

ЕЛЕКТРОННАТА ИДЕНТИФИКАЦИЯ В ЕВРОПЕЙСКИЯ СЪЮЗ И БЪЛГАРИЯ – ТЕКУЩО СЪСТОЯНИЕ, ТЕХНОЛОГИЧНИ ОСОБЕНОСТИ И ВЪЗМОЖНОСТИ ЗА РАЗВИТИЕ

Гл. ас. д-р Кремена Маринова-Костова, k.marinova@uni-svishtov.bg

Катедра „Бизнес информатика“

Стопанска академия „Д. А. Ценов“ – Свищов

Резюме: Електронната идентификация е способ за удостоверяване на самоличността на лицата, използващи електронни услуги. Ето защо, успешното прилагане на електронното управление е немислимо без използването на единен метод за доказване идентичността на участниците в него.

Целта на настоящата статия е да изясни същността на електронната идентификация и да очертае приложението ѝ в Европейския съюз и България. В тази връзка са решени следните **задачи**: дефинирана е същността на е-идентификацията, очертани са основните ползи от прилагането ѝ, разгледани са техническите спецификации на схемата за електронна идентификация, описани са способите за електронна идентификация в Европейския съюз и България. В края на статията е изготвен SWOT анализ, който сравнява използваните варианти за е-идентификация на българските граждани.

Ключови думи: електронна идентификация, схема за електронна идентификация, електронен подпис, персонален идентификационен код, електронен идентификатор

JEL: L86, O38, K33

ELECTRONIC IDENTIFICATION IN THE EUROPEAN UNION AND BULGARIA - CURRENT STATE, TECHNOLOGICAL FEATURES AND OPPORTUNITIES FOR DEVELOPMENT

Head Assist.Prof. Kremena Marinova-Kostova, PhD, k.marinova@uni-svishtov.bg

Department of Business Informatics

D. A. Tsenov Academy of Economics - Svishtov

Abstract: Electronic identification is a means of authentication of individuals using electronic services. The successful application of e-Government is inconceivable without the use of a single method for proving the identity of the participants.

The article aims to clarify the nature of electronic identification and to outline its application in the European Union and Bulgaria. The following tasks are solved: the concept of the e-identification has been defined, the main benefits of its implementation have been outlined, the technical specifications of the electronic identification scheme have been examined, the methods of electronic identification in the European Union and Bulgaria have been described. At the end of the article a SWOT analysis is made, comparing the e-identification options used by Bulgarian citizens.

Key words: electronic identification, electronic identification scheme, electronic signature, personal identification code, electronic identifier

JEL: L86, O38, K33

ЕЛЕКТРОННАТА ИДЕНТИФИКАЦИЯ В ЕВРОПЕЙСКИЯ СЪЮЗ И БЪЛГАРИЯ – ТЕКУЩО СЪСТОЯНИЕ, ТЕХНОЛОГИЧНИ ОСОБЕНОСТИ И ВЪЗМОЖНОСТИ ЗА РАЗВИТИЕ

Гл. ас. д-р Кремена Маринова-Костова, k.marinova@uni-svishtov.bg
Катедра „Бизнес информатика“
Стопанска академия „Д. А. Ценов“ – Свищов

Въведение

Развитието на електронното управление в Европейския съюз (ЕС) и България поражда необходимостта от прилагане на единни средства за идентификация на гражданите, използващи електронни административни услуги. В тази връзка през 2014 г. Европейският парламент приема Регламент, който цели взаимно признаване на схемите за електронна идентификация на всички държави - членки на съюза, които отговарят на определени технически спецификации и съблюдават утвърдени стандарти за сигурност. На практика е-идентификацията в ЕС се осъществява посредством разнообразни инструменти, като част от тях в определена степен се развиват и у нас.

България съществено изостава спрямо останалите страни в ЕС по отношение на прилагането на единен идентификатор за своите граждани, като на този етап схемата за национална идентификация е само проект.

Обект на изследване в статията е електронната идентификация, а **предмет** - способите за нейното реализиране в ЕС и в България.

Основната авторова **цел** е да изясни същността на електронната идентификация и да очертае приложението ѝ в Европейския съюз и България.

За реализирането ѝ се дефинират следните **задачи**:

- да се изясни същността на е-идентификацията;
- да се очертаят основните ползи от прилагането ѝ;
- да се изведат техническите спецификации на схемата за електронна идентификация;
- да се опишат способите за електронна идентификация в Европейския съюз и България;
- да се изготви SWOT анализ на вариантите за е-идентификация в България

1. Същност и значение на електронната идентификация

Електронната идентификация (eID) е цифрово решение за удостоверяване самоличността на гражданите или организациите с цел достъп до административни, банкови, разплащателни и други услуги във виртуална среда. Освен идентификация и автентикация, голяма част от услугите за eID дават възможност и за подписване на електронни документи (Панайотова, 2018).

Електронната идентификация в Европейския съюз се осъществява в съответствие с **Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 година относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО** (Европейски парламент, 2014). Той

определя е-идентификацията като „процес на използване на данни в електронна форма за идентификация на лица, които данни представляват по уникален начин дадено физическо или юридическо лице, или физическо лице, представляващо юридическо лице“.

Във връзка с изискванията на Регламента, през 2016 г. в България е приет **Закон за електронната идентификация** (Народно събрание, 2016). Определението, заложено в него, е близо до това, дадено от ЕС: *тя е процес на използване на данни в електронна форма за идентификация, които представляват по уникален начин дадено физическо лице*. Законът използва понятието „електронна идентичност“, която се отъждествява с минималната съвкупност от характеристики, които отличават едно от друго лицата.

Всички тези дефиниции залагат в основата си главната характеристика на е-идентификацията – тя да е така организирана, че да бъде равностойна по значение и правни последици с идентификацията на лицата посредством техните лични документи или други уникални идентификатори, които те използват, за да се представят по еднозначен начин пред административните органи, бизнес и обществени организации.

Електронната идентификация и удостоверителните услуги при електронни трансакции носят някои съществени **ползи** за гражданите и бизнеса в рамките на ЕС (European Commission, 2018):

- възможност за извършване на разнообразни трансгранични услуги и трансакции – записване в университет, достъп до единно европейско здравно досие, извършване на електронни разплащания и др.;
- откриване на банкова сметка в ЕС без физическо присъствие в държавата;
- проверка на възрастта на лицата за достъп до социални медии и защита на непълнолетните лица, без разкриване на тяхната самоличност;
- споделяне само на необходимата информация за извършване на онлайн трансакцията или взаимодействието;
- намаляване на разходите;
- стимулиране на използването на нови удостоверителни услуги като времеви печати и др.

2. Технически спецификации на схемата за електронната идентификация в Европейския съюз

Съгласно **Регламент (ЕС) № 910/2014** от 29 септември 2018 г. всички държави - членки на ЕС признават средствата за е-идентификация, издадени от страна - член на Съюза, за достъп до електронни административни услуги, при условие че eID се издава в рамките на схема за електронна идентификация, одобрена от ЕС, а нивото на нейната осигуреност е „значително“ или „високо“. Нивата „значително“ или „високо“ гарантират, че използваната схема за електронна идентификация отговаря на определени технически спецификации, стандарти и процедури, които са в значителна и висока степен в състояние да предотвратят злоупотреби или промяна на самоличността.

Европейската Комисия разработва услугата eID Profile (European Commission, 2016), чиято основна цел е да подпомогне държавите-членки да изградят собствена схема за е-идентификация, съвместима с изискванията на ЕС. Последната версия е 1.1. от 16 декември 2016 г., като тя се състои от 4 основни документа, описващи формата на съобщенията, архитектурата на

оперативната съвместимост, криптографските изисквания за рамката за оперативна съвместимост и профила на атрибута eIDAS SAML.

2.1. SAML 2.0 формат на съобщенията (eIDAS Message Format_v1.1)

Обмяната на съобщения между схемите за електронна идентификация в рамките на ЕС става въз основа спецификациите на Security Assertion Markup Language 2.0 (SAML 2.0). Това е отворен стандарт за обмен на данни за удостоверяване и оторизация между страните, по-специално между доставчик на идентичност и доставчик на услуги. Той е XML-базиран протокол, който използва маркери за сигурност, за да предаде съобщения до даден получател. В документа се описва формата на метаданните и входящите и изходящите съобщения между възлите на системата за електронна идентификация.

2.2. Архитектура на оперативната съвместимост (eIDAS – Interoperability Architecture)

Документът определя компонентите, необходими за постигането на оперативна съвместимост между схемите за електронна идентификация, така че те да могат да работят в една обща мрежа. Необходимо е да се осигури рамка за трансгранична оперативна съвместимост, която да гарантира поверителността на данните за лицето, автентичността и целостта на данните за неговата идентификация и сигурната му идентификация в крайните точки за достъп.

На практика съвместимостта се постига чрез определяне на единни технически интерфейси между конекторите, възлите и услугите на схемите за електронна идентификация в страните от ЕС. Комуникацията между различните елементи също се осъществява посредством SAML 2.0.

2.3. Криптографски изисквания към рамката за оперативна съвместимост (eIDAS - Crypto Requirements for the eIDAS Interoperability Framework_v1.0.pdf)

Комуникацията между възлите на схемата за електронна идентификация се осъществява посредством браузър, инсталиран на крайните устройства на потребителите. За гарантиране на сигурността, поверителността и интегритета на изпращаните съобщения се използва хибридна криптографска схема, реализирана чрез XML криптиране със SAML. Съдържанието на съобщението се кодира чрез симетричен ключ, генериран на случаен принцип за всяко предаване. Криптирането на сесийния ключ се осъществява посредством статичен публичен ключ, достъпен за приемащата страна и се основава на сертификати X.509.

За защита на комуникацията посредством Интернет се използват криптографските протоколи Transport Layer Security (TLS). Те предполагат осъществяване на сигурна връзка между сървъра и клиента, като голяма част от параметрите ѝ се договарят между страните – методите за криптиране, алгоритмите за удостоверяване, шифрите и ключовете, които ще се използват по време на сесията. В схемата за трансгранична е-идентификация клиентът обикновено е браузърът на потребителя, докато сървърът е възел на мрежата. Ролята на сървъра е да установи автентичността на клиента въз основа на сертификати X.509.

2.4. Профил на атрибута eIDAS SAML (eIDAS SAML Attribute Profile)

Документът представя пълен списък на всички задължителни и незадължителни атрибути, включени в минималните набори от данни на схемата за електронна идентификация. Описан е способа за тяхното именуване, основаващ се на SAML 2.0, както и тяхното именуване посредством основния речник на ISA.

3. Приложение на електронната идентификация в ЕС

3.1. Електронна идентификация посредством лични карти

Една от формите за електронна идентификация са електронните лични карти, издавани от властите на дадена страна, които освен за физическа идентификация пред съответните държавни органи, могат да се използват и за онлайн доказване на самоличността на техния притежател. Следва да отбележим, че личната карта първоначално се издава, за да послужи пред определени администрации и има по-ограничена употреба от електронната идентификация, но впоследствие с добавянето на елементи за еднозначно удостоверяване на самоличността на индивида при трансакции по електронен път, нейното действие и обхват се разширяват (European Commission).

Електронните лични карти притежават всички особености на обикновените такива – имат физически носител, издават се от легитимна институция, притежават срок на валидност и т.н. В допълнение на това, те са снабдени с микрочип, използващ радиочестотна идентификация (Radio-Frequency Identification - RFID) за предаване на сигнал към устройство, четящо картата. Чипът съдържа информацията, отпечатана на картата, както и допълнителни биометрични данни за лицето като снимка, пръстови отпечатащи и др.

Електронните идентификационни карти, използвани в ЕС, трябва да бъдат разработени в съответствие с изискванията на стандарт ISO/IEC 14443, който дефинира изискванията към безконтактните карти с интегрални схеми, които се използват за идентификация (International Organization for Standardization, 2018). За разлика от традиционните RFID тагове, тези в личните карти трябва да могат да работят от много близо разстояние – под 10 сантиметра. Безжичната комуникация с четеца не може да започне докато личната карта не предаде уникален идентификатор, като по този начин се постига по-високо ниво на сигурност отколкото при комерсиалното използване на RFID.

Към настоящия момент 9 държави в ЕС (32%) използват електронни идентификационни карти с електронен подпис. Това са: Австрия, Белгия, Естония, Финландия, Германия, Италия, Литва, Португалия и Испания. При тях автентикацията се извършва чрез въвеждане на ПИН, а криптирането се осъществява посредством двойка от частен и публичен ключ. В допълнение на това, личната карта на Швеция съдържа допълнителен чип с функционалност, присъща на електронния подпис (Helmbrecht & Naumann, 2011).

3.2. Електронна идентификация посредством схеми, реализирани въз основа на изискванията на Регламент № 910/2014

Както вече споменахме в т.2, изискванията на Регламент № 910/2014 влязоха в сила на 29 септември 2018 г. и важат за всички държави от ЕС. Като първа крачка към предоставянето на трансгранични електронни удостоверителни услуги е прилагането на общите европейски изисквания към тях във възлите, т.е. администрациите, които ще предоставят ЕАУ. До този момент¹ 25 от страните (89%) развиват своята схема за е-идентификация във възлите на мрежата, а в 3 тя е на етап „планирана“ (European Commission, 2019). За съжаление, България е една от държавите, наред с Кипър и Финландия, които само са планирали внедряването на eID.

Макар и да няма задължителен характер, примерният софтуер, предоставян от Механизма за свързване на Европа (The Connecting Europe Facility - CEF), е най-популярният инструмент за внедряване на е-идентификацията – 14 от страните го използват изцяло, а 1 (Австрия) - частично.

12 от страните в ЕС (43%) вече са изградили схеми за електронна идентификация в съответствие с изискванията на Регламента, като при част от тях те са в етап на разглеждане и оценка. Способите, които са залегнали в схемите на отделните държави, са както следва:

- 4 страни (Хърватия, Чехия, Люксембург и Испания) използват само електронна идентификационна карта (eID Card);
- Белгия, освен личната електронна карта на гражданите на страната, прилага и електронна карта за чужденци;
- Естония дава възможност за използването на множество електронни идентификационни карти, в т.ч. лична, мобилна, дипломатическа и др.;
- Германия издава два документа: електронна идентификационна карта и електронно разрешително за пребиваване;
- Италия разработва две схеми. Едната се основава на използването на електронна идентификационна карта, а втората е т.нар. Обществена система за цифрова идентичност;
- Латвия използва както електронна идентификационни карти, така и карти с вграден електронен подпис;
- Португалия прилага три подхода: електронна идентификационна карта, цифров мобилен ключ и система за сертифициране на професионални атрибути;
- В Нидерландия електронната идентификация е само за бизнес организациите и се използват средствата на стандарта eHerkenning;
- Великобритания – системата GOV.UK Verify.

3.3. Други схеми за електронна идентификация

18 от държавите членки на ЕС (64%) използват или са в процес на разработка на други схеми за електронна идентификация. Част от страните прилагат повече от една схема: Кипър, Финландия, Гърция и Швеция – по две, а Нидерландия – три, като общият им брой е 24.

Най-често те използват смарт карти (9 от тях или 38%), потребителският логин се прилага в 7 (29%) от тях, 3 схеми ползват множество средства за идентификация, при 2 от тях се използват цифрови сертификати, а при 1 - удостоверяването е мобилно. При две от схемите в процес на разработка все още не са определени способите за идентификация.

¹ Февруари 2019 г.

4. Електронна идентификация в България – текущо състояние и възможности

4.1. Електронният подпис и персоналните идентификационни кодове като средство за електронна идентификация

Един от първите начини за електронна идентификация в България е чрез използването на електронен подпис. Първият закон, уреждащ електронния подпис, е **Законът за електронния документ и електронния подпис**, който в изпълнение на **Регламент (ЕС) № 910/2014** е преименуван на **Закон за електронния документ и електронните удостоверителни услуги** (Народно събрание, 2017). Съгласно тези нормативни документи, електронният подпис има правна сила, равностойна на саморъчния подпис, поставен от лицето. По смисъла на закона, електронният подпис може да бъде и усъвършенстваният електронен подпис, и квалифицираният електронен подпис. Той може да се прилага и за идентификация на физическите или юридическите лица при тяхното взаимодействие с частни и публични институции, но в допълнение на това се използва и за потвърждаване на волеизявление на неговия притежател.

Основен недостатък на електронния подпис е това, че се издава от частни компании, а не от държавен административен орган, което означава, че гаранциите за неговия притежател се поемат от издателя, а не са на национално ниво. В България оперират 5 компании, които могат да издават удостоверителни услуги: „Банксервиз“ АД, „Информационно обслужване“ АД, „Инфонотари“ ЕАД, „Спектър“ АД и „СЕР България“ АД.

По данни на Комисията за регулиране на съобщенията броят на издадените електронни подписи у нас към м. май 2018 г. е над 200 хил., като 1/3 са притежание на граждани или физически лица, което е под 1% от населението на страната (Любенова, 2018).

Като безплатна алтернатива на електронния подпис, някои институции въвеждат персонален идентификационен код (ПИК). Съществен недостатък на подхода е, че всяка администрация издава свой код и в част от случаите не е възможно да са достъпни услугите, предоставяни от една институция, с ПИК на друга.

Най-популярните персонални идентификационни кодове са тези, предоставяни от Националната агенция за приходите (НАП) и Националният осигурителен институт (НОИ), а Националната здравноосигурителна каса (НЗОК) нарича своя идентификатор уникален код за достъп (УКД). Кодовете съдържат различен брой и вид символи – ПИК-ът на НАП се състои от 12 цифри, докато тези на НОИ и НЗОК са 10 символни буквено-цифрени комбинации. С ПИК на НАП освен услугите на Агенцията, са достъпни и част от тези на НОИ, а от юни 2018 и данните от здравното досие на пациента от системата на НЗОК.

Персоналният идентификационен код е значително по-популярен от електронния подпис. По данни на НОИ броят на издадените кодове е достигнал 1 милион в средата на 2017 г., а на годишна база заявления подават над 150 хил. души (Национален осигурителен институт, 2018). Към средата на 2016 г. издадените персонални кодове от НАП наброяват 500 хил., с които са направени 6.5 мил. справки (24 часа, 2016). Най-слабо популярен е УКД на НЗОК – до края на май 2018 г. са издадени само 40 хил. кода (mediapool.bg, 2018).

4.2. Закон за електронната идентификация

В съответствие с изпълнението на изискванията, заложи в Регламент № 910/2014, през 2016 г. в България е приет **Закон за електронната идентификация** (Народно събрание, 2016). Съгласно Закона, електронната идентификация става посредством уникален за всяко физическо лице електронен идентификатор. Той се съдържа в Удостоверение за електронна идентичност, издадено с определен срок на валидност от министъра на вътрешните работи и от администраторите на електронна идентичност, вписани в регистър.

Удостоверение за електронна идентичност може да притежават всички лица, навършили 14 години, като издаването става след писмено заявление от страна на лицето, както и от неговите родители/настойници при непълнолетните граждани, а самото му получаване е лично срещу валиден документ за самоличност. Действието на удостоверението се прекратява с изтичане на неговия срок или при смърт на титуляря.

Във връзка с изпълнението на разпоредбите на Закона се създава дирекция „Електронна идентификация“, който функционира в рамките на Държавна агенция „Електронно управление“.

4.3. Пилотен проект „Електронна идентичност“

Практическата реализация на заложената в Закона за електронната идентификация Национална схема за електронна идентификация се реализира в рамките на пилотния проект „Електронна идентичност“ (Единен портал за електронни административни услуги, 2015).

Реализирането на услугата става посредством смарт карта за eID, като за целта е необходимо наличието на четец, свързан през USB порта на компютъра, който ще се използва при идентификацията. Достъпът до електронния идентификатор става чрез защитен ПИН код, който може да се променя от притежателя му. eID е разработено по такъв начин, че да е съвместимо с най-много операционни системи (Windows, MacOS и Linux) и работи с най-популярните браузъри (Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari). Необходимо е и инсталирането на актуална версия на Java, а за онези потребители, които желаят да сменят своя ПИК, е и приложението Java WebStart. Важен елемент е зареждането на служебните сертификати в браузъра, което позволява разпознаването на електронната идентичност като сигурен е-идентификатор.

В рамките на пилотния проект са раздадени безплатно 5 хил. карти и четци. Предвижда се в бъдеще вместо смарт карта да се използват и други носители на електронна идентичност – телефон, лична карта с е-идентификатор, флашка с по-малка карта, но тяхната практическа реализация е отложена. По-конкретно издаването на лични карти с чип, в който може да се вгради електронният идентификатор, ще започне от 1 януари 2020 г.

4.4. SWOT анализ на средствата за електронна идентификация в България

За да се направи сравнение между средствата за електронна идентификация, използвани в България, е разработен SWOT анализ, обхващащ описаните по-горе три подхода: чрез електронен подпис, чрез персонален идентификационен

код и посредством удостоверение за електронна идентичност (табл. 1). При изготвянето му се имат предвид анализите на Европейската комисия, свързани с технологиите за електронна идентификация (European Commission, 2017).

Таблица 1

SWOT анализ на средствата за електронна идентификация

Средство за е-идентификация	Електронен подпис	Персонален идентификационен код (ПИК)	Удостоверение за електронна идентичност
Силни страни (Strengths)	<ul style="list-style-type: none"> • Висока сигурност • Универсален характер – 1 идентификатор за връзка с множество администрации институции; • Правна сила, равнозначна на саморъчния подпис 	<ul style="list-style-type: none"> • Лесна употреба; • Независим е от брауъра, чрез който са достъпни електронните услуги; • Издава се от институция на национално ниво; • Безплатен; • Широко разпространен. 	<ul style="list-style-type: none"> • Единен идентификатор в рамките на ЕС; • Разработен е в съответствие с изискванията на Регламент № 910/2014; • Приложим е в компютърни системи с разнообразни операционни системи; • За достъп до електронните услуги се използва голям набор от брауъри; • Безплатен или с ниска цена; • Лесен за употреба; • Висока сигурност.
Слаби страни (Weaknesses)	<ul style="list-style-type: none"> • Издава се от частни компании; • Технически ограничения, свързани с използвания брауър за достъп до услугите; • Необходимост от инсталиране на допълнителен 	<ul style="list-style-type: none"> • Кодът е различен за услугите на всяка администрация, която го издава; • Издава се по постоянен адрес; • Няма универсален 	<ul style="list-style-type: none"> • В България е на ниво пилотен проект; • Необходимо е закупуването на четци за смарт карти; • Приложим е за настолни компютри и лаптопи, но не

	<ul style="list-style-type: none"> софтуер; • Платен; • Ниско разпространение – под 1% от българските граждани 	<ul style="list-style-type: none"> характер; • Ниско ниво на сигурност - не притежава изискуемите от Регламент 910/2014 3 нива на сигурност. 	<ul style="list-style-type: none"> и за мобилни устройства; • Изисква инсталиране на допълнителен софтуер.
Възможности (Opportunities)	<ul style="list-style-type: none"> • Регламент № 910/2014 води до промени, които улесняват употребата му; • Признаване от всички държави - членки на ЕС 	<ul style="list-style-type: none"> • Стандартизиране на кодовете, така че един идентификатор да се използва за достъп до електронните услуги на всички институции. 	<ul style="list-style-type: none"> • Реализация посредством други по-малки по обем технически устройства – флашки или мобилни телефони; • Интеграция с електронни лични карти от 2020 г.
Заплахи (Threats)	<ul style="list-style-type: none"> • Функционалността му може да бъде реализирана чрез транснационалната схема за електронна идентификация eIDAS. 	<ul style="list-style-type: none"> • Услугите с ПИК са достъпни изцяло и с електронен подпис; • Кодът лесно може да бъде „разбит“ и неоторизирани лица да го използват за справки или подаване на електронни документи. 	<ul style="list-style-type: none"> • Невъзможност от страна на всички държави в ЕС да се включат в eIDAS, което да ограничи неговата употреба.

Направеният SWOT анализ показва, че най-добрият и най-широко приложимият способ за е-идентификация е Удостоверението за електронна идентичност, което у нас е все още само пилотен проект, без реална практическа реализация. Електронният подпис, който също има сравнително универсален характер, е слабо разпространен сред физическите лица, най-вече заради цената си и техническите ограничения при прилагането му. Персоналните кодове, които са най-използвани в България, не отговарят на изискванията на ЕС по отношение на сигурността и не могат да бъдат признати извън нашата страна,

но фактът, че са безплатни и лекотата на използване ги правят предпочитани сред българите.

Заклучение

Регламент (ЕС) № 910/2014 определя, че всички държави - членки на Съюза от 29 септември 2018 г. трябва да прилагат средства за електронна идентификация, разработени в съответствие с утвърдена схема и отговарящи на определени стандарти за сигурност. Към днешна дата повечето страни в ЕС развиват своята схема за национална електронна идентификация, но в някои държави, сред които и България, тя е само планирана.

В настоящия момент в България на практика се прилагат два основни способа за е-идентификация: посредством електронен подпис и чрез ПИН, издаден от някоя държавна институция. Те обаче не са повсеместно приложими и не отговарят на всички изисквания, описани в Регламента. За преодоляване на тези недостатъци е необходимо въвеждането на т.нар. Удостоверение за електронна идентичност, което в най-голяма степен съответства на изискванията на законодателството на ЕС, както и на приетия у нас Закон за електронната идентификация. По този начин българските граждани ще имат достъп до електронни административни услуги, предлагани не само в България, но и от всички държави - членки на Европейския съюз, което е практически израз на тенденциите за глобализация и трансгранично сътрудничество.

Цитирана литература

1. 24 часа. (11 07 2016 г.). *6,5 милиона пъти е ползван персоналният код на НАП*. Извлечено от 24 часа.bg: <https://www.24chasa.bg/novini/article/5637368>
2. European Commission. (2016). *eIDAS eID Profile*. Извлечено от European Commission: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Profile>
3. European Commission. (2017). *Study on the use of Electronic Identification (eID) for the European Citizens' Initiative*. Brussels: everis.
4. European Commission. (28 09 2018 г.). *Cross-border digital identification for EU countries: Major step for a trusted Digital Single Market*. Извлечено от European Commission: <https://ec.europa.eu/digital-single-market/en/news/cross-border-digital-identification-eu-countries-major-step-trusted-digital-single-market>
5. European Commission. (2019). *Country overview*. Извлечено от European Commission: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Country+Overview+-+eID>
6. European Commission. (н.д.). *Electronic Identities – a brief introduction*. Извлечено от European Commission: http://ec.europa.eu/information_society/activities/ict_psp/documents/eid_introduction.pdf
7. Helmbrecht, U., & Naumann, I. (2011). *8: Overview of European Electronic Identity Cards*. John Wiley & Sons.
8. International Organization for Standardization. (04 2018 г.). *ISO/IEC 14443-1:2018*. Извлечено от <https://www.iso.org/obp/ui/#iso:std:iso-iec:14443:-1:ed-4:v1:en>

9. mediapool.bg. (31 05 2018 г.). *НЗОК: С кодове за фирмено ползване не могат да се разглеждат пациентски досиета*. Извлечено от mediapool.bg: <https://www.mediapool.bg/nzok-s-kodove-za-firmeno-polzvane-ne-mogat-da-se-razglezhdad-patsientski-dosieta-news279690.html>
10. Европейски парламент. (28 8 2014 г.). РЕГЛАМЕНТ (ЕС) № 910/2014 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 23 юли 2014 година относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО. *Официален вестник на Европейския съюз, L 257*.
11. Единен портал за електронни административни услуги. (2015). *Електронна идентичност Пилотен проект*. Извлечено от Електронна идентичност : <http://eid.egov.bg/>
12. Любенова, Н. (17 05 2018 г.). *Електронен подпис в телефона*. Извлечено от Мениджър.News: <https://www.manager.bg/biznes/elektronen-podpis-v-telefona>
13. Народно събрание. (20 5 2016 г.). Закон за електронната идентификация. *Държавен вестник, 8*.
14. Народно събрание. (24 10 2017 г.). Закон за електронния документ и електронните удостоверителни услуги. *Държавен вестник*.
15. Национален осигурителен институт. (29 01 2018 г.). *Над 150 000 персонални кодове за достъп до е-услугите на НОИ са издадени през 2017 г.* Извлечено от Национален осигурителен институт: <http://noi.bg/newsbg/4942-pic2017>
16. Панайотова, Д. (11 04 2018 г.). *Електронните личности превземат ЕС*. Изтеглено на 23 02 2019 г. от news.bg: <https://news.bg/politics/elektronnite-lichnosti-prevzemat-es.html>