба да биде придружувано и надгледувано од овластеното лице.

Издавачот на шемите за електронска идентификација треба да обезбеди:

1. 24-часовно физичко и електронско набљудување заради спречување на неовластен пристап во просториите кои се користат за функциите на управување со шемите за електронска идентификација;

2. опремата, информациите, медиумите и програмата кои ги користи издавачот на шемите за електронска идентификација да не можат да бидат изнесени од просториите без овластување; и

3. да се води евиденција на секој пристап во просториите и да се врши периодична контрола врз истата.

Физичкото обезбедување на просториите на издавачот на шеми за електронска идентификација треба да има јасен опис кој вклучува:

- безбедносни зони кои се воспоставени и нивните безбедносни карактеристики;
- врските со заштитените средства и
- целосен и ажуриран список на лица вработени кај издавачот на шеми за електронска идентификација кои имаат право на пристап до определните зони, кој е достапен на увид.

Техничката опрема која ја користи издавачот на шемите за електронска идентификација треба да биде заштитена од неовластен пристап.

Капацитетите на издавачот на шемите за електронска идентификација 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.

Издавачот на шеми за електронска идентификација треба да овозможи управување со системот на безбеден начин.

Лицата вработени кај издавачот на шеми за електронска идентификација треба да ја одржуваат и подобруваат доверливоста на услугите.

Системите со кои располага издавачот на шеми за електронска идентификација треба да имаат контрола на пристап и да се употребуваат само од страна на овластени лица.

Системите треба да го идентификуваат секој корисник и успешно да ја потврдат веродостојноста на истиот, пред да овозможат какво било дејствие 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.

Одредбите од ставовите од 1 до 14 на овој член, што се однесуваат на безбедност на системи, се применуваат и на оперативен систем или на ниво на поединечни компененти на системот.

Член 20

Издавачите на шеми за електронска идентификација треба да ги исполнат следните стандарди:

- да донесат внатрешни правила за видовите информации што може да се бараат, процедурата за докажување за идентитет на субјекти кои бараат издавање или употребуваат средство за електронска идентификација и информации за тоа какви податоци може да се задржат и период на нивно чување,
- да објават основни карактеристики за шемата, која ги вклучува сите применливи услови, ограничувања од употреба и надоместоци за нејзино обезбедување, вклучително и политика за приватност,
- заради чување на евиденциите и на релевантните информации, да воспостават ефикасен систем за управување со евиденцијата, земајќи ги предвид важечките стандарди и добрите практики во врска со заштитата на податоците и нивното задржување,
- да воспостават процедури со кои се обезбедува обука, квалификации, искуство и вештини потребни за извршување на задачите што ги извршуваат лицата ангажирани од страна на издавачите на шеми за електронска идентификација и кај нивните подизведувачи,

- да обезбедат лица – вработени/ангажирани за вршење на својата дејност и за обезбедување на услугата според утврдените процедури за нејзино обезбедување и
- да преземат мерки за заштита на средствата и објектите што ги користи од оштетувања предизвикани од еколошки настани, неовластен пристап и други фактори кои можат да влијаат на безбедноста на услугата.

Издавачите на шеми за електронска идентификација што обезбедуваат и друг вид на доверливи услуги определени со закон, треба да имаат внатрешна организација која треба да биде целосно оперативна во сите сектори што се однесуваат на давање на доверливи услуги.

Средствата и објектите што ги користи издавачот на шеми за електронска идентификација треба да гарантираат дека пристапот до средствата на кои се чуваат или обработуваат лични, криптографски или други чувствителни податоци и информации се заштитени од неовластен пристап.

Член 21

Издавачот на шема за електронска идентификација на ниско ниво на сигурност треба:

- да преземе мерки за да обезбеди спроведување на сразмерни технички контроли на управување со ризиците кои може да влијаат на безбедноста на услугите што ги обезбедуваат, заштита на доверливоста, интегритетот и достапноста на обработените информации,
- да ги заштити електронските канали за комуникација што ги користи при размена на лични или чувствителни информации заради нивна заштита од прислушување, манипулација и репродукција,
- јасно да го ограничи пристапот до чувствителен криптографски материјал, доколку се користи за издавање на средства за електронски идентификација и автентикација и да го заштити од неовластен пристап, како и да преземе мерки со кои ќе се осигура дека таквиот материјал не е зачуван во форма на обичен текст,
- да имплементира процедури со кои ќе се осигура одржувањето на безбедноста на долг временски период и ќе обезбеди можност да се одговори на промените во нивото на ризик, инциденти и нарушувања на безбедноста на информасиските системи и средства кои ги употребува и
- за сите медиуми што содржат лични, криптографски или други чувствителни информации да обезбеди чување, транспортирање и отстранување на сигурен и безбеден начин.

Издавачот на шема за електронска идентификација на значително ниво и на високо ниво на сигурност, покрај мерките од став 1 на овој член, треба да преземе мерки чувствителниот криптографски материјал, доколку се користи за издавање на средства за електронски идентификација и автентикацијата да го заштити од потенцијални нарушувања.

Член 22

Издавачот на шема за електронска идентификација на ниско ниво на сигурност треба да обезбеди спроведување на периодични внатрешни контроли кои ќе вклучат и контрола на сите делови што се релевантни за обезбедување на доверливите услуги, со цел да се обезбеди оценка за усогласеност со релевантните стандарди.

Издавачот на шема за електронска идентификација на значително ниво на сигурност треба да обезбеди спроведување на периодични внатрешни и надворешни контроли кои ќе вклучат и контрола на сите делови што се релевантни за обезбедување на доверливите услуги, со цел да се обезбеди оценка за усогласеност со релевантните стандарди.

Издавачот на шема за електронска идентификација на високо ниво на сигурност треба да обезбеди спроведување на периодични надворешни контроли кои ќе вклучат и контрола на сите делови што се релевантни за обезбедување на доверливите услуги, со цел да се обезбеди оценка за усогласеност со релевантнните стандарди.

За да се обезбеди оценка за усогласеност со релевантните стандарди над шемите за електронска идентификација кои се издаваат за остварување на надлежностите на органите на државната управа на секои три години се врши надворешна контрола.

Член 23

Заштита на приватноста и доверливоста на разменетите податоци и одржување на интегритетот на податоците помеѓу јазлите се обезбедува со употреба на најдобри достапни технички решенија и практики за заштита.

Јазлите не содржат лични податоци, освен за целта утврдена во член 26 став 3 од овој правилник.

Член 24

Комуникацијата помеѓу јазлите треба да обезбеди интегритет на податоците и автентичност со цел да обезбеди сигурност дека сите барања и одговори се автентични и не се менувани.

Јазлите користат технички и технолошки решенија што биле успешно спроведени за оперативна употреба.

Член 25

Јазлите треба да користат синтаксични формати на вообичаени пораки засновани врз стандарди кои се повеќе од еднаш користени за комуникација и за кои е утврдено дека функционираат во оперативно опкружување.

Синтаксата треба да дозволува:

(а) соодветна обработка на минималниот сет на податоци за идентификација на лица кои на единствен начин претставуваат конкретно физичко или правно лице;

(б) соодветна обработка за нивото на сигурност на средствата за електронска идентификација;

(в) разлика помеѓу телата на јавниот и приватниот сектор;

(г) флексибилност за задоволување на потребите за дополнителни атрибути поврзани со идентификација.

Член 26

Операторот на јазли ги соопштува метаподатоците за управување со јазлите на стандардизиран машински обработлив начин, кој е сигурен и доверлив.

Параметрите кои се релевантни за безбедноста, се преземаат автоматски.

Операторот на јазли чува податоци кои, во случај на инцидент, овозможуваат реконструкција на секвенцата на размена на пораки за утврдување на местото и природата на инцидентот.

Податоците се чуваат за временски период од пет години и се состојат од следниве елементи:

(а) идентификација на јазол;

(б) идентификација на порака;

(в) датум и време на пораката.

Член 27

Операторите на јазли за јазлите кои обезбедуваат автентикација треба да докажат дека, во однос на јазлите кои учествуваат во рамката за интероперабилност, јазолот за автентикација го исполнува стандардот ISO / IEC 27001, преку сертификација или со еквивалентни методи на проценка.

Операторите за јазли обезбедуваат критични ажурирања за безбедноста без непотребно одложување.

Член 28

Минималниот сет на податоци за лична идентификација, кој на единствен начин претставува конкретно физичко лице, треба да содржи:

1. Задолжителни атрибути, кумулативно:

(а) сегашно презиме (и);

(б) тековно име (и);

(в) датум на раѓање;

(г) единствен идентификатор создаден од испраќачот во согласност со техничките спецификации за целите на прекуграничната идентификација и што е непроменлив со текот на времето.

2. Еден или повеќе од следниве дополнителни атрибути:

(а) име (и) и презиме (и) при раѓање;

(б) место на раѓање;

(в) тековна адреса;

(г) пол.

Минималниот сет на податоци за лична идентификација, кој на единствен начин претставува конкретно правно лице, треба да содржат комбинација на атрибути, и тоа:

1. Задолжителни атрибути, кумулативно:

(а) тековно име на правното лице;

(б) единствен идентификатор изработен од испраќачот во согласност со техничките спецификации за целите на прекуграничната идентификација и што е непроменлив со текот на времето.

2. Еден или повеќе од следниве дополнителни атрибути:

(а) тековна адреса;

(б) единствен даночен број;

(в) единствен матичен број на субјектот;

Податоците се пренесуваат врз основа на оригинални знаци и доколку е соодветно, се преведуваат на латински ознаки.

Член 29

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

Бр. 08/1-1205/2
26 февруари 2020 година
Скопје

Министер за информатичко
општество и администрација,
Дамјан Манчевски, с.р.