На основу члана 18. став 2. Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС”, број 94/17) и члана 42. став 1. Закона о Влади („Службени гласник РС”, бр. 55/05, 71/05 – исправка, 101/07, 65/08, 16/11, 68/12 – УС, 72/12, 7/14 – УС, 44/14 и 30/18 – др. закон),

Влада доноси

УРЕДБУ

о ближем уређењу услова које морају да испуне шеме електронске идентификације за одређене нивое поузданости

Предмет уредбе

Члан 1.

Овом уредбом ближе се уређују услови које морају да испуне шеме електронске идентификације за одређене нивое поузданости.

Сви појмови који се користе у овој уредби у мушком роду, обухватају исте појмове у женском роду.

Електронска идентификација

Члан 2.

Електронска идентификација је поступак коришћења личних идентификационих података у електронском облику који једнозначно одређују правно лице, физичко лице или физичко лице у својству регистрованог субјекта.

Када регистрована шема електронске идентификације испуњава услове за виши ниво поузданости шеме електронске идентификације, у том случају се сматра да испуњава и услове за ниже нивое поузданости.

Захтев за издавање средства електронске идентификације

Члан 3.

Захтев за издавање средства електронске идентификације подноси се пружаоцу услуге електронске идентификације.

Приликом подношења захтева за издавање средства електронске идентификације, пружалац услуге електронске идентификације је у обавези да подносиоца захтева упозна са:

1) начином употребе средства електронске идентификације;

2) прописима и правилима који се односе на коришћење услуге електронске идентификације;

3) информацијама о нивоу поузданости шеме електронске идентификације за коју се подноси захтев;

4) ризицима од евентуалне злоупотребе односно неистинитог представљања;

5) мерама које подносилац захтева треба да предузме ради безбедног коришћења средства електронске идентификације.

Пружалац електронске идентификације дужан је да прибави сагласност корисника за обраду података о личности у оквиру пружања услуге електронске идентификације и у свему поступа сагласно закону којим се уређује заштита података о личности.

Провера идентитета за издавање средства електронске идентификације основног нивоа поузданости

Члан 4.

За издавање средства електронске идентификације основног нивоа поузданости провера идентитета врши се на основу једног од следећих начина:

1) личне карте или друге јавне исправе са фотографијом;

2) јавне исправе која служи као средство идентификације на даљину;

3) средства идентификације које је издато у оквиру регистроване шеме истог или вишег нивоа поузданости.

У случају када захтев за издавање средства електронске идентификације основног нивоа поузданости подноси правно лице, врши се провера идентитета овлашћеног представника правног лица уз достављање доказа о овлашћењу.

Доказ из става 1. тачка 1) и става 2. овог члана подносилац захтева доставља електронским путем пружаоцу услуге.

Издавање средства електронске идентификације основног нивоа поузданости може се вршити уз физичко присуство подносиоца захтева, уколико је то предвиђено интерним актима пружаоца услуге електронске идентификације.

Провера идентитета за издавање средства електронске идентификације средњег нивоа поузданости

Члан 5.

За издавање средства електронске идентификације средњег нивоа поузданости провера идентитета врши се на основу једног од следећих начина:

1) личне карте или путне исправе уз физичко присуство подносиоца захтева;

2) јавне исправе која служи као средство идентификације на даљину;

3) средства идентификације које је издато у оквиру регистроване шеме истог или вишег нивоа поузданости.

У случају када захтев за издавање средства електронске идентификације средњег нивоа поузданости подноси правно лице, врши се провера идентитета овлашћеног

представника правног лица, сходном применом става 1. овог члана, уз достављање доказа о овлашћењу.

Уколико се провера идентитета подносиоца врши на основу документа из става 1. тачка 1) овог члана пружалац електронске идентификације може да изврши проверу валидности документа и тачност података из документа код органа надлежног за издавање документа у складу са законом којим се регулишу евиденције и обрада података у области унутрашњих послова.

Орган надлежан за издавање документа из става 1. тачка 1) овог члана обезбедиће проверу валидности документа и тачности података из документа за потребе пружаоца електронске идентификације путем електронског сервиса, уз примену одговарајућих мера информационе безбедности.

Провера идентитета за издавање средства електронске идентификације високог нивоа поузданости

Члан 6.

За издавање средства електронске идентификације високог нивоа поузданости провера идентитета врши се на основу једног од следећих начина:

1) личне карте или путне исправе уз физичко присуство подносиоца захтева;

2) јавне исправе која служи као средство идентификације на даљину, у складу са законом;

3) средства идентификације које је издато у оквиру регистроване шеме високог нивоа поузданости.

У случају када захтев за издавање средства електронске идентификације високог нивоа поузданости подноси правно лице, врши се провера идентитета овлашћеног представника правног лица, сходном применом става 1. овог члана, уз достављање доказа о овлашћењу.

Уколико се провера идентитета подносиоца врши на основу документа из става 1. тачка 1) овог члана, пружалац електронске идентификације може да изврши проверу валидности документа и тачност података из документа код органа надлежног за издавање документа у складу са законом којим се регулишу евиденције и обрада података у области унутрашњих послова.

Орган надлежан за издавање документа из става 1. тачка 1) овог члана обезбедиће проверу валидности документа и тачности података из документа за потребе пружаоца електронске идентификације путем електронског сервиса, уз примену одговарајућих мера информационе безбедности.

Провера идентитета страног држављанина

Члан 7.

Провера идентитета страног држављанина врши се на основу стране путне исправе, путне исправе за странце или личне карте за странце које издају надлежни органи Републике Србије.

Пружалац електронске идентификације може да изврши проверу валидности путне исправе за странце или личне карте за странце и тачност података из тих докумената код органа надлежног за издавање документа, у складу са законом којим се регулишу евиденције и обрада података у области унутрашњих послова.

Орган надлежан за издавање документа из става 2. овог члана обезбедиће проверу валидности тих докумената и тачности података из докумената за потребе пружаоца електронске идентификације путем електронског сервиса, уз примену одговарајућих мера информационе безбедности.

Издавање и активација средства електронске идентификације

Члан 8.

У поступку издавања средство електронске идентификације испоручује се на начин који осигурава испоруку само лицу којем је намењено, односно кориснику средства.

Након испоруке, средство електронске идентификације средњег и високог нивоа поузданости се активира путем активационог кода који је достављен подносиоцу захтева.

Суспензија, опозив и поновна активација средства електронске идентификације

Члан 9.

Средство електронске идентификације може се суспендовати, односно опозвати.

Пружалац услуге електронске идентификације дужан је да предузме мере у циљу спречавања неовлашћене суспензије, опозива или поновне активације.

Средство електронске идентификације може се поново издати ако су испуњени услови за поуздано издавање.

У случају обнове или замене средства електронске идентификације, потребно је извршити поновно доказивање и проверу идентитета на начин предвиђен чл. 4–7. ове уредбе.

Аутентикациони механизам за шему електронске идентификације основног нивоа поузданости

Члан 10.

Пружалац услуга електронске идентификације основног нивоа поузданости у обавези је да:

1) издаје средство електронске идентификације које садржи најмање један елемент аутентикације;

2) предузме мере које обезбеђују употребу средства електронске идентификације само кориснику средстава;

3) обезбеди поуздану проверу средства електронске идентификације и њихове ваљаности приликом откривања личних идентификационих података корисника средстава;

4) обезбеди заштитне контроле за проверу средства електронске идентификације приликом процеса аутентикације, у циљу онемогућавања угрожавања механизма аутентикације, као што је откривање фактора аутентикације, неовлашћени приступ, неовлашћено пресретање и други начини угрожавања.

Аутентикациони механизам за шему електронске идентификације средњег нивоа поузданости

Члан 11.

Пружалац услуга електронске идентификације средњег нивоа поузданости у обавези је да:

1) издаје средство електронске идентификације које садржи најмање два елемента аутентикације различитих категорија (нешто што лице зна, нешто што лице поседује, нешто што лице јесте);

2) средство из тачке 1. овог става је пројектовано тако да обезбеђује могућност коришћења средства електронске идентификације само кориснику средстава, односно да се може претпоставити да се средство електронске идентификације употребљава само под контролом корисника средства;

3) обезбеди поуздану проверу средства електронске идентификације и њихове ваљаности приликом откривања личних идентификационих података путем динамичке аутентикације;

4) обезбеди заштитне контроле за проверу средства електронске идентификације приликом процеса аутентикације, у циљу онемогућавања угрожавања механизма аутентикације, као што је откривање фактора аутентикације, неовлашћени приступ, неовлашћено пресретање и други начини угрожавања.

Динамичка аутентикација представља електронски процес у коме се употребљава криптографија или друге технике, како би се створио електронски доказ да корисник контролише или поседује податке за идентификацију, а који се мења са сваком аутентикацијом.

Аутентикациони механизам за шему електронске идентификације високог нивоа поузданости

Члан 12.

Пружалац услуга електронске идентификације високог нивоа поузданости у обавези је да:

1) предузме мере које обезбеђују употребу средства електронске идентификације само кориснику средства, односно да се може претпоставити да се средство електронске идентификације употребљава само под контролом корисника средстава;

2) обезбеди поуздану проверу средства електронске идентификације и њихове ваљаности путем динамичке аутентикације из члана 11. став 2. ове уредбе пре откривања личних идентификационих података корисника средства;

3) обезбеди заштитне контроле за проверу средства електронске идентификације приликом процеса аутентикације, у циљу онемогућавања угрожавања механизма аутентикације, као што је откривање фактора аутентикације, неовлашћени приступ, неовлашћено пресретање и други начини угрожавања;

4) обезбеди висок ново заштите средства за електронску идентификацију од копирања, неовлашћене измене и злоупотребе од стране других лица;

5) издаје квалификовано средство за креирање електронског потписа односно печата које уједно представља средство идентификације;

6) врши аутентикацију корисника на основу квалификованог електронског потписа односно квалификованог електронског печата корисника који се тиме идентификује, засновано на сертификатима корисника које је сам издао.

Технички, организациони и безбедносни услови за пружаоце услуге електронске идентификације

Члан 13.

Пружалац услуге електронске идентификације је правно или физичко лице у својству регистрованог субјекта који пружа услуге електронске идентификације.

Пружалац услуге електронске идентификације дужан је да:

1) усвоји и примењује Опште услове за пружање услуге, Политику пружања услуга и Практична правила за пружање услуга, у складу са прописима, као и домаћим и међународним стандардима у области електронске идентификације;

2) упозна корисника средства са условима коришћења услуге, укључујући сва ограничења њене употребе, као и са евентуалним накнадама за коришћење услуге;

3) усвоји политику заштите приватности, у складу са прописима Републике Србије;

4) успостави одговарајуће политике и поступке које осигуравају кориснику средства правовремено и поуздано информисање о променама услова коришћења услуге, односно политике заштите приватности за одређену услугу;

5) чува податке о издавању средства електронске идентификације, укључујући податке везане за проверу идентитета корисника, најмање десет година по издавању;

6) води евиденцију и чува информације о значајним догађајима везаним за оперативни рад пружаоца и безбедносне претпоставке регистроване шеме електронске идентификације;

7) води евиденцију о коришћењу средства електронске идентификације и чува податке из евиденције уколико је то неопходно за потребе ревизије, истраге у случају кршења безбедности информација и за потребе задржавања података, у складу са законом;

8) обезбеди извор тачног времена који је синхронизован са извором референтног времена који одреди министарство надлежно за послове информационог друштва и поуздано уграђује информацију о тачном времену у евиденције из тач. 5), 6) и 7) овог члана;

9) обезбеди да су његови запослени и подизвођачи обучени и квалификовани за послове који се односе на услугу електронске идентификације;

10) обезбеди адекватан број запослених и подизвођача за примерено обављање услуге;

11) обезбеди непосредан надзор и заштиту објеката који се употребљавају за пружање услуга, од штете узроковане временским условима, неовлашћеним приступом и другим узроцима који могу утицати на безбедност услуге;

12) обезбеди да у објектима који се користе за пружање услуге приступ подручјима у којима се налазе или се обрађују лични, криптографски или други поверљиви подаци могу имати само овлашћена запослена лица или подизвођачи;

13) дужан је да има план завршетка рада у случају престанка пружања услуге електронске идентификације, којим се обезбеђује обавештавање корисника о престанку пружања услуга и адекватно чувања података;

14) обезбеди да, у циљу усклађености услуге са релевантном политиком, врши периодичне ревизије којима су обухваћени сви делови који се односе на испоруку услуга, и то:

(1) периодичне интерне ревизије код пружања услуге електронске идентификације основног нивоа поузданости;

(2) периодичне независне интерне или екстерне ревизије код пружања услуге електронске идентификације средњег нивоа поузданости;

(3) периодичне независне екстерне ревизије код пружања услуге електронске идентификације високог нивоа поузданости.

Техничке и безбедносне карактеристике средства електронске идентификације

Члан 14.

Пружалац услуге електронске идентификације дужан је да успостави ефикасан систем управљања безбедношћу информација у циљу управљања ризицима који се односи на безбедност информација.

Пружалац услуге електронске идентификације средњег и високог нивоа поузданости дужан је да успостави систем из става 1. овог члана у складу са стандардима и начелима за управљање ризицима који се односе на безбедност информација.

Пружалац услуге електронске идентификације дужан је да:

1) успостави одговарајуће техничке контроле за управљање ризицима за безбедност услуга којима се штити поверљивост, целовитост и доступност информација које се обрађују;

2) обезбеди да су електронски комуникациони канали који се употребљавају за размену личних или поверљивих информација заштићени од неовлашћеног приступа, неовлашћеног пресретања, неовлашћеног коришћења и других начина угрожавања;

3) ограничи приступ криптографском материјалу, ако се употребљава за издавање средства електронске идентификације и аутентикацију на овлашћена лица и апликације за које се тај приступ изричито захтева, као и да обезбеди да се такав материјал никад континуирано не чува у формату обичног некриптованог текста;

4) осигура континуирану безбедност информација, као и да обезбеди да је систем отпоран на промене нивоа ризика, инциденте и кршење безбедности;

5) да обезбеди да се медији који садрже личне, криптографске или друге поверљиве информације складиште, преносе и уништавају на сигуран начин.

Поред услова из става 3. овог члана, пружаоци услуге електронске идентификације средњег и високог нивоа поузданости дужни су да поверљиви криптографски материјал, уколико се употребљава за издавање средства електронске идентификације и аутентикације, заштите од неовлашћене измене.

Интероперабилност шема електронске идентификације

Члан 15.

У циљу обезбеђивања интероперабилности шема електронске идентификације пружаоци услуге електронске идентификације морају да испуне техничке и организационе услове из чл. 13. и 14. ове уредбе.

Пружаоци услуге електронске идентификације дужни су да: поуздајућим странама омогуће проверу идентитета путем „OAuth” протокола у складу са стандардом RFC 6749 „The OAuth 2.0 Authorization Framework” или путем „SAML” протокола у складу са стандардом „OASIS Security Assertion Markup Language (SAML) v2.0”, што не искључује могућност понуде додатних начина провере идентитета.

Завршна одредба

Члан 16.

Ова уредба ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Србије”.

05 број 110-3780/2018-1

У Београду, 2. августа 2018. године

Влада

Председник,

Ана Брнабић, с.р.