**Р Е П У Б Л И К А  Б Ъ Л Г А Р И Я**
**М И Н И С Т Е Р С К И  С Ъ В Е Т**

**Проект!**

**П О С Т А Н О В Л Е Н И Е №**

**от ……. 2016 г.**

**ЗА ПРИЕМАНЕ НА ПРАВИЛНИК ЗА ПРИЛАГАНЕ НА ЗАКОНА ЗА ЕЛЕКТРОННАТА ИДЕНТИФИКАЦИЯ**

**М И Н И С Т Е Р С К И Я Т  С Ъ В Е Т**
**П О С Т А Н О В И:**

Член единствен. Приема Правилник за прилагане на Закона за електронната идентификация.

МИНИСТЪР-ПРЕДСЕДАТЕЛ:

(БОЙКО БОРИСОВ)

И.Д. ГЛАВЕН СЕКРЕТАР НА
МИНИСТЕРСКИЯ СЪВЕТ:

(ВЕСЕЛИН ДАКОВ)

# Правилник за прилагане на Закона за електронната идентификация

## Глава първа.
## ОБЩИ ПОЛОЖЕНИЯ

**Обхват**

**Чл. 1.** (1) Този правилник урежда прилагането на Закона за електронната идентификация (ЗЕИ).

(2) Правилникът урежда:

1. алгоритмите и методите за създаване на електронни идентификатори;

2. алгоритмите и методите за създаване на секторни електронни идентификатори;

3. реда и условията за регистрация на администратори на електронна идентичност и изискванията към дейността им;

4. реда и условията за регистрация на центрове за електронна идентификация и изискванията към дейността им;

5. реда за воденето, съхранението и достъпа на регистрите по чл. 19 от Закона за електронната идентификация;

6. реда за проверка на удостоверения за електронна идентичност по чл. 25 от ЗЕИ;

7. изискванията към стандартите и реквизитите на удостоверението за електронна идентичност по чл. 3 от ЗЕИ;

8. изискванията към носителите на удостоверения за електронна идентичност по чл. 13, ал. 7 и чл. 20, ал. 6 от ЗЕИ, както и правилата за издаването и управлението им;

9. протоколите, техническите изисквания и начините за проверка на електронна идентичност по чл. 24 от ЗЕИ;

10. протоколите и техническите изисквания по чл. 28 от ЗЕИ;

11. обхвата на съхраняваните данни по чл. 27 от ЗЕИ;

12. изискваните за регистрация по чл. 11 от ЗЕИ;

13. изискванията по отношение на техническото оборудване и технологиите по чл. 13, ал. 6 от ЗЕИ;

14. изискванията и процедурите за сигурност по чл. 13, ал. 3 и чл. 14, ал. 2 от ЗЕИ;

15. изискванията към информационните системи, подлежащи на контрол по чл. 38 от ЗЕИ;

16. реквизитите на заявлението по чл. 15, ал. 1;

17. реда за воденето, съхранението и достъпа на регистъра на администраторите и центровете, по чл. 10 от ЗЕИ;

18. реда на водене и редът на достъп до регистъра на овластяванията, съответно по чл. 29, ал. 4 и чл. 32 от ЗЕИ.

**Трансгранична електронна идентификация**

**Чл. 2.** Редът за достъп до националните схеми за електронна идентификация, установени в страните-членки на Европейския съюз, както и редът за предоставяне на

трансгранична електронна идентификация, се определят с инструкция на председателя на Държавна агенция "Електронно управление", съгласувана с министъра на вътрешните работи.

## Глава втора.
## РЕГИСТРИ ЗА ЕЛЕКТРОННА ИДЕНТИЧНОСТ

### Раздел I.
### Регистър на електронните идентификатори

**Обхват и вписвания**

**Чл. 3.** (1) В регистъра на електронните идентификатори се вписва всеки създаден електронен идентификатор и уникалния граждански идентификатор, на който той съответства.

(2) Вписванията в регистъра по ал. 1 се извършват в процеса на издаване на удостоверение за електронна идентичност по реда на чл. 14.

(3) Преди вписване в регистъра по ал. 1 на нов електронен идентификатор се извършва проверка дали същият вече не съществува. Ако съществува, се генерира друг електронен идентификатор.

(4) Регистърът по ал. 1 се съхранява безсрочно.

**Достъп до регистъра**

**Чл. 4.** (1) Регистърът по чл. 3, ал. 1 не е публичен и се защитава от проникванията с инструменти за сигурност, в съответствие с изискванията за информационна сигурност по Закона за електронното управление.

(2) Достъп до регистъра по чл. 3, ал. 1 имат само регистрираните центрове за електронна идентификация.

(3) Достъп до регистъра по чл. 3, ал. 1 имат и лица, определени със заповед на министъра на вътрешните работи, които се идентифицират по електроннен път преди всяко осъществяване на достъп.

(4) Всички операции, извършени в регистъра по чл. 3, ал. 1, се съхраняват в журнал на събитията.

### Раздел II.
### Регистър на удостоверенията за електронна идентичност

**Обхват и вписвания**

**Чл. 5.** (1) Регистърът на удостоверенията за електронна идентичност съдържа всички издадени удостоверения за електронна идентичност, както и списък на спрените и прекратените такива.

(2) Вписването на удостоверение в регистъра по ал. 1 се извършва в процеса на издаването му по реда на чл. 14.

(3) Вписванията и заличаванията в списъка на прекратените удостоверения се извършват от длъжностно лице, определено със заповед на министъра на вътрешните работи или автоматизирано, при заявление от страна на титуляря.

(4) Списъците на прекратените удостоверения трябва да се актуализират автоматично през не повече от 3 часа.

(5) Всички операции, извършени в регистъра по ал. 1, се съхраняват в журнал на събитията.

(6) Регистърът по ал. 1 се съхранява безсрочно.

**Достъп до регистъра**

**Чл. 6.** (1) Регистърът по чл. 5, ал. 1 е публичен. Достъпът до удостоверенията, вписани в него, е свободен и безплатен.

(2) Достъпът до регистъра по чл. 5, ал. 1 се осъществява съгласно стандарта X.500 и протоколите LDAP (Lightweight Directory Access Protocol) и HTTPS.

(3) Проверките за валидност на удостоверения за електронна идентичност, включително от центровете за електронна идентификация, се извършват чрез протокола OCSP или чрез извличане на списък с прекратени и спрени удостоверения във формат CRL.

## Глава трета.
## ЕЛЕКТРОННИ ИДЕНТИФИКАТОРИ

### Раздел I.
### Електронен идентификатор

**Създаване**

**Чл. 7.** Електронният идентификатор се създава от органа за електронна идентификация по чл. 7 от Закона за електронната идентификация автоматично, в процеса на издаване на удостоверение за електронна идентичност по реда на чл. 14.

**Формат**

**Чл. 8.** Електронният идентификатор е универсално уникален идентификатор (UUID) според RFC 4122 (A Universally Unique IDentifier (UUID) URN Namespace) на Работната група за интернет инженеринг (Internet Engineering Task Force, IETF).

### Раздел II.
### Секторни електронни идентификатори

**Обхват**

**Чл. 9.** (1) Физическите лица могат да се идентифицират пред държавен орган или група държавни органи чрез секторни електронни идентификатори в секторите на държавното управление, определени по реда на чл. 4, ал. 5 от Закона за електронната идентификация.

(2) Физическите лица могат да се идентифицират чрез секторни електронни идентификатори, установени от частноправни субекти за идентификация в отношенията помежду им.

(3) За целите на електронната идентификация информационните системи на всеки частноправен субект се считат за отделен сектор.

(4) Секторен електронен идентификатор е електронен идентификатор, преобразуван от център за електронна идентификация, чрез прилагането на определени алгоритми.

**Създаване и използване**

**Чл. 10.** (1) Центровете за електронна идентификация предоставят идентификатор на всеки сектор.

(2) За идентификатор на сектор може да бъде използван и уникалния ресурсен локатор (URL) на интернет страницата, инициираща електронната идентификация.

(3) Секторният идентификатор на физическите лица се генерира при всяка заявка към център за електронна идентификация. Генерирането се извършва на основата на електронния идентификатор, идентификатора на сектора и други данни, чрез еднопосочна криптографска функция.

(4) Методът за преобразуване по ал. 3 не трябва да позволява секторен идентификатор да бъде преобразуван в електронен идентификатор, от който е преобразуван, включително чрез изпробване на предполагаеми електронни идентификатори с еднопосочната функция.

(5) Председателят на Държавна агенция “Електронно управление” определя реда за генерирането на идентификатора по ал. 3 с инструкцията по чл. 2.

## Глава четвърта.
## ИЗДАВАНЕ И УПРАВЛЕНИЕ НА УДОСТОВЕРЕНИЕ ЗА ЕЛЕКТРОННА ИДЕНТИЧНОСТ

### Раздел I.
### Стандарти и реквизити на удостоверението за електронна идентичност

**Формат**

**Чл. 11.** (1) Удостоверението за електронна идентичност се издава съгласно стандарт X.509.

(2) Удостоверението съдържа публичния ключ, съответстващ на частния ключ, записан в защитената зона на носителя на електронна идентичност.

(3) Удостоверението се представя във формат, описан в общопризнати в практиката международни спецификации, използващ стандартен абстрактен език - ASN.1 (Abstract Syntax Notation One) за неговото описание и стандартно двоично кодиране.

(4) Удостоверението се подписва с електронен печат на Министерството на вътрешните работи, създаден само за нуждите на издаването на удостоверения за електронна идентичност.

(5) Удостоверението се вписва в регистъра по чл. 5, ал. 1.

**Съдържание**

**Чл. 12.** Удостоверението за електронна идентичност съдържа най-малко следните данни:

1. уникален сериен номер;
2. период на валидност;
3. електронния идентификатор на лицето.

### Раздел II.
### Издаване на удостоверение за електронна идентичност

**Заявления**

**Чл. 13.** (1) Издаването на удостоверение за електронна идентичност започва по писмено заявление, подадено по реда на чл. 20 от Закона за електронната идентификация.

(2) Заявлението съдържа единния граждански номер, съответно - личния номер на чужденец на на физическото лице - титуляр на електронната идентичност.

(3) Заявлението се приема от:

1. определено от министъра на вътрешните работи длъжностно лице в местата за явяване по чл. 20, ал. 2 от Закона за електронната идентификация;

2. администратор на електронна идентичност;

3. определено от ръководителя на дипломатическо или консулско представителство на Република България длъжностно лице.

(4) Заявлението може да се приема и по електронен път.

(5) Искане за продължаване срока на издадено удостоверение за електронна идентичност, ако е направено преди изтичането на срока на удостоверението, може да се подаде по електронен път, без да са спазени изискванията за първоначално издаване.

**Издаване на удостоверение за електронна идентичност**

**Чл. 14.** (1) Издаването на удостоверението се извършва при последователното спазване на следните действия:

1. Лицето по чл. 13, ал. 3, приело заявлението, го изпраща за генериране на електронен идентификатор до органа за електронна идентификация.

2. Органът за електронна идентификация проверява автентичността на лицето изпращач по т. 1 чрез удостоверението по ал. 37, ал. 4 по ред, определен с инструкцията по чл. 2.

3. Органът за електронна идентификация проверява данните от заявлението, генерира електронен идентификатор на заявителя, проверява уникалността на идентификатора и вписва съотствествието между уникалния граждански идентификатор и създадения електронен идентификатор в регистъра по чл. 3, ал. 1;

4. Органът за електронна идентификация изпраща генерирания електронен идентификатор на лицето по чл. 13, ал. 3.

5. Лицето по чл. 13, ал. 3 генерира двойка криптографски ключове на електронен носител на информация и създава искане за подписване на удостоверение за публичния ключ, съдържащо електронния идентификатор на титуляря. Искането е електронен документ, който отговаря на изискванията на PKCS #10.

6. Лицето по чл. 13, ал. 3 изпраща искането за подписване на удостоверение на органа за електронна идентификация;

7. Органът за електронна идентификация подписва удостоверението, подадено чрез искането от т. 5, вписва го в регистъра по чл. 5, ал. 1, вписва серийния му номер в регистъра по чл. 3, ал. 1, и го изпраща на лицето по чл. 13, ал. 3 , заедно с необходимата удостоверителна верига.

8. Подписаното удостоверение и удостоверителната верига се записват на електронния носител.

9. Лицето по чл. 13, ал. 3 изпраща до органа за електронна идентификация потвърждение за записването по т. 8.

10. Електронният носител с удостоверението за електронна идентичност или средство за достъп до него се предава на титуляря.

(2) Ако някое от действията по ал. 1 не приключи успешно, процесът се прекратява, а данните за него се изтриват от базите данни, с изключение на журналите на събитията по чл. 4, ал. 4 и чл. 5, ал. 5. Лицето, инициирало процеса, бива уведомено за възникналите проблеми.

(3) Адресите и протоколите за комуникация се определят със заповед на министъра на вътрешните работи.

(4) Действията по ал. 1, т. 2-9 са автоматизирани.

(5) Удостоверение се издава само ако заявителят се е явил лично пред лице по чл. 13, ал. 3.

(6) Ако заявлението е подадено по електронен път, издаването на удостоверението се спира временно, до личното явяване на титуляря пред лице по чл. 13, ал. 3.

(7) В случай, че персонализирането на удостоверението за електронна идентичност на електронен носител не се извършва в момента на заявяване, личното явяване на лицето може да се осъществи и при получаване на електронния носител, на който е записано удостоверението.

(8) За лично явяване се счита и използване на други методи за идентификация, по чл. 24, ал. 1, б. “г” от Регламент (ЕС) 910/2014.

## Раздел III.
## Носители на електронна идентичност

**Изисквания**

**Чл. 15.** (1) Персонализирането на удостоверенията за електронна идентичност се извършва върху устройства, които отговарят на изискванията по чл. 29 от Регламент (ЕС) 910/2014.

(2) Електронният носител трябва да поддържа стандартни криптографски операции - подписване и криптиране, както и необходимост от потвърждение на операциите с ПИН код или друго средство.

(3) В случай на възможност за безконтактен достъп, електронният носител трябва да предотвратява злонамерени опити за узнаване и/или използване на ПИН-кода чрез неоторизирани безконтактни сесии.

(4) Електронният носител може да поддържа и друга функционалност извън необходимата за извършване на електронна идентификация.

## Раздел IV.
## Спиране, възобновяване и прекратяване на удостоверение за електронна идентичност

**Спиране и възобновяване на удостоверение**

**Чл. 16.** (1) Спирането на удостоверението за електронна идентичност представлява временно преустановяване удостоверителната му сила по отношение на електронната идентичност на физическото лице – титуляр на удостоверението.

(2) При спирането на действието на удостоверението се ограничава възможността за потвърждаване на валидността му.

(3) Спирането на удостоверението се извършва чрез временното му публикуване в списъка с прекратените удостоверения в регистъра на удостоверенията за електронна идентичност.

(4) За всяко спиране се създава запис в отделен списък, съдържащ причината и началния момент на спирането, удостоверени по реда на Регламент (ЕС) 910/2014.

(5) Възобновяването се извършва чрез премахването на спряното удостоверение от списъка с прекратени удостоверения.

(6) В списъка по ал. 4 се създава запис за възобновяването по ал. 5.

(7) Когато едно лице има повече от едно удостоверения, те се разграничават по сериен номер.

**Прекратяване на удостоверение**

**Чл. 17.** (1) Прекратяването на удостоверение за електронна идентичност се извършва чрез публикуването му в списъка с прекратените удостоверения в регистъра на удостоверенията за електронна идентичност.

(2) Вписването в списъка по ал. 1 се извършва незабавно след възникването на съответното обстоятелство по чл. 22, ал. 1 и 2 от Закона за електронната идентификация.

**Управление на удостоверения от страна на титулярите**

**Чл. 18.** (1) Органът за електронна идентичност поддържа и предоставя достъп до интернет страница, на която титулярите могат да управляват удостоверенията си за електронна идентичност.

(2) Прекратяването и възобновяването на спряно удостоверение за електронна идентичност могат да се извършват от титуляря на удостоверението по електронен път с електронен подпис.

(3) Подновяването и временното спиране на удостоверение може да се извърши от титуляря по електронен път след успешна електронна идентификация.

(4) Прекратяването/спирането и възобновяването на спряно удостоверение за електронна идентичност по ал. 2 се вписват автоматично в списъците по чл. 17, ал. 1, съответно - чл. 16, ал. 4.

(5) Титулярите могат да дават наименования на удостоверенията си, в случай, че имат повече от едно. Наименованията са достъпни само за титулярите, органа за електронна идентичност и администраторите на електронна идентичност.

## Глава пета.
## ПРОВЕРКА НА ЕЛЕКТРОННА ИДЕНТИЧНОСТ

### Раздел I.
### Извършване на проверки на електронна идентичност

**Ред на проверка. Център за електронна идентификация.**

**Чл. 19.** (1) Проверката на електронната идентичност се извършва от всеки, който има правен интерес да идентифицира гражданите чрез електронния им идентификатор.

(2) Проверката на електронна идентичност се извършва автоматизирано по електронен път чрез център за електронна идентификация, при спазване изискванията на тази глава.

(3) Проверката на електронната идентичност, се извършва при спазване на технологичните стандарти за информационната сигурност по чл. 43, ал. 2 от Закона за електронното управление, както и на добри практики надеждност на инфраструктурата на публичният ключ и държането на криптографска двойка ключове от титуляря на електронната идентичност.

(4) Частно-правни субекти могат да използват удостоверението за електронна идентичност за идентифициране на повторно посещение на едно и също лице, в случай че удостоверението е предоставено директно, без участие на център за електронна идентификация. В този случай могат да се използват метода за преобразуване на електронния идентификатор в секторен електронен идентификатор, който да съхраняват. Действията по тази алинея нямат характера на електронна идентификация по смисъла на ЗЕИ.

(5) Проверката за електронна идентичност може да бъде свързана с предоставянето на конкретна услуга, когато доставчикът на услуги заяви това в комуникацията си с център за електронна идентификация.

(6) Центърът за електронна идентификация в Държавна агенция “Електронно управление” извършва и трансгранични проверки за електронна идентификация по реда на Регламент (ЕС) № 910/2014.

**Стандарти и протоколи**

**Чл. 20.** (1) Центровете за електронна идентификация извършват проверки на електронна идентичност чрез проверка на удостоверението за електронна идентичност, както и на притежанието на двойката криптографски ключове от титуляря на електронна идентичност, използвайки взаимна автентикация (mutual authentication) по протокола Transport Layer Security (TLS) 1.2 или по реда на ал. 2.

(2) Центровете за електронна идентификация трябва да позволяват идентификация и с използване на мобилно устройство за прочитане на електронния носител, като в този случай при стартиране на процеса на идентификация от друго устройство, титулярят посочва номер на мобилния телефон, чрез който да се осъществи идентификацията. Редът за проверка в този случай се определя от председателя на Държавна агенция “Електронно управление” с инструкцията по чл. 2.

(3) Проверката на удостоверенията за електронна идентичност включва:

1. проверка на съответствието на структурата на удостоверението със стандарта X.509

2. проверка за цялостност, непроменимост и интегритет на съдържанието на удостоверението;

3. проверка на валидността на удостоверението чрез проверка на удостоверителната му верига, срока му на действие и неговия статус в съответния списък с прекратени удостоверения.

(4) Допълнителни технически параметри на проверката са определят от председателя на Държавна агенция “Електронно управление” с инструкцията по чл. 2.

**Комуникация с центъра за електронна идентификация**

**Чл. 21.** (1) Центърът за електронна идентификация потвърждава електронната идентичност, като изпраща формализирано съобщение, съдържащо данни, заявени от

лице по чл. 19, ал. 1, ако то имат право на достъп до тях по силата на закон или с изричното съгласие на лицето, за което се отнасят данните.

(2) Комуникацията между центровете и лицата по чл. 19, ал. 1 се извършва по един от следните протоколи:

1. OpenID Connect;
2. SAML.

(3) Версиите на протоколите по ал. 1 се определят с инструкцията по чл. 2.

(4) Центърът за електронна идентификация може да отговаря и на запитвания относно данни и обстоятелства за идентифицираното лице по запитване на лице по чл. 19, ал. 1, без да разкрива самите обстоятелства.

(5) Данните и обстоятелствата, предоставяни от центъра за електорнна идентификация, се извличат в реално време от първичните администратори на данни.

(6) Центърът за електронна идентификация предоставя цялата си функционалност и в тестови режим, който е достъпен свободно и безплатно за доставчици на услуги.

**Регистрация на доставчици на услуги**

**Чл. 22.** (1) Лицата, извършващи проверки на електронна идентичност, се регистрират в един или повече центрове за електронна идентификация. Регистрацията е безплатна, и се извършва по електронен път, без да е необходимо одобрение от страна на центъра.

(2) След регистрация, лицата по ал. 1 получават идентификатор и ключ, чрез които могат да заявят електронна идентификация от центъра за електронна идентификация.

(3) Лицата по ал. 1 използват административен интерфейс, за да заявят данните, до които да им бъде осигурен достъп в процеса на идентификацията, като представят доказателства за правните основания за събирането и обработката на тези данни.

(4) За държавните органи данните по ал. 3 се получават чрез интеграция с административния регистър по чл. 61 от Закона за администрацията.

(5) В административния интерфейс лицата вписват и допълнителни данни, определени от председателя на Държавна агенция “Електронно управление” с инструкцията по чл. 2.

## Раздел II.
## Съхраняване на данни, свързани с електронната идентичност

**Ред и срок на съхраняване**

**Чл. 23.** (1) При извършване на проверка на електронна идентичност, лицата, осъществяващи дейност на център за електронна идентификация и държавните органи, съхраняват информация за извършените проверки по реда на този раздел.

(2) Информацията се съхранява за срок от 10 години.

**Обхват на данните**

**Чл. 24.** (1) Данните, които се съхраняват от центровете за електронна идентификация за всяка проверка, включват най-малко:

1. Резултата от извършеното подписване с частния ключ на титуляря при реализиране на взаимната автентикация по TLS 1.2 или автентикацията чрез мобилен телефон;

2. Времето на идентификацията, удостоверено в съответствие с Регламент (ЕС) № 910/2014;

3. Предоставените данни за титуляря на електронната идентичност;

4. Данни за доставчика на услуги, пред който е извършена идентификацията;

5. IP адреса, от който е извършена идентификацията.

(2) Титулярят на електронна идентичност има право на безплатен достъп до данните по ал. 1, отнасящи се за него. Достъпът се предоставя от центъра за електронна идентификация чрез публичен интерфейс, предоставен от център за електронна идентификация, след като титулярят се е идентифицирал електронно по реда на Закона за електронната идентификация.

(3) Титулярят има право да не позволи на центъра за електронна идентификация да записва IP адресите, от които е извършена идентификацията чрез приложението по ал. 2.

## Глава шеста.
## АДМИНИСТРАТОРИ НА ЕЛЕКТРОННА ИДЕНТИЧНОСТ

**Администратор на електронна идентичност**

**Чл. 25**. Администратор на електронна идентичност е лице, регистрирано от министъра на вътрешните работи, което отговаря на изискванията на Закона за електронната идентификация и този правилник и може да осигурява на дейностите по чл. 8, ал. 3 от Закона за електронната идентификация.

**Дейности**

**Чл. 26.** (1) Администраторът на електронна идентичност извършва чрез използване на собствени технически и програмни средства и персонал следните дейности:

1. приемане на писмени заявления от физически лица за издаване на удостоверения за електронна идентичност;

2. идентифициране на заявителя чрез проверка на представен документ за самоличност;

3. проверка по електронен път чрез защитена сесия за обмен на данни към органа за електронна идентификация за валидност на представения документ за самоличност и допълнително идентифициране на заявителя чрез изпратената от органа за електронна идентификация информация;

4. изпращане по електронен път до органа за електронна идентификация на заявления за издаване на удостоверения;

5. заявяване пред органа за електронна идентификация на промени в данните, въз основа на които е издадено удостоверението, както и на спиране, възобновяване и прекратяване на удостоверения;

6. персонализиране на удостоверения за електронна идентичност чрез запис върху електронни носители.

(2) Администраторите съхраняват информация и документация за дейностите по ал. 1 за срок от 20 години по реда на този правилник.

**Мерки за сигурност**

**Чл. 27.** (1) Администраторът на електронна идентичност е длъжен да вземе подходящи мерки за сигурност в съответствие с общоприети в международната практика документи (стандарти, технически спецификации, препоръки, ръководства и др.).

(2) Мерките за информационна сигурност трябва да са съобразение с изискванията на Закона за електронното управление.

(3) Работните станции, чрез които се персонализират удостоверения за електронна идентичност, трябва да отговарят на следните минимални условия:

1. да не се използват с администраторски профил;

2. да използват винаги последни версии на инсталирания софтуер;

3. в случай, че използват четци за електронни носители, да използват такива с хардуерна клавиатура;

4. да имат сигурна парола и автоматично заключване;

5. да разполагат със софтуер за защитна стена;

6. да са максимално защитени срещу вируси и друг зловреден софтуер;

7. да са част от мрежа, отговаряща на добрите практики за мрежова сигурност.

**Покриване на отговорността за вреди**

**Чл. 28.** (1) Администраторът на електронна идентичност поддържа разполагаеми финансови средства или застраховка, която да покрива отговорността за причинените на титуляря на електронната идентичност и на всички трети лица неимуществени и имуществени вреди от неизпълнение на задълженията му по закона и този правилник или поддържа финансови средства.

(2) Застраховката трябва да е с минимално застрахователно покритие в размер на 100 000 лв. за всяко увредено лице от всяко събитие.

(3) Администраторът на електронна идентичност е длъжен да уведомява незабавно органа за електронна идентификация за прекратяването на сключен договор за застраховка.

(4) Администраторът на електронна идентичност, който не е сключил договор за застраховка, е длъжен по време на дейността си да разполага с бързоликвидни разполагаеми средства (парични наличности и парични еквиваленти) в размер, не по-малък от 300 000 лв.

**Изисквания по отношение на наетия персонал**

**Чл. 29**. (1) Администраторът на електронна идентичност е длъжен да има на разположение необходимия брой квалифицирани служители, които във всеки момент от осъществяването на неговата дейност да осигуряват изпълнението на задълженията му.

(2) Техническият персонал на администратора на електронна идентичност трябва да притежава професионална квалификация или познания най-малко в следните области:

1. технологии за сигурност, криптография, инфраструктура на публични ключове (PKI);

2. технически норми за оценка на сигурността;

3. информационни системи.

(3) Всяко лице от техническият персонал на администратора на електронна идентичност трябва да не е осъждано за умишлено престъпление от общ характер, освен ако е реабилитирано, и да отговаря на изискванията за надеждност.

(4) Надеждност на лицето е налице, когато липсват данни относно:

1. осъществяване на дейност, насочена срещу обществения ред;

2. укриване или даване на невярна информация от проучваното лице за целите на проучването;

3. зависимост на лицето от алкохол и наркотични вещества.

**Изисквания по отношение на техническото оборудване и технологиите**

**Чл. 30**. (1) Администраторът на електронна идентичност следва да осигури и използва процедури и методи за администриране и управление на сигурността на използваната инфраструктура в съответствие с общоприети в международната практика стандарти за управление на информационната сигурност.

(2) Администраторът на електронна идентичност използва техническо оборудване и технологии, чрез които се изпълняват най-малко следните функции в използваната от него система за заявяване издаването и управлението на удостоверения за електронна идентичност:

1. проверки за доказване произхода на получаваната и обменяната информация, свързана с издаването и управлението на удостоверенията;

2. проверка на целостта на обменяните съобщения;

3. подписване на изпращаните съобщения;

4. архивиране на служебните данни и електронното им подписване;

5. поддържане целостта на съхраняваните и обменяните данни, в това число на данните за използваните криптографски ключове;

6. сигурно съхраняване на използваните от администратора частни ключове;

7. сигурно управление на достъпа до информационните ресурси;

8. създаване и архивиране на записи от вътрешни проверки, свързани с възникнали критични ситуации по отношение на информационната сигурност.

**Оценка на сигурността**

**Чл. 31.** (1) Методите за оценка на сигурността на използваната система се основават на разработената към стандарта ISO Standard 15408 обща методика за оценка (CEM) или други методики, осигуряващи еквивалентна оценка на сигурността.

(2) Проверките по чл. 13, ал. 2 от Закона за електронната идентификация се извършват на всеки 3 години или при промяна, която засяга надеждността.

**Процедури за сигурност**

**Чл. 32.** (1) Всеки администратор на електронна идентичност е длъжен да създаде и поддържа вътрешни процедури за сигурност, съгласно които осъществява дейността си.

(2) Процедурите за сигурност трябва да съответстват на общоприетите международни стандарти за информационната сигурност и нейното управление.

(3) Администраторът на електронна идентичност трябва да сертифицира процедурите си за сигурност по стандарта ISO 27001 или еквивалентен на него стандарт.

## Глава седма.
## ЦЕНТРОВЕ ЗА ЕЛЕКТРОННА ИДЕНТИФИКАЦИЯ

**Центрове за електронна идентификация**

**Чл. 33.** (1) В Държавна агенция “Електронно управление” се създава център за електронна идентификация.

(2) Дейност на център за електронна идентификация могат да осъществяват и лицата, регистрирани от министъра на вътрешните работи по реда на Закона за електронната идентификация и този правилник.

(3) Центровете за електронна идентификация осигуряват проверка на електронна идентичност по реда на глава пета.

(4) Извършваните услуги от лицата, осъществяващи дейност на център за електронна идентификация, могат да са възмездни.

(5) Центровете по ал. 2, могат да участват в процеса на трансгранична електронна идентификация по реда на чл. 2.

**Изисквания**

**Чл. 34.** Изискванията към администраторите на електронна идентичност по глава пета се прилагат към лицата, осъществяващи дейност на център за електронна идентификация.

**Софтуерно приложение**

**Чл. 35.** Софтуерното приложение, използвано от Центъра за електронна идентификация в Държавна агенция “Електронно управление” е с отворен код и свободен лиценз и може да бъде използвано от лицата по чл. 33, ал. 2 за техните нужди.

## Глава осма.
## РЕГИСТРАЦИЯ НА АДМИНИСТРАТОРИ НА ЕЛЕКТРОННА ИДЕНТИЧНОСТ И ЦЕНТРОВЕ ЗА ЕЛЕКТРОННА ИДЕНТИФИКАЦИЯ

**Изисквания за регистрация**

**Чл. 36.** (1) Лицата, които желаят да извършват дейност на администратор на електронна идентичност, съответно на център за електронна идентификация, подават до министъра на вътрешните работи заявление по образец, утвърден от него.

(2) Заявлението съдържа:

1. уникален идентификатор, име, съответно наименование, на заявителя;

2. уникален идентификатор, име, телефон и адрес на електронна поща на представляващите заявителя лица.

(3) Към заявлението, освен документите по чл. 15, ал. 2 от Закона за електронната идентификация, се прилагат:

1. списък на техническите средства, с които заявителят ще извършва на съответната дейност, включващ описание на техническите средства по тип и фабричен номер, както и копие от техническите паспорти, съгласно образец, утвърден със заповед на министъра на вътрешните работи, както и доказателства, че разполага с тях;

2. списък на персонала, извършващ дейностите, съдържащ имена, уникален идентификатор, образование, специалност и заемана длъжност, както и документи, удостоверяващи образование и квалификация, съгласно образец, утвърден със заповед на министъра на вътрешните работи;

3. доказателства за разполагаеми финансови средства или копие от договор за застраховка за вредите, които могат да настъпят вследствие на неизпълнение на задълженията му, с размер на застрахователното покритие;

4. за администраторите на електронна идентичност - прилаганите процедури за проверки на лични данни на титулярите на електронна идентичност и персонализиране на електронни носители;

(4) Заявителите трябва да отговарят на условията по чл. 11 от Закона за електронната идентификация

(5) За проверка на обстоятелствата по ал. 4 министърът на вътрешните работи събира информация от първичните администратори на съответните данни.

(6) Образците на заявлението и списъците по ал. 3, т. 1 и 2 се публикуват на интернет страницата на Министерството на вътрешните работи.

**Регистър на администраторите на електронна идентичност и на центровете за електронна идентификация**

**Чл. 37.** (1) Регистърът на администраторите на електронна идентичност и на центровете за електронна идентификация се води от длъжностни лица, упълномощени със заповед на министъра на вътрешните работи.

(2) Вписване в регистъра се осъществява след като длъжностното лице се е идентифицирало по реда на Закона за електронната идентификация.

(3) Всяко вписване, заличаване или промяна на обстоятелства се записва в журнал на събитията.

(4) За всеки администратор на електронна идентичност или център за електронна идентификация се вписва и удостоверение, чрез което администраторът, съответно центърът се идентифицира пред органа за електронна идентификация.

(5) За всеки администратор на електронна идентичност се вписват локациите на обектите му, включително с геокоординати.

(6) Удостоверението по ал. 4 е във формат X.509 и съдържа публичния ключ, съответстващ на частния ключ на администратора, съответно центъра.

(7) Частният ключ по ал. 6 се съхранява на електронен носител, отговарящ на изискванията по чл. 15.

(8) Регистърът предоставя данни за местоположението на администраторите на електронна идентичност в отворен, машинно-четим формат.

**Техническа свързаност**

**Чл. 38.** (1) Всяко лице, вписано в регистъра по чл. 37, ал. 1, е длъжно в 30-дневен срок от вписването да изгради свързаност, както следва:

1. за центрове за електронна идентификация - с регистъра за електронна идентичност;

2. за администратори на електронна идентичност - със системите за издаване на удостоверения за електронна идентичност.

(2) Министърът на вътрешните работи предоставя софтуерни средства за свързване на информационните му системи със съответния регистър.

(3) Наличието на свързаност се установява с протокол за 36-часови тестове за работоспособност, проведени под ръководството на Министъра на вътрешните работи.

(4) Наличието на свързаност се вписва в регистъра по чл. 37, ал. 1.

(5) Ръководителите на дипломатическите и консулските представителства на Република България, както и на местата по чл. 20, ал. 2 от Закона за електронна иденетификация, изграждат техническа свързаност със системите за издаване на електронна удостоверения за електронна идентичност.

**Архив на провежданите проверки**

**Чл. 39.** (1) За всяко регистрирано лице, в регистъра на по чл. 37 се създава и поддържа архив, в който се съхраняват данните и документите, предоставени по време на проверките по чл. 36, ал. 1 от Закона за електронната идентификация.

(2) Архивът не е публичен.

(3) Достъп до архива по ал. 1 имат лица, определени със заповед на министъра на вътрешните работи, които се идентифицират по електроннен път преди всяко осъществяване на достъп. Съхранява се пълна история на достъпа.

## Глава девета.
## РЕГИСТЪР НА ОВЛАСТЯВАНИЯТА

### Раздел I.
### Общи положения

**Регистър на овластяванията**

**Чл. 40**. (1) Регистърът на овластяванията, воден от министъра на вътрешните работи, е електронна база данни, съдържаща информация за овластяванията при упражняването на права пред държавен орган, организация, предоставяща обществени услуги и лица, осъществяващи публични функции.

(2) Центровете за електронна идентификация могат да водят регистър на овластяванията за упражняване на права пред лица, различни от посочените по ал. 1.

### Раздел II.
### Водене и съхраняване на регистъра

**Вписване в регистър**

**Чл. 41.** (1) Вписването в регистър по чл. 40 става въз основа на овластително изявление в електронна форма чрез интернет-страницата на регистъра или автоматизирано, чрез програмен интерфейс.

(2) Овластителното изявление съдържа следните полета:

1. уникален идентификатор на юридическото лице, когато упълномощителят е юридическо лице;

2. уникален идентификатор на пълномощника;

3. указване на услугите от административния регистър, от друг регистър на услуги, за които се извършва овластяване за представителство или услугите, предоставяни от лицата по чл. 29, ал. 4 от ЗЕИ;

4. указване за всяка от посочените по т. 3 услуги на обема на представителната власт, по номенклатура на възможната представителна власт за всяка услуга;

5. начална дата на представителството, ако упълномощителят желае представителството да възникне след определена дата;

6. крайна дата на овластяването, ако упълномощителят желае представителството да има действие до определена дата.

(3) Овластителното изявление се извършва след идентифициране на упълномощителя по реда на Закона за електронната идентификация.

(4) Овластителното изявление се подписва с електроненния подпис на лицето, извършващо изявлението.

(5) Всяко овластително изявление се вписва в регистъра по чл. 40, ал. 1 или ал. 2 заедно с времето на подаване, удостоверено в съответствие с Регламент (ЕС) № 910/2014.

**Условия за овластително изявление от името на юридическо лице**

**Чл. 42.** (1) Овластително изявление от името на юридическо лице може да се извърши само от законния му представител, вписан в регистрите на съответния първичен администратор на данни, създаващ уникалния идентификатор на юридическото лице.

(2) Проверката на законната представителна власт на лицето, извършващо овластителното изявление спрямо юридическото лице, се извършва автоматизирано.

**Оттегляне и разширяване обема на представителната власт**

**Чл. 43**. (1) Оттеглянето и разширяването на обема на представителната власт се заявява по реда на овластяването, като на упълномощителя се дава възможност да отбележи за кои услуги и за какъв обем на представителната власт за тези услуги оттегля, съответно разширява се извършва като ново вписване.

(2) За оттегляне на представителна власт не се изисква електронен подпис.

**Услуги и номенклатура за представителна власт**

**Чл. 44.** (1) Услугите, за които е възможно овластяване по чл. 40, ал. 1, както и номенклатурите за представителна власт, се извличат автоматизирано от административния регистър.

(2) Ако за определена услуга от административния регистър не е налична номенклатура за представителна власт, тя се състои от следните възможности:

1. заявяване на услугата;

2. заявяване представянето на информация и документи;

3. получаване на съобщения, свързани с електронната административна услуга;

4. получаване на резултатите от услугата;

5. обжалване на административния акт, резултат от услугата, или отказът от издаването на такъв;

6. оттегляне на заявлението.

(3) Услугите, за които е възможно овластяване чрез регистър по чл. 40, ал. 2, както и номенклатурите на представителната власт се заявяват пред центъра за електронна идентификация, от лицето по чл. 29, ал. 4 от Закона за електронната идентификация.

**Корекция на грешки**

**Чл. 45.** Грешки във вписани в регистър по чл. 40 обстоятелства, допуснати поради грешки в овластителното изявление, се поправят чрез подаване на ново изявление за промяна или оттегляне на представителната власт.

## Раздел III.
## Достъп до регистър на овластяванията. Извършване на справки.

**Достъп до регистър на овластяванията**

**Чл. 46.** (1) Регистрите по чл. 40 не са публични. Достъп до регистър има само лицето, извършило овластителното изявление, овластеното лице и лицето, предоставящо услугата, за която се отнася овластяването.

(2) Достъпът до регистър по чл. 40 се осъществява автоматизирано чрез програмни интерфейси или чрез интернет страницата на регистъра.

(3) Лицата, предоставящи услугата, за които се отнася овластяването, се идентифицират пред регистъра:

1. По реда на Закона за електронната идентификация, в случай на ръчен достъп от страна на длъжностно лице;

2. По реда на Закона за електронното управление, при автоматизиран достъп.

(4) При извършване на действие от страна на овластено лице, лицето, предоставящо услугата, за която се отнася овластяването, трябва да провери дали данните от електронния подпис на извършващия действието съвпадат с предоставените данни за овластеното лице, ако за предоставянето на услугата се изисква електронен подпис.

**Проверки и справки в регистър на овластяванията**

**Чл. 47**. (1) Проверки и справки в регистър по чл. 40 могат да се извършват само от лицето, извършило овластителното изявление, овластеното лице и лицето, предоставящо услугата, за която се отнася овластяването.

(2) Проверките и справките се извършват по идентификатор на услуга и/или:

1. уникален идентификатор на лицето, извършило овластителното изявление;

2. уникален идентификатор на юридическото лице - упълномощител;

3. уникален идентификатор на упълномощеното лице;

4. номера, под който е вписано овластителното изявление в регистъра.

(3) При проверка или справка, освен данните за овластяването, се предоставят и данните на лицата, участващи в него - име и уникален граждански идентификатор.

(4) Проверки и справки могат да се извършват за определен период.

## Допълнителна разпоредба

**§ 1.** По смисъла на този правилник “уникален граждански идентификатор” е единният граждански номер на българските граждани или личният номер на чужденците.

## Заключителна разпоредба

**§ 2.** Правилникът се приема на основание чл.5 от Закона за електронната идентификация.

**§ 3.** (1) Председателя на Държавната агенция “Електронно управление” приема инструкцията по чл. 2 в срок до 21 ноември 2016 г.

(2) Министърът на вътрешните работи издава заповедите по чл. 4, ал. 3, чл. 5, ал. 3, чл. 14, ал. 3, чл. 36, ал. 3, т. 1 и 2, чл. 37, ал. 1, чл. 39, ал. 3 в срок до 21 ноември 2016 г.

(3) Министърът на вътрешните работи и ръководителите на дипломатическите и консулските представителства определят със заповед лицата по чл. 13, ал. 1, съответно - чл. 13, ал. 3, в срок до 21 ноември 2016 г.

**§ 4.** Този правилник влиза в сила на 21 ноември 2016 г., с изключение на:

1. Членове 25-39, които влизат в сила на 21 декември 2016 г.;
2. Членове 3-6, чл. 9, 10, 13, чл. 14, ал. 1, 2 и ал. 4-8, чл. 16-19, чл. 20, ал. 1-3, чл. 21 и 22, които влизат в сила на 21 май 2017 г.;
3. Членове 40-47, които влизат в сила на 21 ноември 2017 г.