Електронна търговия и електронен подпис

правни аспекти

Център за изследване на демокрацията
София, 2000 г.

Публикува се със съдействието на Българската народна банка

ISBN 954-9791-33-5

ул. „Лазар Станев“ № 1, 1113 София
тел. 971 3000, факс 971 2233
www.csd.bg csd@online.bg

Съдържание

Предговор **5**

Законопроект за електронния документ и електронния подпис, България **15**

Международни инструменти и актове на Европейския съюз **25**

Закон-модел на УНСИТРАЛ за електронната търговия 27
Директива 1999/93/ЕС на Европейския парламент и на Съвета на Европейския съюз от 13 декември 1999 г. относно правната рамка на общността за цифрови подписи 30
Предложение на Европейската комисия до Европейския парламент и Съвета на Европейския съюз за директива относно правните аспекти на електронната търговия в Общия пазар 39

Европа **43**

Кралски Указ-закон № 14 за електронния подпис от 17 септември 1999 г., Испания 45
Закон за цифровия подпис, Федерална република Германия 56
Закон за електронните комуникации, Великобритания 60
Законопроект за цифровия подпис, Дания 63
Законопроект за електронния подпис, Чехия 65

Америка **71**

Закон за цифровия подпис, щат Юта (САЩ) 73
Указ № 472 от 1998 г. на президента, Аржентина 78
Закон за достъп и използване на електронни съобщения, електронна търговия и електронен подпис, Колумбия 83

Азия **87**

Закон за електронните трансакции, Сингапур 89

Предговор

Глобалните предизвикателства

Не без основание последните пет години на XX в. се сочат като определящ период за информационната революция. Бързото развитие на информационните технологии в края на века е свързано с широко навлизане на електронни средства за комуникация във всички обществени сфери. Обменът на данни в електронна форма има много предимства в сравнение с традиционните методи. Откритите мрежи, като например Интернет, са достъпни и позволяват бърз и евтин обмен на информация независимо от нейния обем и разстоянията. Това оказва съществено влияние върху публичното управление, икономиката, търговията и личната сфера на гражданите. Все по-масовото използване на електронна поща и обмен на информация чрез Интернет променя начина на живот и на работа на хората. В развитите в стопанско и технологично отношение общества, преди всичко в Северна Америка[1], Западна Европа и Азия (Сингапур, Хонконг, Япония, Корея), все повече се използват електронни средства за сключване на договори и парични разплащания, включително за автоматичен обмен на бизнес документация. Появяват се нови бизнес конфигурации като виртуални предприятия, виртуални магазини и т. н.

Електронната търговия разкрива възможностите си радикално да промени икономическата дейност и социалната сфера. Тя се разпростира вече в такива сектори, като съобщения и пощенски услуги, радио и телевизия, финанси, дребна търговия, борсово посредничество, публична администрация, здравеопазване, образование и т. н.

Радикалните промени в технологиите обхващат и страните в преход. За това съдействат и други фактори – глобализирането на интеграционните процеси в световната икономика и прекратяването на глобалното стопанско противопоставяне.

Въпреки все още големите различия между развития и развиващия се свят по отношение на достъпа до телекомуникационни мрежи и Интернет и въпреки съществуващите неравномерности в развитието на електронната търговия в отделните страни и региони[2], тя постепенно се универсализира и глобализира и се превръща във важен елемент на световната икономика. Главната причина за това е, че електронната търговия значително подобрява ефективността и конкурентността на икономиката, увеличава бързината на сключване на сделки и води до чувствително намаляване цената на бизнес операциите.

Съществуват различни опити за дефиниране на понятието *електронна търговия*, но най-общо те се свеждат до разбирането ѝ като форма на покупко-продажба, осъществявана по електронен път, включително чрез Интернет като обмен на информация през електронни мрежи във всеки един етап от веригата на доставка, независимо дали се осъществява в рамките на една организация, между търговци, между търговци и потребители или между частния и публичния сектор, без оглед дали се заплаща, или не.[3] Електронната търговия създава съвършено нов модел на отношения по цялата верига „производство – потребление“, чиято цел е всички действия по една търговска сделка да се извършват по електронен път – отправянето на оферта, преговорите, сключва-

[1] В Доклад на Организацията за икономическо сътрудничество и развитие се сочи, че САЩ заемат водещо място с 80% от общия обем на електронна търговия в световен мащаб, което се обяснява преди всичко с липсата на пречки, типични за Европа и Азия, каквито са по-високата цена, липсата на достатъчно линии, по-бавната либерализация на телекомуникационния сектор, по-неразвитото законодателство (вж. The Economic and Social Impact of Electronic Commerce – Preliminary Findings and Research Agenda, OECD, 1999, p. 13).

[2] По данни на Европейската комисия в САЩ и Канада около 30% от населението има връзка с Интернет, докато в страните – членки на Европейския съюз – по-малко от 15%, като обаче последните са изпреварили Америка по брой на мобилните телефони, разглеждани като ключов терминал в бъдеще (вж. Financial Times, November 16, 1999). Очакванията на комисията са до 2005 г. половината от населението на Европа да има достъп до Интернет (вж. Commission Welcomes New Legal Framework to Guarantee Security of Electronic Signatures. IP/99/915. Brussels, 30 November 1999).

[3] E-commerce@its.best.uk, A Performance and Innovation Unit Report – September 1999, p. 10 (доклад на британското правителство, разработен по поръчка на премиер-министъра Тони Блеър, който се основава на шестмесечно изследване, анализира предприетите съвместни инициативи на правителството и бизнес организациите и съдържа стратегия за създаване на най-добри условия във Великобритания за развитие на електронната търговия).

нето на сделката и плащането. Ефективността на този модел се дължи на интегрирането на информационните потоци, на стандартизирането на процедурите и на откритостта му за всички участници в търговските сделки.

Електронният подпис е ключов въпрос и средство за създаване на сигурност и доверие в електронната търговия, в електронния обмен на данни и в откритите мрежи изобщо. Той позволява на получателя на изпратени по електронен път данни да определи от кого произхождат данните, както и да се провери дали тези данни не са били променени, дали не е била нарушена тяхната цялост. За разлика от сканираното изображение на саморъчния подпис на определено лице електронният подпис представлява информация в цифрова форма, набор от цифри, които служат за разкриване самоличността на автора му и съгласието му със съответните данни. Електронният подпис се основава на технологии за автентификация, на системи за кодиране и декодиране. Независимо от конретните методи за осъществяване на електронните подписи тяхната уредба трябва да е технологично неутрална.

Най-често използвана е асиметричната система за криптиране на данни, основана на *двойка ключове – публичен и частен. Частният ключ* се използва за генериране и кодиране на електронния подпис по определен алгоритъм. Достъп до него има само лицето, което създава електронно подписания документ. Частният ключ е свързан със съответен *публичен ключ* – публично достъпен код, с помощта на който адресатът на електронното съобщение може да разчете кодираното съобщение и да удостовери автентичността на електронното изявление и ненакърнеността на съдържанието му. За да изпълни своето предназначение електронният подпис следва да се признае по законодателен път за правно валиден наравно със саморъчния подпис, а правната валидност на всяка двойка ключове – да се удостоверява със специално електронно удостоверение от специализирана институция с удостоверителни функции. Удостоверението свързва притежателя на частния ключ и титуляр на електронния подпис с публичния ключ.

Създавайки несъществуващи досега възможности за развитие на бизнеса и на взаимоотношенията между публичните власти и частните лица, електронните средства за комуникация представляват сериозно предизвикателство за сигурността и защитата на трансакциите и взаимоотношенията, осъществявани по електронен път, за взаимоотношението между национално и наднационално правно регламентиране. Технологичните нововъдения се нуждаят от съответна нова правна регламентация на национално, регионално и международно равнище. Класическите правни уредби се основават на изискването за хартиен документ и саморъчен подпис, поради което не съдържат гаранции за правно валидно и надеждно осъществяване на електронна търговия и електронен обмен на данни. Въпросът обаче не може да бъде решен с промени само в националното право на отделните държави. Доколкото географските и националните граници стават ирелевантни за електронните комуникации, на дневен ред излиза понятието за „право на киберпространството“, различно от типичното национално право.[4]

Правно регулиране – състояние и динамика

С оглед посочените предизвикателства в последните години се активизират усилията за създаване на международни, общоевропейски и национални правни рамки за използването на електронните средства за комуникация – както общо, така и по отделни аспекти като електронна търговия, цифров подпис, електронен документ и т. н.

1. Международни инструменти и актове на Европейския съюз

Сред най-важните международни инструменти, приети през последните години или в процес на разработване и приемане, следва да се отбележат:

- *Закон-модел за електронната търговия*, приет от Комисията на ООН по международно търговско право през 1996 г.[5] и ръководство за прилагането му;
- *Проект на единни правила относно електронните подписи,* разработени и предложени от Комисията на ООН по международно търговско право;
- Проект за споразумение за електронна търговия, предложен от Икономическата комисия на ООН за Европа през 1999 г.[6];
- *Указания относно криптографията,* приети от Организацията за икономическо сътрудничество и развитие[7] през март 1997 г., с оглед понататъшното развитие на електронната търговия посредством използването на криптографията и цифровите подписи;
- *Общи обичаи в осигурената по цифров път меж-*

[4] Oppenheim, Charles. The Legal and Regulatory Environment for Electronic Information (third edition),1999, Infonortics Ltd, England, pp. 166 – 167; Johnson, D. & D. Post. Law and Borders – The Rise of Law in Cyberspace, 48 Stan. L. Rev. 1367, 1369-70, 1996.

[5] United Nations Commission on International Trade Law (UNCITRAL) – www.uncitral.com.

[6] United Nations Economic Commission for Europe UN/ECE – www.unece.org, CEFACT Electronic Commerce Agreement (проект от 3 март 1999 г.).

[7] Organization for Economic Co-operation and Development (OECD) – www.oecd.org.

дународна търговия (GUIDEC)[8]*,* известни повече като *Единни международни автентификационни и удостоверителни практики* – документ, разработен и публикуван от Международната търговска камара през 1997 г.[9] ;

- В рамките на Европейския съюз след дългогодишна подготвителна работа, многобройни дискусии и труден процес на постигане на съгласие на 30 ноември 1999 г. Съветът на министрите по телекомуникации приема представеното от Европейската комисия преработено *Предложение за Директива на Европейския парламент и Съвета на Европейския съюз относно общата рамка за електронни подписи (COM1998297final, 13.05.98)*. Директивата е обнародвана в „Официален вестник на Европейските общности“ от 19 януари 2000 г. като **Директива 1999/93/ЕС на Европейския парламент и Съвета на Европейския съюз от 13 декември 1999 г. относно рамката на общността върху електронните подписи.** Директивата е в сила от 20 януари 2000 г. Въз основа на вече приетата директива (по-специално чл. 13) държавите – членки на ЕС, се задължават да приведат в съответствие с нея законодателството си преди 19 юли 2001 г.
- През ноември 1998 г. комисията представя и *Предложение за Директива на Европейския парламент и Съвета на Европейския съюз относно правните аспекти на електронната търговия в Общия пазар.* През септември 1999 г. е прието изменено Предложение относно правната рамка на електронната търговия, а на 7 декември 1999 г. Съветът на министрите приема политическо решение относно развитието на електронната търговия. Очаква се в близко бъдеще предложението за директива да се приеме от Съвета на Европейския съюз.

Сред приоритетите на Европейската комисия е приемането на директиви за авторското право, за дистанционна продажба на финансови услуги, законодателство за електронните пари и електронната търговия, конвенции за договорно право и процедура за разрешаване он-лайн на спорове във връзка с електронната търговия.

2. Национално законодателство

Редица развити страни от Европа (главно държавите – членки на Европейския съюз), Америка и Азия са предприели значителни стъпки към създаване и въвеждане на законодателство, регулиращо използването на електронни средства за комуникация.

В най-общ план състоянието на законодателството в тези страни е следното:

2.1. Държави – членки на Европейския съюз

- На 15 юли 1999 г. долната камара на парламента на **Австрия** прие *Закон за цифровия подпис* и се очаква горната камара да го гласува в най-скоро време. Законът следва изискванията на директивата на ЕС.
- Правителството на Белгия изготви документ във връзка с признаването на електронните подписи и прегледа на съществуващото законодателство. Подготвен е и Закон за електронните подписи, чието внасяне в парламента е предстоящо.
- В **Дания** е подготвен законопроект за цифровите подписи, основаващ се на международните постижения в областта.
- През септември 1998 г. Държавният съвет на **Франция** публикува доклад относно необходимостта френското законодателство да регулира правната валидност на електронните подписи. Една година по-късно, през септември 1999 г., правителството одобрява *Законопроект за електронните подписи*, който признава еднаква правна сила на електронните и саморъчните подписи.
- На 13 юли 1997 г. парламентът на **Федерална република Германия** приема *Закон за цифровите подписи* като част III от пакета закони за регулиране на рамковите условия за информационните и комуникационните услуги. Законът е в сила от 1 август 1997 г. Правителството приема и Наредба за приложението на закона, в сила от 1 ноември 1997 г., която определя изискванията и отговорностите на удостоверяващите организации и техническите компоненти, използвани за създаването на цифрови подписи. Наред с вече действащите удостоверяващи организации в Трир (Германия) като удостоверяваща организация действа и *първият електронен нотариус*.
- През август 1999 г. в **Ирландия** излиза документ с цел формулиране на правни предложения за регламентиране на електронните подписи, електронните договори, удостоверителните услуги и други свързани с това въпроси. Крайна цел на обсъждането е изготвянето на *Закон за електронната търговия*. Формулираните в резултат на консултации предложения следват директивата на Европейския съюз и въвеждат конструкцията на усъвършенстван електронен подпис.
- Със *Закон № 59 от 15 март 1997 г.* във връзка с улесняване работата на публичната администрация в **Италия** се приема, че използването на електронни средства е правно валидно. През

[8] General Usage in International Digitally Ensured Commerce (GUIDEC), известни още като International Authentication and Certification Practices (UIACP), приети на 6 ноември 1997 г.

[9] International Chamber of Commerce (ICC) – www.icc.com.

октомври 1997 г. е приета правителствена Наредба за електронните документи, с която се признава правното действие на електронните документи, електронните подписи, електронните договори и електронните плащания. Съгласно наредбата електронният подпис служи като еквивалент на саморъчния подпис. Наредбата установява строги изисквания за формирането и дейността на удостоверяващите организации. Публична организация може да стане удостоверяваща организация за своите служители, но ако желае да предоставя удостоверителни услуги на други лица, публичната организация трябва да се регистрира по общия ред.

На 15 април 1999 г. в „Официален вестник на Европейските общности“ № 87 са публикувани *Технически правила за цифровите подписи*.

- В **Люксембург** е подготвен Законопроект за електронния подпис, чиято версия е от март 1999 г. и е съобразена с Директивата на ЕС за електронните подписи. Очаква се законопроектът да бъде приет в най-скоро време.
- Министерството на икономиката на **Холандия** прие план за действие във връзка с електронната търговия. Първият електронен нотариус действа он-лайн и предоставя цифрови удостоверения.[10]
- На 17 септември 1999 г. в **Испания** е приет кралски Указ-закон за електронния подпис, съобразен с правната рамка на общността за електронните подписи, създадена с директивата на ЕС.
- Правителството на **Швеция** проучва въпросите на електронните подписи и документи от 1996 г. и през февруари 1998 г. междуведомствена група с представители от различни министерства приема доклад „Електронните подписи – правен и технологичен преглед“. Докладът разглежда въпроси във връзка с формата, удостоверяващите организации и контрола върху тях, признаването на чуждестранни удостоверителни организации, съдържанието и ефекта на удостоверенията, доказателствената сила в съдебния процес.
- Във **Великобритания** на 18 ноември 1999 г. Камарата на общините приема Закон за електронните комуникации, който влиза в сила през април 2000 г. Във връзка с това е в ход реформа, целяща промени в над 40 000 акта на английското право, основаващи се на хартиен документ и саморъчен подпис. Британските телекомуникации са в процес на преструктуриране, насочено към намаляване на тарифите за достъп и опериране в мрежите.[11]
- Министерството на правосъдието на **Финландия** проучва опита на други държави в регулирането на електронните подписи. Приет е Закон за електронни персонални идентификационни карти. Тези карти са снабдени с необходимите ключове и предоставят възможност за електронно подписване на данни във връзка с данъчните задължения и социалното осигуряване на субектите, но трансакции като покупко-продажба на недвижима собственост изискват изповядване пред нотариус.

2.2. Америка

- В **САЩ** в законодателството на **отделните щати** през последните 4 години са приети закони относно цифровия подпис и електронната търговия. Първият закон е приет в щат Юта[12]. Сега такива закони има във всички щати.

  На своята годишна конференция през 1999 г. комисията за унифициране законодателството на щатите одобри *Единен закон за електронните трансакции* (Uniform Electronic Transactions Act), който се препоръчва да бъде приет във всички щати.

  На **федерално ниво** на 19 ноември 1999 г. в Сената е приет *Закон за електронната търговия* (Millenium Digital Commerce Act). Законът регламентира доказателствената сила на електронните подписи в съдебния процес.

  През май 1998 г. САЩ излиза с *Проект за международна Конвенция за електронни трансакции*, представен на работна сесия на УНСИТРАЛ.
- От 17 март 1997 г. в **Аржентина** по силата на правителствена *Резолюция № 45 от 1997 г.* относно приложението на електронните подписи в публичната администрация се допуска използването на цифров подпис в националния публичен сектор съгласно „Технически насоки относно стандартите за цифрови подписи“ на Подкомитета по криптография и електронни подписи. С Указ на президента № 427/98 се предвижда за срок от 2 години използването на цифров подпис със същата правна сила като саморъчен подпис с цел въвеждане на електронен документооборот в националния публичен сектор – централни и местни органи на държавната администрация, държавни предприятия, предприятия, банки и финансови институции с преобладаващо държавното участие. На 18 август 1999 г. правителството на Аржентина представи *Законопроект за цифровите подписи*, който регламентира общото правно действие на електронните договори, подписани с цифрови подписи. Подготвени са и изменения в Гражданския кодекс, отразяващи промените

[10] Вж. www.diginotar.nl.

[11] Вж. Financial Times, November 20/November 21, 1999.

[12] Законът за цифровия подпис на щат Юта е приет на 27 февруари 1995 г. и е в сила от 1 май с. г.

във формата на сделките от гледна точка на електронната търговия.

- През 1998 г. в **Колумбия** е приет *Закон за достъпа и използването на електронни съобщения, електронна търговия и електронен подпис*.

2.3. Азия

- В **Сингапур** през 1998 г. е приет Закон за електронните трансакции, с който се регламентират електронните подписи, електронните договори, удостоверителните услуги и електронното вписване. Законът е комбинация от опита на щатите Илинойс и Юта, Закона-модел на УНСИТРАЛ за електронната търговия, Закона на ФРГ за цифровия подпис и съответния закон на Малайзия.
- В края на 1999 г. в **Хонконг** е приет *Закон за електронните трансакции*.
- От 1997 г. в **Малайзия** е в сила *Закон за цифровия подпис*. Съществува и организация, която предоставя удостоверителни услуги.
- Министерството на информацията и комуникациите в **Южна Корея** работи върху приемането на законодателство, което да осигури използването на цифрови подписи. В процес на подготовка са проекти за *Закон за електронната търговия* и *Закон за електронния подпис*.

2.4. Централна и Източна Европа

В страните от Централна и Източна Европа се работи по приемане и утвърждаване на законодателство относно електронния подпис (**Чехия**, **Естония**, **България** и др.)

Национални аспекти и приоритети в България

1. Инициативи в България

Електронната търговия е от изключителна важност за структурната реформа на икономиката и за успешната административна реформа, както и за присъединяването на страната ни към Европейския съюз. В контекста на тези потребности българското правителство прие решение, насочено към интегриране в европейската инфраструктура за електронна търговия, обявена в документа COM(97)157 на Комисията на Европейския съюз „Европейска инициатива за електронна търговия“ и в Декларацията на Бонската конференция на министрите „Глобални информационни мрежи“ за един от приоритетите на съюза. В решение на Министерския съвет от 1 декември 1997 г., което предвижда разработване на *Национална програма за електронна търговия,* електронната търговия е определена като национален приоритет за България.

С Постановление № 40 от 1998 г. Министерският съвет създава Координационен съвет по проблемите на информационното общество с основна функция „да разработва и предлага за приемане от Министерския съвет на стратегията и националната програма за развитие на информационното общество в Република България“. С Решение на МС № 679 от 29 октомври 1999 г. са приети Стратегия за развитие на информационното общество и Национална програма за развитие на информационното общество. В стратегията се посочва изрично, че една от основните цели на прехода към информационно общество е „създаването на *правна и регулаторна рамка* за предоставяне на услуги, за живот и работа в новата информационна среда, хармонизирана с тази на Европейския съюз“[13].

Наред с прегледа на приетите в последно време закони, имащи отношение към информационното общество (Закон за далекосъобщенията, Закон за радиото и телевизията, Закон за националната стандартизация, Закон за статистиката, Закон за топологиите на интегралните схеми и т. н.), особено внимание в стратегията се обръща на необходимостта от правна уредба на: достъпа до информация, развитието на Интернет като глобална комуникационна среда, услугите на информационното общество, *електронните подписи и сигурността на информационния обмен и защитата на данните*, компютърните престъпления. Важно място в контекста на предложените комплексни мерки заема правната уредба на електронните подписи, която в съответствие с нормите на Европейския съюз следва да гарантира сигурността на информационния обмен, целостта и достоверността на съобщенията в мрежата. Посочени са и редица съществени елементи, подлежащи на правна уредба:

- отговорността на участниците в информационния обмен;
- еднаквото значение на електронните подписи с установените досега в практиката форми за идентификация на страните;
- технологично неутралната уредба на електронните подписи без оглед на конкретните методи за осъществяването им;
- определянето на „удостоверяващи органи“ – трети лица за страните, използващи електронни подписи, – които могат да потвърдят „ключа“ на разменяното между страните кодирано съобщение;
- международното сътрудничество за взаимно

[13] Стратегия за развитие на информационното общество в България, в: „Информационно общество“, Информационен бюлетин на Комитета по пощи и далекосъобщения, 1999 , с. 6. http://www.cpt.bg/BG/Infosoc/str.htm.

признаване на сертифицирането на двустранна и многостранна основа.

Заинтересованите институции и бизнес организации в България също предприемат стъпки в отговор на глобалните предизвикателства и националните приоритети. Внимание заслужават усилията за създаване на система за плащания на стоки и услуги чрез Интернет с национални дебитни или международни кредитни карти[14]; предложеният от Централния депозитар проект на „Концепция за изграждане на комуникационна инфраструктура на капиталовия пазар в страната и използването на цифров подпис"; стартиралата в началото на тази година практика за издаване на цифрови сертификати от Българската стопанска камара (като изключителен представител на „Глобал сайн" – официална сертифицираща институция на Европейската комисия)[15]; разработваната от Софийската стокова борса система за електронно борсово търгуване на стандартизирани зърнени контракти.

За повечето от предлаганите технически и технологични решения обаче липсва необходимата правна основа. Те могат да помогнат при разработването на новото законодателство, но не се съпътстват от конкретни предложения за съответно правно регулиране.

Предвид необходимостта от законодателна уредба в края на 1998 г. в рамките на Правната програма[16] на Центъра за изследване на демокрацията (www.csd.bg) започна работа по правните аспекти на електронната търговия и електронния подпис. Работната група включва изявени юристи с трайни интереси в областта на разглежданата проблематика:

Ангел Калайджиев – доктор по право, доцент в СУ „Св. Кл. Охридски"[17],

Борислав Белазелков – съдия във Върховния касационен съд, преподавател в СУ „Св. Кл. Охридски",

Весела Станчева – доктор по право, адвокат в адвокатска кантора „Джингов, Гугински, Кючуков и Величков", преподавател в УНСС,

Мария Йорданова – доктор по право, адвокат, ръководител на Правната програма на Центъра за изследване на демокрацията[18],

Стефан Кючуков – адвокат в адвокатска кантора „Джингов, Гугински, Кючуков и Величков", бивш ръководител на Правната програма на Центъра за изследване на демокрацията[19].

Работата на групата започна с проучване на чуждото законодателство и съществуващия опит и разработване на концепция за законодателната уредба. Същевременно бяха проведени редица консултации с институциите, заинтересовани от законодателно регулиране на електронната търговия и електронния подпис – Българската народна банка, Централния депозитар АД, Българската фондова борса АД, „Банксервиз" АД, БОРИКА АД, Асоциацията на търговските банки, Българската търговско-промишлена палата, Българската стопанска камара, Междуведомствената комисия по електронна търговия, отделни търговски банки, Министерския съвет, Министерството на правосъдието, Министерството на финансите, Държавната комисия по ценните книжа, Държавната комисия по далекосъобщения, Софийската стокова борса АД и др. Представители на тези институции и широк кръг експерти – юристи, икономисти и специалисти по информационни технологии, се включиха в **Експертен съвет** който оказваше консултантска помощ на работата на групата. Бяха поканени и взеха участие в работата *ad hoc* консултанти от страната и чужбина. В отделните фази от работата по законопроекта се провеждаха обсъждания и дискусии.[20]

Представеният в настоящото издание вариант на законопроекта отразява виждането за законодателната уредба на електронния документ и електронния подпис на членовете на работната група. Отразени са направените от членовете на Експертния съвет, консултантите и представителите на всички заинтересовани институции бележки, препоръки и коментари. Законопроектът е представен и обсъден на разширено заседание на Националния съвет по платежни системи към БНБ, проведено на 7 март т. г., и е съобразен с предложенията на участниците в него.

Предложеният законопроект за електронния документ и електронния подпис е съобразен с основните положения на **Директива 1999/93/ЕС на Европейския парламент и Съвета на Европей-**

[14] Матрозов, Александър, Георги Маринов. Е-плащания чрез Интернет с банкови карти, издадени в България, в. „Пари", приложение Банки и финанси, 18 октомври 1999 г.

[15] Вж. в. „Капитал", 8 – 14 януари 2000 г.

[16] Правната програма работи с широк кръг експерти и е натрупала значителен опит в анализа на законодателни актове и разработването на законопроекти, някои от които вече са приети и се прилагат успешно (Закона за особените залози), други са в процес на разглеждане (един от внесените в парламента законопроекти за организациите с нестопанска цел), а трети са подготвени и представени за публично обсъждане (законопроект за народния защитник, законопроект за електронния документ и електронния подпис).

[17] Вж. Калайджиев, Ангел. За електронната форма на сделките с ценни книжа, Бюлетин № 9/1999 г., Комисия по ценните книжа и фондовите борси.

[18] Вж. Йорданова, Мария. Правна уредба на електронния подпис у нас, сп. „Банкови информационни технологии" № 1/1999 г.; Електронният подпис – предложение за законодателна уредба, в. „Пари", 6 март 2000 г.

[19] Вж. Кючуков, Стефан. Правни аспекти на „електронния подпис" и „електронния документ", сп. „Банкови информационни технологии", 1997 г.

[20] По-подробно за работата по законопроекта и участниците в процеса вж.: www.csd.bg.

ския съюз от 13 декември 1999 г. относно рамката на общността върху електронните подписи (в сила от 20 януари 2000 г.), както и с редица от успешно прилаганите вече законодателни решения в други страни. Взети са предвид и приетите международни инструменти в тази област.

2. Законопроект за електронния документ и електронния подпис

Предложението за законопроект урежда електронния документ и електронния подпис, както и условията и реда за предоставяне на удостоверителни услуги.

Законът урежда приложимостта на електронния документ и електронния подпис не само в областта на задълженията и договорите, но и в останалите правни сфери. При уреждане на правното значение на електронното изявления и електронния подпис е изходено от начина, по който са уредени писменото изявление и саморъчният подпис в гражданското и административното право, като са отчетени всички особености, дължащи се на електронната форма. Това ще позволи при приложението на закона да бъдат ползвани всички достижения на доктрината и съдебната практика в областта на доказването, оспорването и признаването на писмените изявления и саморъчния подпис.

С влизането в сила на закона не се предвижда задължение за никого да използва електронни документи и електронен подпис. Въз основа на закона гражданскоправните субекти могат да възприемат тази възможност, което ще рече, че без допълнителна намеса на държавата на практика приложното поле на закона ще се ограничи само в областта на задълженията и договорите.

На Министерския съвет е предоставено да посочва кога и кои подчинени на него административни органи, общини и кметства ще бъдат задължени да приемат и издават електронни документи, подписани с електронен подпис, като по този начин приложното поле на закона ще се разпростира постепенно (в зависимост от технологичната готовност на отделните административни органи) и в областта на административното право.

Предвид изискването съдебните процедури да бъдат уредени в закон, разширяването на приложното поле на закона и в областта на съдопроизводството следва да бъде извършено с отделен закон, който да предвиди специални правила в съответните процесуални закони, като разпоредбите на този закон ще се прилагат на общо основание.

Останалите държавни институции, неподчинени на Министерския съвет (като Народното събрание, Конституционния съд, Сметната палата, Българската народна банка, Държавната комисия по ценните книжа, Комисията за защита на конкуренцията и т. н.) ще решават със свои актове от кога са в готовност да приемат и издават електронни документи, подписани с електронен подпис, като приемат и съответни вътрешни правила за това. Разбира се, за държавата остава открита възможността да задължи със закон всяка институция да приема и издава електронни документи, подписани с електронен подпис.

„Електронен подпис“ по смисъла на закона е „сигурният подпис“ по смисъла на директивата, а обикновен или „несигурен“ по смисъла на директивата е „автентификация“ по смисъла на закона. Обикновеният електронен подпис е определен в Директивата на Европейския парламент и Съвета на Европейския съюз относно правната рамка на общността за електронните подписи като „информация в електронна форма, придружена или логически свързана с друга електронна информация и служеща като средство за автентификация, а *сигурният* (или *„усъвършенстван“) електронен подпис* – като „електронен подпис, който отговаря на следните изисквания: 1) свързан е по уникален начин с титуляря; 2) дава възможност за идентифициране на титуляря; 3) създаден е със средства, които титулярят държи единствено под свой контрол; и 4) е свързан с информацията по такъв начин, че всяка последваща промяна в нея може да бъде открита“.

Законът приема названията „електронен документ“, „електронно изявление“ и „електронен подпис“ от съображения, че те са приели гражданственост и се използват широко заедно с други сходни названия като „електронен обмен на данни“ (електронни съобщения), „електронна поща“, „електронна търговия“ и др. Електронните изявления, документ и подпис са уредени като *цифрови* съгласно чл. 2, ал. 1, чл. 3, ал. 1 и чл. 15, ал. 1 от законопроекта. Гражданственост е придобило и понятието „цифров подпис“, но ако се възприеме, то би създало погрешното впечатление за наличието на разлика от електронното изявление и електронния документ (които също са уредени като цифрови), но „цифрово изявление“ и „цифров документ“ не звучат добре и не се използват нито в приетата директива, нито в приетото в отделни страни ново законодателство. По-точно би било да се възприемат понятията „изявление в цифрова форма“ и „документ в цифрова форма“, но те са по-тежки за употреба.

Материята е изложена по институти и основните понятия са дефинирани на съответното място. Не се обясняват термини, когато законът не им придава особено значение в сравнение с тяхното обикновено значение. По тази причина законът не съдържа списък на използваните термини с тяхното значение.

- Общите положения са предмет на регулиране в първа глава.
- Във втора глава е закрепен принципът, че писмената форма се смята спазена, ако е съставен електронен документ. В нея се дефинират понятията електронно изявление – „словесно изявление, представено в цифрова форма чрез общоприет стандарт за преобразуване, разчитане и визуално представяне на информацията“, и електронен документ – „електронно изявление, записано върху магнитен, оптичен или друг носител, който дава възможност да бъде възпроизвеждано“. Въвеждат се специални правила за определяне на автора, титуляря и адресата на електронното изявление, за времето и мястото на неговото изпращане и получаване. Регламентират се автентификацията на електронното изявление, защитата на неговото съдържание и рискът от грешки при предаване на електронно изявление.
- В трета глава се прогласява правната валидност на електронния подпис и се дава определение на сигурния електронен подпис като „преобразувано електронно изявление, включено, добавено или логически свързано със същото електронно изявление, преди преобразуването“. Определени са принципите за преобразуване чрез използване на одобрен от регистърната институция алгоритъм, основаващ се на асиметрична криптосистема, чрез която се създава двойка ключове (публичен и частен), така че: 1) чрез използването на публичния ключ да може по несъмнен начин да се установи дали преобразуването на първоначалното електронно изявление е извършено чрез използване на съответния му частен ключ и изменяно ли е електронното изявление след преобразуването; 2) от публичния ключ да не може да се открие съответният му частен ключ.

Тайната на частния ключ гарантира сигурността на електронния подпис.

Регулирането и контролът върху дейността по предоставяне на удостоверителни услуги се възлагат на Държавната комисия по далекосъобщения (ДКД) като *национална регистърна институция*, която да регистрира удостоверяващите организации и да води публичен регистър на удостоверенията за публичния им ключ. Възприетият режим е регистрационен, а не лицензионен. ДКД може да откаже регистрация само, когато не са налице предвидените в закона условия. Редът за регистрация следва да бъде определен с наредба на Министерския съвет. Предвидени са правомощията на регистърната институция, както и производствата за регистрация на удостоверяващите организации и за заличаване на регистрацията им.

Регламентиран е и статутът на удостоверяващите организации – търговец, регистриран в ДКД, който извършва следните удостоверителни услуги: издаване на удостоверения за електронен подпис и водене на публичен електронен регистър за тях, предоставяне на възможност на титулярите на електронни подписи за създаване на частен и публичен ключ, предоставяне на всяко трето лице на достъп до регистрираните при тях удостоверения, удостоверяване на датата и часа на представяне на електронен документ, подписан с електронен подпис. Детайлно са уредени изискванията към дейността на удостоверяващите организации, техните задължения и отговорността, която носят пред титуляря на електронния подпис и пред всички трети лица, с цел да се гарантира в най-голяма степен сигурността и надеждността на използването на електронни подписи. Същевременно е предвидена и отговорност на титуляря и автора на електронния подпис към трети лица и към удостоверяващата организация. Предвидено е отношенията между съответната удостоверяваща организация и титуляря на електронен подпис да се уреждат с писмен договор.

В законопроекта са уредени реквизитите на удостоверението като електронен документ, издаден и подписан от удостоверяващата организация, процедурите по издаване на удостоверение, по спиране, възобновяване и прекратяване действието на удостоверението. Формулирани са общите изисквания към публичните регистри на издадените удостоверения, като се предвижда устройството и дейността им да се уреди с наредба на Министерския съвет.

- В четвърта глава се съдържат общите правила за приложение на елекронния документ и електронния подпис от държавата и общините, което ще бъде постигнато постепенно със създаване на необходимите за това условия и инфраструктура и с приемането на съответните актове.
- В пета глава се предвижда защитата на личните данни, събирани от удостоверяващите организации за нуждите на извършваната от тях дейност и водените от тях регистри, както и на личните данни, известни на ДКД, да се урежда със закон. Според законопроекта събирането на лични данни за автора и титуляря на подписа и използването на тези данни е допустимо, само доколкото е необходимо за издаването и ползването на удостоверение. Изключения от този принцип са възможни само, ако това е позволено със закон или с изричното съгласие на лицето, за което се отнасят личните данни.
- Шеста глава определя условията, които следва да са изпълнени, за да се признават удостоверения, издадени от удостоверяващи организа-

ции, регистрирани в други държави, за равностойни на удостоверения, издадени от българска удостоверяваща организация. Предвижда се установяването на предвидените условия да се извършва от Държавната комисия по далекосъобщения по искане на лицето, на което чуждестранната удостоверяваща организация е издала удостоверение, или на трето лице по ред, определен с наредба на Министерския съвет. Това не се отнася за случаите, когато удостоверението или удостоверяващата организация, издала удостоверението, са признати съгласно влязъл в сила международен договор. Електронна справка за чуждестранните удостоверяващи организации, относно които е признато съответствие, съдържаща публичните ключове на чуждестранните удостоверяващи организации, подписана с електронния подпис на ДКД, може да бъде поискана от всяко лице.

В закона се съдържат административнонаказателни разпоредби като за съставянето на актове, издаването, обжалването и изпълнението на наказателни постановления се препраща към Закона за административните нарушения и наказания.

В преходните и заключителни разпоредби се уреждат промените в действащото законодателство с оглед съобразяването му с изискванията на предлагания законопроект. Предвидено е ново нотариално удостоверяване – „удостоверяване на електронен подпис“, като е уредена процедурата по извършването му. Предвидено е като единствена възможност удостоверяване на електронен подпис, извършен лично от автора пред нотариуса, с което е изключена възможността за удостоверяване на електронен подпис, изпратен до нотариуса по електронен път. С удостоверяването на подписа се удостоверява и датата, но ако титулярят на подписаното с електронен подпис изявление има интерес да получи само достоверна дата, той може да се обърне към удостоверяващата организация.

***

Настоящото издание цели да представи правните аспекти на електронния документ и електронния подпис на вниманието на заинтересованите институции и широката публика, както и да стимулира публичния дебат по предложения законопроект с оглед ускорено приемане на най-подходящото за България законодателно решение.

В сборника са включени предложението за *Законопроект за електронния документ и електронния подпис*, както и най-важните приети или разработени международни инструменти, актове на Европейския съюз и чуждестранни закони – в превод на български език или реферирани. Срещащите се терминологични несъвършенства се дължат главно на липсата на утвърдена единна терминология на български език за новите феномени. Има известни разминавания и различия в използваната терминология, възникнали поради обстоятелството, че макар използваните източници да са главно на английски език, част от тях са преводни – от различни езици на държави с различни правни системи и традиции.

Включените материали са актуализирани към март т. г. Посочените Интернет-адреси на всеки отделен акт дават възможност на всички, които проявяват интерес към проблематиката, да следят нейната динамика.

Мария Йорданова,
ръководител на Правната програма на
Центъра за изследване на демокрацията

Законопроект за електронния документ и електронния подпис, България

Закон за електронния документ и електронния подпис

(Проект)

Глава първа
Общи положения

Приложно поле

Чл. 1. (1) Този закон урежда електронния документ, електронния подпис и условията и реда за предоставяне на удостоверителни услуги.

(2) Този закон не се прилага, когато държането на документа или на екземпляр от него има правно значение.

Глава втора
Електронен документ

Електронно изявление

Чл. 2. (1) Електронно изявление е словесно изявление, представено в цифрова форма чрез общоприет стандарт за преобразуване, разчитане и визуално представяне на информацията.

(2) Електронното изявление може да съдържа и несловесна информация.

Електронен документ

Чл. 3. (1) Електронен документ е електронно изявление, записано върху магнитен, оптичен или друг носител, който дава възможност да бъде възпроизвеждано.

(2) Писмената форма се смята спазена, ако е съставен електронен документ.

Автор и титуляр на електронното изявление

Чл. 4. (1) Автор на електронното изявление е физическото лице, което в изявлението се сочи като негов извършител. Титуляр на електронното изявление е лицето, от името на което е извършено електронното изявление.

(2) Лицето, посочено като титуляр или автор на изявлението, не може да оспори авторството спрямо адресата, ако изявлението е отправено чрез съгласувана процедура за идентификация и адресатът е установил авторството чрез нея, когато:

1. изявлението е отправено чрез информационна система, предназначена да работи в автоматичен режим; или
2. изявлението е извършено от лице, на което е предоставен достъп до начина на идентифициране.

(3) Ал. 2, т. 2 не се прилага от момента, в който адресатът получи уведомление, че електронното изявление не изхожда от автора и адресатът има достатъчно време да съобрази поведението си с уведомлението.

(4) Ал. 2 не се прилага, когато адресатът на изявлението не е положил дължимата грижа.

Адресат на електронното изявление

Чл. 5. Адресат на електронното изявление е лице, което по силата на закон е длъжно да получава електронни изявления или за което въз основа на недвусмислени обстоятелства може да се смята, че се е съгласило да получи изявлението в електронна форма.

Посредник при електронното изявление

Чл. 6. (1) Посредник при електронното изявление е лице, което по възлагане изпраща, получава, записва или съхранява електронно изявление или извършва други услуги, свързани с него.

(2) Посредникът при електронното изявление е длъжен:

1. да разполага с техническо и технологично оборудване, което да осигурява надеждност на използваните системи;
2. да поддържа персонал, притежаващ необходимите експертни знания, опит и квалификация;
3. да осигурява условия за точно определяне на времето и източника на предаваните електронни изявления;
4. да използва надеждни системи за съхраняване на информацията по т. 3.

(3) Посредникът при електронното изявление отговаря за вредите от неизпълнение на задълженията му по ал. 2.

Автентификация

Чл. 7. (1) Автентификацията на електронното изявление разкрива самоличността на автора и съгласието му с изявлението.

(2) Автентифицирането се извършва чрез електронен подпис или по друг начин, съгласуван между автора и адресата, който е достатъчно сигурен с оглед нуждите на оборота.

Защита на съдържанието на електронното изявление

Чл. 8. (1) Съдържанието на електронното изявление трябва да бъде защитено от последващи промени.

(2) Защитата се осъществява чрез електронен подпис или по друг начин, съгласуван между автора и адресата, който е достатъчно сигурен с оглед нуждите на оборота.

Грешка при предаване на електронно изявление

Чл. 9. Авторът носи риска от грешки при предаване на електронното изявление, освен ако адресатът не е положил дължимата грижа.

Получаване на електронното изявление

Чл. 10. (1) Електронното изявление се смята получено, ако адресатът потвърди получаването.

(2) Ако не е посочен срок за потвърждаване на получаването, потвърждаването трябва да бъде извършено в разумен срок.

(3) Потвърждаването на получаването не удостоверява съдържанието на електронното изявление.

Време на изпращане на електронното изявление

Чл. 11. Електронното изявление е изпратено с постъпването му в информационна система, която не е под контрола на автора.

Време на получаване на електронното изявление

Чл. 12. (1) Електронното изявление е получено с изпращането на потвърждение за получаването му.

(2) Ако потвърждаване не се изисква, електронното изявление е получено с постъпването му в посочената от адресата информационна система. Ако адресатът не е посочил информационна система, изявлението е получено с постъпването му в информационна система на адресата, а ако адресатът няма информационна система – с изтеглянето му от адресата от информационната система, в която изявлението е постъпило.

Време на узнаване на електронното изявление

Чл. 13. Смята се, че адресатът на електронното изявление е узнал съдържанието му в разумен срок след неговото получаване.

Място на изпращане и получаване на електронното изявление

Чл. 14. (1) Електронното изявление се смята изпратено в мястото на дейност на неговия титуляр.

(2) Електронното изявление се смята получено в мястото на дейност на неговия адресат.

(3) Ако титулярят или адресатът на изявлението има повече от едно място на дейност, за място на дейност се счита това, което е в най-тясна връзка с изявлението и неговото изпълнение, като се държи сметка за обстоятелствата, които са били известни на титуляря и адресата или са били взети предвид от тях по всяко време преди или при извършване на изявлението.

(4) Ако титулярят или адресатът няма място на дейност, взема се предвид неговото постоянно местопребиваване.

Глава трета

Електронен подпис

Раздел I

Общи положения

Определение и действие

Чл. 15. (1) Електронен подпис е преобразувано електронно изявление, включено, добавено или логически свързано със същото електронно изявление преди преобразуването.

(2) Електронният подпис има значението на правно валиден подпис.

(3) Авторът и титулярят на електронния подпис не могат да оспорят авторството на електронното изявление, когато:

1. електронното изявление е преобразувано с частния ключ чрез информационна система, предназначена да работи в автоматичен режим; или
2. електронното изявление е било преобразувано чрез частния ключ от лице, на което е предоставен достъп до частния ключ.

(4) Ал. 3, т. 2 не се прилага от момента, в който адресатът получи уведомление, че електронното изявление не изхожда от автора, и адресатът има достатъчно време да съобрази поведението си с уведомлението.

Преобразуване

Чл. 16. (1) Преобразуването по чл. 15, ал. 1 се извършва чрез използване на алгоритъм, одобрен от Държавната комисия по далекосъобщенията, включващ използването на частния ключ на асиметрична криптосистема.

(2) Асиметричната криптосистема е система, чрез която се създава двойка ключове (частен и публичен), така че:

1. чрез използването на публичния ключ може по несъмнен начин да се установи дали преобразуването на първоначалното електронно изявление е извършено чрез използване на съответния му частен ключ и изменяно ли е електронното изявление след преобразуването;
2. от публичния ключ не може да се открие съответният му частен ключ.

Автор и титуляр на електронния подпис

Чл. 17. Автор и титуляр на електронния подпис са лицата, посочени като такива в удостоверението по чл. 29.

Тайна на частния ключ

Чл. 18. Никой освен автора няма право на достъп до частния ключ и до данните за създаването му.

Раздел II
Регистърна институция

Регулиране и контрол

Чл. 19. (1) Държавната комисия по далекосъобщения регулира и контролира дейността по предоставяне на удостоверителни услуги от удостоверяващите организации по този закон.

(2) Държавната комисия по далекосъобщения регистрира удостоверяващите организации и води регистър на удостоверенията за публичния им ключ.

(3) Държавната комисия по далекосъобщения публикува в регистъра по ал. 2 удостоверението за своя публичен ключ.

Правомощия на Държавната комисия по далекосъобщения

Чл. 20. (1) Държавната комисия по далекосъобщения има следните правомощия:

1. вписва удостоверяващите организации в регистъра и издава удостоверения за публичния им ключ;
2. отказва вписването на удостоверяваща организация, когато тя не отговаря на необходимите изисквания;
3. спира действието или заличава вписването на удостоверяващите организации;
4. осъществява контрол върху регистрираните удостоверяващи организации относно надеждността и сигурността на удостоверителната услуга;
5. одобрява наръчниците за потребителите и предписваните процедури за сигурност;
6. разработва, съгласува и предлага за приемане от Министерския съвет проекти на наредби по този закон, както и относно:
   а) уреждането на дейността на регистрираните удостоверяващи организации и реда за прекратяване на дейността им;
   б) изискванията относно формата на удостоверенията, издавани от удостоверяващите организации;
   в) изискванията за съхраняване на информация за услугите, предоставени от удостоверяващите организации;
   г) изискванията за съдържанието, формата и източниците във връзка с разкриваната информация от удостоверяващите организации;

(2) В изпълнение на своите функции Държавната комисия по далекосъобщения има право:

1. на свободен достъп в подлежащите на контрол обекти;
2. да проверява документите, доказващи квалификацията на служителите в удостоверяващите организации;
3. да изисква сведения и документи, свързани с осъществяване на контрола.

(3) Държавната комисия по далекосъобщения осигурява възможност за установяване на съществуващите удостоверения. Всяко лице може да иска справка за съществуващите удостоверения на определен титуляр. Справката е електронна, съдържа удостоверенията и се подписва с електронния подпис на Държавната комисия по далекосъобщения.

Раздел III
Регистърно производство

Регистрация на удостоверяващи организации

Чл. 21. (1) При подаване на заявление за регистрация като удостоверяваща организация заявителят представя:

1. удостоверение за актуална съдебна регистрация;
2. правилата за издаване на удостоверение, включително правилата за установяване идентичността на титуляря на електронен подпис;
3. процедурите за сигурност, прилагани при издаване и ползване на електронния подпис;
4. условията и реда за използване на електронния подпис, включително изискванията за съхраняване на частния ключ;
5. цената за получаване и използване на удостоверение, както и цените на останалите услуги, предоставяни от удостоверяващата организация;
6. други документи, определени с наредба на Министерския съвет.

(2) Заявлението за регистрация се разглежда в едномесечен срок. Регистрация може да бъде отказана само ако заявителят не е представил необходимите документи, не отговаря на изискванията на чл. 26, ал. 1 или не е внесъл необходимата държавна такса.

(3) Съобщението за отказа трябва да посочва всички основания.

(4) Отказът за регистрация се обжалва по реда на Закона за административното производство.

(5) Заявителят може да отстрани пороците и да подаде ново заявление.

(6) Редът за регистрация се определя с наредба на Министерския съвет.

Заличаване на регистрацията

Чл. 22. Регистрацията се заличава, в случай че:

1. заявителят е представил неверни данни;
2. при груби или системни нарушения на този закон и актовете за прилагането му.

Регистър на удостоверяващите организации

Чл. 23. (1) Регистърът на удостоверяващите организации е публичен. Всеки може да иска справка за регистрираните удостоверяващи организации.

(2) Всеки може да иска справка за условията и реда за регистриране на удостоверяваща организация.

Държавни такси

Чл. 24. (1) За вписване в регистъра, за даването на справки и за издаването на удостоверения се събира държавна такса.

(2) Размерът на държавната такса се определя с тарифа, одобрена от Министерския съвет.

Раздел IV
Удостоверяващи организации

Дейност на удостоверяващата организация

Чл. 25. (1) Удостоверяващата организация е лице, което извършва удостоверителните услуги по ал. 2 след регистрация в Държавната комисия по далекосъобщения.

(2) Удостоверяващата организация:

1. издава удостоверения по чл. 29 и води регистър за тях;
2. предоставя възможност на титулярите на електронни подписи за създаване на частен и публичен ключ;
3. предоставя на всяко трето лице достъп до регистрираните при нея удостоверения;
4. удостоверява датата и часа на представяне на електронен документ, подписан с електронен подпис.

Изисквания към дейността на удостоверяващите организации

Чл. 26. (1) Удостоверяващите организации са длъжни:

1. да поддържат разполагаеми средства, които да им осигуряват възможност да извършват дейност в съответствие с изискванията на този закон;
2. да се застраховат за времето на своята дейност за вредите от неизпълнението на задълженията им по този закон;
3. да прилагат механизъм за създаване на електронния подпис, който гарантира, че:
   а) данните за създаване на частния ключ могат да се възпроизведат само при създаването му и тяхната сигурност е надеждно защитена;
   б) данните за създаване на частния ключ не са достъпни и ключът е защитен срещу подправяне;
   в) данните за създаване на частния ключ могат да бъдат защитени от автора срещу използването им от други лица;
   г) съдържанието на изявлението е достъпно за автора и остава непроменено до преобразуването му с частния ключ.
4. да прилагат механизъм за установяване използването на частния ключ, който да гарантира, че:
   а) данните за установяване използването на частния ключ съответстват на данните, предоставени на лицето, използващо публичния ключ;
   б) използването на частния ключ е надеждно проверено и резултатите от тази проверка са предоставени коректно на лицето, използвало публичния ключ.
5. да разполагат с техническо и технологично оборудване, което да осигурява надеждност на използваните системи и техническа и криптографска сигурност на осъществяваните чрез тях процеси;
6. да поддържат персонал, притежаващ необходимите експертни знания, опит и квалификация за извършване на дейността, по-специално в областта на технологията на електронните подписи, както и добро познаване на процедурите за сигурност;
7. да осигурят условия за точно определяне на времето на издаване, спиране, възобновяване и прекратяване на действието на удостоверенията;
8. да осигурят мерки срещу подправяне на удостоверенията и да осигуряват поверителност на данните, до които имат достъп в процеса на създаване на подписа;
9. да използват надеждни системи за съхраняване на удостоверенията, които да осигуряват:
   а) само надлежно овластени служители да имат достъп за внасяне на промени;
   б) автентичността и верността на информацията, включена в удостоверенията, да може да бъде проверена;
   в) възможност потвърждение за частния ключ да може да се издава само на посочени от титуляря и автора лица;
   г) възникването на технически проблеми във връзка със сигурността да става незабавно достояние на обслужващия персонал;
   д) с изтичане на срока на удостоверението да се прекратява възможността за потвърждаване на частния ключ.
10. да осигурят възможност за незабавно спиране и прекратяване действието на удостоверенията.

(2) Министерският съвет приема наредби по ал. 1, т. 1, 2 и 5.

(3) Удостоверяващата организация не може да използва съхраняваната от нея информация за цели, различни от тези, свързани с нейната дейност. Тя може да предоставя на трети лица само съдържащата се в удостоверенията информация.

Задължения на удостоверяващата организация

Чл. 27. Удостоверяващата организация е длъжна:

1. да издава удостоверение по искане на всяко лице;
2. когато издава удостоверения, да проверява чрез допустимите средства самоличността, съответно идентичността на автора и титуляря на електронния подпис, и, ако е необходимо, други данни за тези лица, включени в удостоверението;
3. по искане на всяко лице да му предостави възможност за създаване на частен и публичен ключ;
4. да публикува издаденото удостоверение, така че трети лица да имат достъп до него съгласно указанията на титуляря;
5. да не съхранява или копира данни за създаване на частните ключове;
6. да информира в достъпна и разбираема форма лицата, желаещи да им бъде издадено удостоверение, за условията за издаване и използване на удостоверението, включително ограниченията на неговото действие, както и за процедурите за подаване на жалби и решаване на спорове;
7. да предприема незабавни действия във връзка със спиране, възобновяване и прекратяване действието на удостоверението при установяване на съответните основания за това;
8. незабавно да уведомява титуляря, както и автора за обстоятелства относно валидността или надеждността на издаденото удостоверение.

Отношения с титуляря

Чл. 28. Отношенията между удостоверяващата организация и титуляря се уреждат с писмен договор.

Раздел V
Удостоверения

Удостоверение

Чл. 29. (1) Удостоверението е електронен документ, издаден и подписан от удостоверяваща организация, който съдържа:

1. фирмата, адреса и БУЛСТАТ на удостоверяващата организация, както и указание за българската ѝ националност;
2. името или фирмата, адреса, единния граждански номер или БУЛСТАТ на титуляря на електронния подпис;
3. основанието на овластяването, името и ЕГН на физическото лице (автор), което е овластено да извършва електронни изявления от името на титуляря на електронния подпис;
4. публичния ключ, който съответства на частния ключ на титуляря на електронния подпис;
5. алгоритмите, с помощта на които се използват публичните ключове на титуляря на електронния подпис и на удостоверяващата организация;
6. датата и часа на издаването, спирането, възобновяването и прекратяването на действието;
7. срока на действие;
8. ограниченията на действието на подписа;
9. уникалния идентификационен код на удостоверението;
10. отговорността и гаранциите на удостоверяващата организация;
11. указание за начина на достъп до удостоверенията за електронните подписи на удостоверяващата организация и на Държавната комисия по далекосъобщенията.

(2) Когато овластяването на автора произтича от други овластени лица, удостоверението трябва да съдържа данните по ал. 1, т. 2 за тези лица.

(3) Публичният ключ има действие от момента на издаване на удостоверението.

(4) Освен ако е уговорено друго, удостоверението има действие за срок от 3 години.

Издаване на удостоверение

Чл. 30. (1) Удостоверяващата организация издава удостоверение по писмено искане на титуляря.

(2) Искането се удовлетворява, ако:

1. изхожда от титуляра или надлежно овластено от него лице;
2. информацията относно титуляра, представена за включване в удостоверението е вярна и пълна; и
3. частният ключ:
   а) се държи от титуляря;
   б) е технически годен да бъде използван за създаване на електронен подпис; и
   в) съответства на публичния ключ, така че чрез публичния ключ може да се удостовери, че определен електронен подпис е създаден с частния ключ.

(3) Ако исканото удостоверение се отнася до електронен подпис с автор, различен от титуляря, искането се удовлетворява, ако са спазени изискванията по ал. 2, като:

1. представената за включване в удостоверението информация относно автора също е вярна и пълна; и
2. частният ключ се държи от автора.

(4) При удовлетворяване на искането удостоверяващата организация изисква от титуляря, съответно от автора, да приеме съдържанието на поисканото удостоверение. Тя променя съдържанието на удостоверението, ако титулярят, съответно авторът, посочи неточности или непълноти.

(5) Удостоверяващата организация издава незабавно удостоверението, чието съдържание е прието съгласно ал. 4, посредством публикуването му.

Спиране и възобновяване на действието на удостоверението

Чл. 31. (1) Освен ако е уговорено друго, удостоверяващата организация има право да спре действието на издадено от нея удостоверение за необходимия според обстоятелствата срок, но не повече от 48 часа, ако съществува основателно съмнение, че действието на удостоверението следва да бъде прекратено.

(2) Освен ако е уговорено друго, удостоверяващата организация е длъжна да спре действието на издадено от нея удостоверение за необходимия според обстоятелствата срок, но не повече от 48 часа:

1. по искане на титуляря, съответно автора, без да е длъжна да се увери в самоличността или представителната му власт;
2. по искане на лице, за което според обстоятелствата е видно, че може да знае за нарушения на сигурността на частния ключ, като представител, съдружник, служител, член на семейството и други.

(3) При непосредствена опасност за интересите на трети лица или при наличие на достатъчно данни за нарушение на закона председателят на Държавната комисия по далекосъобщения може да спре действието на удостоверението за необходимия според обстоятелствата срок, но не повече от 48 часа.

(4) Удостоверяващата организация незабавно уведомява титуляря и автора за спирането действието на удостоверението.

(5) Спирането на действието на удостоверението се извършва чрез внасяне на промяна в съдържанието на удостоверението, така че да не е възможно потвърждение на частния ключ.

(6) Действието на удостоверението се възобновява:

1. с изтичане на срока;

2. от удостоверяващата организация, съответно от Държавната комисия по далекосъобщения, при отпадане на основанието за спиране или по искане на титуляря, след като удостоверяващата организация, съответно Държавната комисия по далекосъобщения, се е уверила, че той е узнал причината за спирането, както и че искането за възобновяване е направено вследствие на узнаването.

Прекратяване на действието на удостоверението

Чл. 32. (1) Действието на удостоверението се прекратява:

1. с изтичането на срока;
2. при прекратяване на удостоверяващата организация без прехвърляне на дейността на друга удостоверяваща организация.

(2) Удостоверяващата организация е длъжна да прекрати действието на удостоверението по искане на титуляря или автора, след като се увери в самоличността и представителната власт на титуляря, съответно автора.

(3) Удостоверяващата организация прекратява действието на удостоверението при:

1. смърт или поставяне под запрещение на титуляря или автора;
2. прекратяване на юридическото лице на титуляря;
3. прекратяване на представителната власт на автора по отношение на титуляря;
4. установяване, че удостоверението е издадено въз основа на неверни данни.

Регистър на удостоверенията

Чл. 33. (1) Удостоверяващата организация води публичен електронен регистър, в който публикува действащите удостоверения.

(2) Удостоверяващата организация публикува в регистъра по ал. 1 и информация за:

1. условията и реда за издаване на удостоверение, включително за правилата за установяване идентичността на титуляря на електронен подпис;
2. процедурите за сигурност на удостоверяващата организация;
3. начина на използване на електронния подпис;
4. условията и реда за използване на електронния подпис, включително изискванията за съхраняване на частния ключ;
5. цената за получаване и използване на удостоверение, както и цените на останалите услуги, предоставяни от удостоверяващата организация;
6. отговорността на удостоверяващата организация и титуляря на електронен подпис;
7. условията и реда, по които титулярят прави искане за прекратяване действието на електронен подпис.

(3) Устройството и дейността на регистъра по ал. 1 се уреждат с наредба на Министерския съвет.

Раздел VI
Отговорност

Отговорност на удостоверяващата организация

Чл. 34. (1) Удостоверяващата организация отговаря пред титуляря на електронния подпис и пред всички трети лица за вредите:

1. от неизпълнението на изискванията по чл. 26 и на задълженията по чл. 27 и 30;
2. от неверни или липсващи данни в удостоверението;
3. които са им причинени, в случай че по време на издаване на удостоверението лицето, посочено като автор, не е разполагало с частния ключ, съответстващ на публичния ключ;
4. от несъответствието между данните за създа-

ване на частния ключ и алгоритмите за използване на публичния ключ.

(2) Недействителни са уговорките, с които се изключва или ограничава отговорността на удостоверяващата организация за небрежност.

(3) Удостоверяващата организация не отговаря за вреди, причинени от използване на удостоверението извън пределите на вписаните в него ограничения на неговото действие.

Отговорност на титуляря и автора към трети лица

Чл. 35. (1) Титулярят отговаря спрямо третите добросъвестни лица, ако авторът**:**

1. не изпълнява точно изискванията за сигурност, определени от удостоверяващата организация;
2. не поиска от удостоверяващата организация прекратяване действието на удостоверението, когато е узнал, че частният ключ е бил използван неправомерно или съществува опасност от неправомерно използване на частния ключ.

(2) Титулярят, който е приел удостоверението при неговото издаване, отговаря спрямо третите добросъвестни лица:

1. ако авторът не е овластен да държи частния ключ, съответстващ на посочения в удостоверението публичен ключ;
2. за неверни изявления, направени пред удостоверяващата организация и имащи отношение към съдържанието на удостоверението.

(3) Авторът, който е приел удостоверението при неговото издаване, отговаря спрямо третите добросъвестни лица, ако не е бил овластен да поиска издаването на удостоверението.

Отговорност на титуляря и автора към удостоверяващата организация

Чл. 36. Титулярят, съответно авторът, отговаря спрямо удостоверяващата организация, ако е приел удостоверението, издадено от удостоверяващата организация въз основа на неверни данни, предоставени от него, съответно въз основа на премълчани от него данни.

Глава четвърта

Приложение на електронния документ и електронния подпис от държавата и общините

Задължение за приемане и издаване на електронни документи

Чл. 37. (1) Министерският съвет определя подчинените си органи, общините и кметствата, които:

1. не могат да откажат приемането на електронни документи, подписани с електронен подпис;
2. не могат да откажат издаването във формата на електронен документ, подписан с електронен подпис, на разрешения, лицензии, одобрения и други административни актове.

(2) Приемането и издаването на електронни документи, подписани с електронен подпис, в съдебната система се урежда със закон.

(3) Приемането и издаването на електронни документи, подписани с електронен подпис, от останалите държавни органи се урежда с техен акт. Редът и формата за извършване и съхраняване на електронните документи се уреждат с вътрешни правила.

Съхраняване на електронни документи

Чл. 38. Държавните и общинските органи са длъжни да съхраняват електронните документи в установените срокове за съхраняване на документи.

Глава пета

Защита на личните данни

Задължение за защита на личните данни

Чл. 39. (1) Защитата на личните данни, събирани от удостоверяващите организации за нуждите на извършваната от тях дейност, и защитата на водените регистри се уреждат със закон.

(2) Режимът по ал. 1 се прилага и по отношение на личните данни, известни на Държавната комисия по далекосъобщенията, която при изпълнение на задълженията си наблюдава дейността на удостоверяващите организации.

(3) Удостоверяващите организации събират лични данни за автора и титуляря на подписа, само доколкото са необходими за издаването и ползването на удостоверение.

(4) Данни за трето лице могат да се събират само с изричното съгласие на лицето, за което се отнасят.

(5) Събраните данни не могат да се използват за цели, различни от посочените в ал. 3, освен с изричното съгласие на лицето, за което се отнасят, или ако това е позволено със закон.

Глава шеста

Признаване на удостоверения, издадени от удостоверяващи организации, установени в други държави

Основания и ред

Чл. 40. (1) Удостоверения, издадени от удостоверяващи организации, регистрирани в други държави съгласно националното законодателство на тези държави, се признават за равностойни на удостоверения, издадени от българска удостоверяваща организация, ако е изпълнено някое от

следните условия:

1. задълженията на удостоверяващата организация, издала удостоверението, и изискванията към нейната дейност съответстват на изискванията, предвидени в този закон, и удостоверяващата организация е призната в държавата по месторегистрацията си; или
2. българска удостоверяваща организация се е задължила да отговаря за действията и бездействията на удостоверяващата организация, регистрирана в друга държава, в случаите по чл. 34;
3. удостоверението или удостоверяващата организация, издала удостоверението, са признати съгласно влязъл в сила международен договор.

(2) Условията по ал. 1, т. 1 и 2 се установяват от Държавната комисия по далекосъобщения по искане на лицето, на което чуждестранната удостоверяваща организация е издала удостоверение, или на трето лице по ред, определен с наредба на Министерския съвет.

(3) Държавната комисия по далекосъобщения осигурява възможност за установяване на чуждестранните удостоверяващи организации, относно които тя е признала съответствие по ал. 1, т. 1. Всяко лице може да иска справка за чуждестранните удостоверяващи организации, относно които е признато съответствие. Справката е електронна, съдържа публичните ключове на чуждестранните удостоверяващи организации и се подписва с електронния подпис на Държавната комисия по далекосъобщения.

Глава седма

Административнонаказателни разпоредби

Чл. 41. (1) Който извърши или допусне извършването на нарушение на този закон и на издадените за неговото прилагане нормативни актове, се наказва с глоба от 100 до 10 000 лв., ако деянието не съставлява престъпление.

(2) В случаите на ал. 1 на юридическото лице или едноличния търговец се налага имуществена санкция в размер от 500 до 50 000 лв.

Чл. 42. (1) Актовете за констатираните нарушения се съставят от лица, оправомощени от председателя на Държавната комисия по далекосъобщения, а наказателните постановления се издават от него или от оправомощено от него длъжностно лице.

(2) При констатиране на нарушенията актосъставителите могат да изземват и задържат веществените доказателства, свързани с установяване на нарушенията по реда на чл. 41 от Закона за административните нарушения и наказания.

(3) Съставянето на актовете, издаването, обжалването и изпълнението на наказателните постановления се извършват по реда на Закона за административните нарушения и наказания.

Преходни и заключителни разпоредби

§ 1. В Гражданския процесуален кодекс (обнародван, Изв., бр. 12 от 8 февруари 1952 г., изм. и доп., бр. 92 от 1952 г., бр. 89 от 1953 г., бр. 90 от 1955 г., бр. 90 от 1956 г., бр. 90 от 1958 г., бр. 50 и 90 от 1961 г., попр., бр. 99 от 1961 г., изм. и доп., ДВ, бр.1 от 1963 г., бр. 23 от 1968 г., бр. 27 от 1973 г., бр. 89 от 1976 г. бр. 36 от 1979 г., бр. 28 от 1983 г., бр. 41 от 1985 г., бр. 27 от 1986 г., бр. 55 от 1987 г., бр. 60 от 1988 г., бр. 31 и 38 от 1989 г., бр. 31 от 1990 г., бр. 62 от 1991 г., изм. и доп., бр. 55 от 1992 г., бр. 61 и 93 от 1993 г., бр. 87 от 1995 г., бр. 12, 26, 37, 44 и 104 от 1996 г., бр. 43 от 1997 г., доп., бр. 55 от 1997 г., бр. 124 от 1997 г., бр. 59 от 1998 г., доп., бр. 70 от 1998 г., бр. 20 от 1999 г., бр. 64 от 1999 г., бр. 65 от 1999 г., бр. 103 от 1999 г.):

1. В чл. 465:

а) се създава нова б. „е“ със следното съдържание:

„е) удостоверяване на електронен подпис;“

б) досегашната б. „е“ става б. „ж“;

2. В чл. 485 се създава нова ал. 3 със следното съдържание:

„При удостоверяване на електронен подпис лицата, чиито подписи подлежат на удостоверяване, трябва да се явят лично пред нотариуса и пред него да извършат електронния подпис. Извършването на електронния подпис се удостоверява с електронния подпис на нотариуса.“

3. Досегашната ал. 3 на чл. 485 става ал. 4.

§ 2. (1) Този закон влиза в сила шест месеца след обнародването му.

(2) Министерският съвет приема наредбите по прилагането на този закон пет месеца след обнародването му.

§ 3. Изпълнението на този закон се възлага на Държавната комисия по далекосъобщенията.

Международни инструменти и актове на Европейския съюз

Закон-модел на УНСИТРАЛ за електронната търговия

(Резюме)

www.un.or.at/uncitral

I. Приложно поле

Законът-модел за електронната търговия е приет от Комисията на ООН по международно търговско право (УНСИТРАЛ) през 1996 г. Той се състои от две части. В първата част са посочени общите правила за електронната търговия, а във втората са включени специални разпоредби за отделни стопански отрасли. Засега във втора част има разпоредби само във връзка с превоза на стоки, но структурата на закона е отворена за включване на нови разпоредби относно други сфери на икономиката.

Законът-модел се прилага за всяка информация, която има връзка с търговската дейност (чл. 1).

II. Определения

В закона-модел са дадени определения на основните понятия (чл. 2): електронно съобщение, електронен обмен на данни, съставител, посредник и адресат на електронно съобщение и информационна система.

- **Електронно съобщение** (data message) – информация, изготвена, изпратена, получена или съхранявана с помощта на електронни, оптически или други подобни средства, включително електронен обмен на данни, електронна поща, телеграма, телекс или телефакс и др.
- **Електронен обмен на данни** (Electronic Data Interchange, EDI) – електронно предаване на информация от един компютър на друг при използване на съгласуван стандарт за структуриране на информацията.
- **Съставител на електронно съобщение** (originator) – всяко лице, което или от името на което електронното съобщение се предполага, че е било изпратено или приготвено за съхранение, с изключение на лицата, действащи в качеството на посредници по отношение на това електронно съобщение.
- **Адресат на електронното съобщение** (addressee) – всяко лице, което съгласно намерението на съставителя е трябвало да получи електронното съобщение, с изключение на лицата, действащи в качеството им на посредници.
- **Посредник по отношение на конкретно електронно съобщение** (intermediary) – всяко лице, което от името на другиго изпраща, получава или съхранява това електронно съобщение или извършва по отношение на него други действия.
- **Информационна система** (information system) – система за подготовка, изпращане, получаване, съхраняване или друга обработка на електронни съобщения.

III. Основни положения

В закона-модел се съдържа специална разпоредба, според която информацията не може да бъде лишена от валидност или правна сила само на основание, че е под формата на електронно съобщение (чл. 5).

Възприет е принципът, че когато законодателството изисква писмена форма, тя се счита спазена и когато информацията е представена под формата на електронно съобщение, ако тя е достъпна за последващо използване (чл. 6).

Когато законодателството изисква наличието на подпис, това изискване се счита спазено и когато той е под формата на електронно съобщение, ако е използван какъвто и да било способ за идентификация на лицето и за установяване съгласието му с информацията, съдържаща се в електронното съобщение, и ако този способ е надежден и съответства на целите, за които е било приготвено или изпратено съобщението, като се отчитат всички обстоятелства, които имат значение в конкретния случай (чл. 7).

В случаите, когато законодателството изисква определена информация да се представи или съхранява в оригинал, се приема, че това изискване е спазено и ако тя е под формата на електронно съобщение, ако има надеждни доказателства за ненакърнеността на информацията към момента, в който тя е била първоначално изготвена в нейната окончателна форма във вид на електронно съобщение или какъвто и да било друг вид, и ако при необходимост от представяне на тази информация, тя може да бъде демонстрирана на лицето, на което е трябвало да бъде представена. Ненакърнеността на информацията се преценява, без

да се отчитат промените, които настъпват обикновено в процеса на нейното предаване, съхранение и демонстриране. Надеждността се оценява с оглед на целите, за които информацията е била изготвена, и на други обстоятелства, които имат значение за конкретния случай (чл. 8).

IV. Доказателствена сила

На информацията, представена под формата на електронно съобщение, се признава съответна доказателствена сила. Не се допуска неприемане на електронните съобщения за доказателства само на основание, че са електронни съобщения, както и че не са под формата на оригинал. При оценката на доказателствената сила на електронните съобщения се обръща внимание на надеждността на способа, с помощта на който електронното съобщение е било приготвено, съхранявано или предадено, надеждността на способа, с помощта на който се обезпечава ненакърнеността на информацията, способа, с помощта на който се идентифицира съставителят, и други обстоятелства, имащи значение в конкретния случай (чл. 9).

Когато законодателството изисква съхраняването на определени документи, записи или друга информация, това изискване се смята изпълнено и под формата на електронно съобщение при няколко условия. Информацията, която се съдържа в електронното съобщение, трябва да е достъпна за последващо използване. Електронното съобщение трябва да се съхранява във формата, в която е било подготвено, изпратено или получено, или във формат, в който може да бъде показано, че подготвената, изпратената или получената информация е представена точно. Трябва също така да се съхранява и информацията, ако такава съществува, която позволява да се установи произходът и предназначението на електронното съобщение, както и датата и времето на неговото изпращане и получаване (чл. 10).

V. Сключване на договор по електронен път. Отправяне и получаване на предложението

При сключване на договор ако страните не са уговорили друго, предложението и неговото приемане могат да бъдат под формата на електронни съобщения. В тези случаи договорът не може да бъде лишен от действителност или доказателствена сила само на основание използването на електронни съобщения (чл. 11). Това важи и за волеизявленията и другите изявления на съставителя и адресата под формата на електронни съобщения (чл. 12).

Електронното съобщение се счита изходящо от съставителя, ако е било отправено от самия него. В отношенията между съставителя и адресата то се счита за изходящо от съставителя, ако е било изпратено от лице, упълномощено да действа от името на съставителя по отношение на електронното съобщение, или от информационна система, програмирана от съставителя или от негово име да функционира на автоматичен режим. В отношенията между съставителя и адресата адресатът има право да счита, че електронното съобщение изхожда от съставителя, и да извършва действия в съответствие с това предположение, ако за да установи, че електронното съобщение изхожда от съставителя, адресатът надлежно е приложил предварително съгласувана за целта процедура, както и ако полученото от адресата електронно съобщение е резултат от действията на лице, чиито отношения със съставителя му дават възможност да получи достъп до способа, използван от съставителя за идентифициране на електронните съобщения като свои. Последната разпоредба не се прилага, ако към момента на получаването адресатът е бил уведомен от съставителя, че електронното съобщение не изхожда от него, при условие, че адресатът е имал достатъчно време да извърши надлежните действия, както и когато адресатът е знаел или е могъл да научи, ако беше положил дължимата грижа или приложил съгласуваната процедура, че електронното съобщение не изхожда от съставителя.

Във всички случаи, когато адресатът има право да счита електронното съобщение за изходящо от съставителя и да действа съгласно това предположение, той има право да счита и че съдържанието на това електронно съобщение е такова, каквото е било намерението на съставителя, освен ако е знаел или е могъл да знае, ако беше положил дължимата грижа или приложил съгласуваната процедура, че е допусната грешка.

Адресатът има право да счита всяко електронно съобщение за самостоятелно, освен ако е налице дублиране или ако е знаел или е могъл да знае, че е налице дублиране, ако беше положил дължимата грижа или приложил съгласуваната процедура (чл. 13).

VI. Потвърждаване. Изпращане и получаване на потвърждението

Съставителят и адресатът могат да уговорят потвърждение. Ако не е уговорена форма или способ за извършване на потвърждението, то може да бъде всякакво съобщение от страна на адресата, направено по електронен или друг път, както и всяко действие на адресата, достатъчни за установяване, че електронното съобщение е получено. Ако електронното съобщение е обусловено от

потвърждение, то не се счита получено, докато не се получи потвърждението. Ако електронното съобщение не е било обусловено от потвърждение и потвърждение не е получено в уговорения срок или срок въобще не е уговорен, съставителят може да уведоми адресата, че не е получил потвърждение и да му даде разумен срок да изпрати такова. Ако в този срок не се получи потвърждение, адресатът може, след като уведоми съставителя, да счита електронното съобщение за неполучено (чл. 14).

Ако съставителят и адресатът не са уговорили друго, за момент на изпращането се счита моментът, в който електронното съобщение постъпи в информационна система извън контрола на съставителя или на лицето, изпратило съобщението от негово име. Определянето на момента на получаването е по-сложно. Ако съставителят и адресатът не са уговорили друго, но адресатът е посочил информационна система за получаване на такива съобщения, съобщението се счита получено, когато постъпи в посочената система, а ако е било изпратено в друга система на адресата, различна от посочената – това е моментът, когато адресатът го изтегли от там. Ако адресатът не е посочил информационна система, съобщението се счита получено в момента, когато постъпи в която и да е информационна система на адресата. Ако съставителят и адресатът не са уговорили друго, електронното съобщение се счита изпратено от местонахождението на търговското предприятие на съставителя и получено в местонахождението на търговското предприятие на адресата. Ако съставителят или адресатът имат повече от едно търговско предприятие, за място на изпращането съответно получаването на електронното съобщение се счита това, което се намира в най-тясна връзка с основната сделка, а ако няма основна сделка – това по местонахождението на основното търговско предприятие. Ако съставителят или адресатът нямат търговско предприятие, за такова се смята обичайното им местожителство (чл. 15).

Директива 1999/93/ЕС на Европейския парламент и на Съвета на Европейския съюз от 13 декември 1999 г. относно правната рамка на общността за цифрови подписи

www.ipso.cec.be/ecommerce/welcome.html

ЕВРОПЕЙСКИЯТ ПАРЛАМЕНТ И СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

Като взеха предвид Договора за създаване на Европейската общност и в частност чл. 47, ал. 2, чл. 55 и 95 от него,

Като взеха предвид предложението на Комисията[1],

Като взеха предвид мнението на Икономическия и социален комитет[2],

Като взеха предвид мнението на Комитета на регионите[3],

Действайки в съответствие с процедурата, установена в чл. 251 от договора[4],

Като се има предвид:

(1) На 16 април 1997 г. Комисията представи на Европейския парламент, Съвета на Европейския съюз, Икономическия и социален комитет и Комитета на регионите Комюнике върху „Европейската инициатива за електронна търговия“;

(2) На 8 октомври 1997 г. Комисията представи на Европейския парламент, Съвета на Европейския съюз, Икономическия и социален комитет и Комитета на регионите Комюнике относно „Осигуряване на сигурност и доверие при електронните комуникации – за създаването на европейска правна уредба на цифровите подписи и криптиране“;

(3) На 1 декември 1997 г. Съветът на Европейския съюз покани Комисията да внесе предложение за Директива на Европейския парламент и Съвета на ЕС за цифровите подписи колкото е възможно по-скоро;

(4) Електронната комуникация и търговия правят необходими „електронните подписи“ и свързаните с тях услуги, позволяващи автентификация на данните; различните норми относно правното признаване на електронните подписи в държавите членки могат да създадат значителни препятствия при използването на електронната комуникация и електронната търговия; от друга страна, ясната правна рамка на общността относно условията, приложими към електронните подписи, ще засили доверието в новите технологии и общото им приемане; законодателството на държавите членки не трябва да възпрепятства свободното движение на стоки и услуги във вътрешния пазар;

(5) Съвместимостта на продуктите на електронните подписи следва да се промоцира; съгласно чл. 14 от договора вътрешният пазар включва пространство без вътрешни граници, в което е осигурено свободното движение на стоки; следва да бъдат постигнати съществени изисквания, специфични за продуктите на електронните подписи, за да се осигури свободното движение във вътрешния пазар и да се изгради доверие в електронните подписи, без да се накърняват разпоредбите на Регламента на Съвета на Европейския съюз № 3381/94 от 19 декември 1994 г., установяващ режима на общността за контрола върху износа на стоки с двойствена употреба[5] и Решението на Съвета на Европейския съюз 94/942/CFSP от 19 декември 1994 г. за съвместните действия, приети от Съвета на Европейския съюз относно контрола върху износа на стоки с двойствена употреба[6];

(6) Тази директива не хармонизира услугите относно конфиденциалността на информацията, когато те са регламентирани в националните разпоредби за обществен ред и обществена сигурност;

(7) Вътрешният пазар осигурява свободно движение на хора, в резултат на което гражданите и пребиваващите в Европейския съюз имат нарастваща необходимост да се обръщат към властите в държавите членки, различни от тази, в която живеят; наличието

[1] OJ C 325, 23.X.1998, p. 5.

[2] OJ C 40, 15.II.1999, p. 29.

[3] OJ C 93, 6.IV.1999, p. 33.

[4] Мнение на Европейския парламент от 13 януари 1999 г. (OJ C 104, 14.IV.1999, p. 49), Обща позиция на Съвета на Европейския съюз от 28 юни 1999 г. (OJ C 243, 27.VIII.1999 г., p. 33) и Решение на Европейския парламент от 27 октомври 1999 г. (все още не е публикувано в „Официален вестник на Европейските общности“).

[5] OJ L 367, 31.XII.1994, p. 1 Регламент, изменен от Регламент 837/95/EC (OJ L 90, 21.IV.1995, p. 1).

[6] OJ L 367, 31.XII.1994, p. 8. Решение, изменено с Решение 99/193/CFSP (OJ L 73, 19.III.1999, p. 1).

на електронна комуникация ще бъде от голяма полза в тази връзка;

(8) Бързото технологично развитие и глобалният характер на Интернет правят необходим такъв подход, който е отворен към различни технологии и услуги, способни да автентифицират данни по електронен път;

(9) Електронните подписи ще се използват при различни условия и приложения, произтичащи от широкия кръг нови услуги и продукти, свързани с използването на електронните подписи; определянето на тези продукти и услуги не трябва да се ограничава до издаването и управлението на удостоверения, а трябва да включва също така и други услуги и продукти, използващи или допълващи електронните подписи, като регистрационни услуги, услуги, предоставящи удостоверяване на време, справочни услуги, компютърни услуги или консултантски услуги, свързани с електронните подписи;

(10) Вътрешният пазар позволява на доставчиците на удостоверителни услуги да развиват трансгранична дейност с оглед увеличаване на конкурентоспособността им и по този начин да предлагат на потребителите и бизнеса нови възможности за сигурен обмен на информация и електронно търгуване без оглед на границите; за да се стимулира предлагането на удостоверителните услуги в откритите мрежи, доставчиците на удостоверителни услуги в общността следва да бъдат свободни да предоставят услугите си, без да им е необходима предварителна оторизация; предварителната оторизация означава не само разрешението, съгласно което доставчикът на удостоверителни услуги следва да получи решение от националните органи, преди да му бъде позволено да предоставя удостоверителни услуги, но също така и всички други мерки, които имат подобен ефект;

(11) Схемите за доброволна акредитация за предоставяне на по-високо ниво на услуги могат да предложат на доставчиците на удостоверителни услуги подходящата рамка за по-напреднало развитие на услугите им към степен на доверие, сигурност и качество, необходими на развиващия се пазар; такива схеми следва да насърчат развитието на най-добра практика сред доставчиците на удостоверителни услуги; доставчиците на удостоверителни услуги следва да бъдат свободни да прилагат и се ползват от такива схеми за акредитация;

(12) Удостоверителните услуги могат да се предлагат от публична организация или от юридическо или физическо лице, когато то е установено в съответствие с националното законодателство; държавите членки не трябва да забраняват на доставчиците на удостоверителни услуги да действат извън схемите за доброволна акредитация; трябва да се осигури схемите за акредитация да не ограничават конкуренцията при удостоверителните услуги;

(13) Държавите членки могат да определят как да се осигури контролът за съответствие с разпоредбите на тази директива; тази директива не предотвратява установяването на частно базирани контролни системи; тя не задължава доставчиците на удостоверителни услуги да бъдат контролирани съгласно която и да е приложима схема за акредитация;

(14) Важно е да бъде намерен баланс между потребителите и нуждите на бизнеса;

(15) Приложение III регламентира изискванията за сигурен механизъм за създаване на подписа, който осигурява функционирането на усъвършенствания електронен подпис; приложението не включва цялата системна среда, в която такива механизми действат; функционирането на вътрешния пазар изисква Комисията и държавите членки да действат бързо, за да позволят на органите, които са натоварени с преценката за съответствие на сигурните механизми за подписа съгласно приложение III, да бъдат назначени; за да съответства на потребностите на пазара, преценката за съответствие трябва да бъде навременна и ефикасна;

(16) Тази директива допринася за използването и правното признаване на електронните подписи в общността; правна рамка не е необходима за електронни подписи, използвани предимно в системи, основаващи се на доброволни споразумения съгласно частното право между определен кръг от участници; свободата на страните да договарят помежду си условия, съгласно които те приемат електронно подписаните данни, ще се зачита, доколкото това е позволено в националното законодателство; правната сила на електронните подписи, използвани в такива системи, и тяхната допустимост като доказателство в съдебния процес трябва да се признава;

(17) Тази директива не цели да хармонизира националните норми на договорното право и по-специално сключването и изпълнението на договорите или други формални изисквания от извъндоговорен характер относно подписите; поради тази причина разпоредбите относно правната сила на електронните подписи следва да не накърняват изиск-

ванията към формата, възприети в националното законодателство, относно сключването на договора и правилата, определящи дали договорът е бил сключен;

(18) Съхраняването и копирането на данни за създаване на подписа могат да застрашат правната валидност на електронните подписи;

(19) Електронните подписи ще се използват в публичния сектор на националните администрации и администрацията на общността и при комуникацията между тези администрации и между тях и гражданите и икономическите субекти, например при държавните поръчки, данъчното облагане, социалното осигуряване, здравната и съдебната система;

(20) Хармонизираните критерии относно правната сила на електронните подписи ще запазят ясната правна рамка в общността; националните законодателства възприемат различни изисквания към правната валидност на саморъчните подписи; удостоверенията могат да бъдат използвани за потвърждаване самоличността на лицето, което се подписва електронно; усъвършенстваните електронни подписи, които се основават на квалифицирани удостоверения и които са създадени чрез сигурен механизъм за създаване на подписа, могат да се смятат за правно еквивалентни на саморъчните подписи, само при условие че изискванията за саморъчните подписи са спазени;

(21) С цел да се стимулира общото приемане на методите на електронна автентификация, трябва да се гарантира, че електронните подписи могат да бъдат използвани като доказателство в съдебния процес във всички държави членки; правното признаване на електронните подписи следва да се основава на обективни критерии и да не се свързва с оторизирането на доставчика на удостоверителни услуги; националното законодателство следва да регламентира правните аспекти, при които електронните документи и електронните подписи могат да се използват; тази директива не накърнява правото на националните съдилища да се произнасят относно съответствието с изискванията в директивата и не оказва въздействие върху националните норми относно свободната съдебна преценка на доказателствата;

(22) Доставчиците на удостоверителни услуги, предоставящи удостоверителни услуги на обществеността, подлежат на отговорност съгласно националните правила.

(23) Развитието на международната електронна комуникация изисква трансгранични споразумения, включващи трети държави; за да се осигури съвместимост на глобално ниво, споразуменията за многостранни правила с трети държави относно взаимното признаване на удостоверителни услуги могат да бъдат от полза;

(24) За да се увеличи доверието на потребителя в електронната комуникация и електронната търговия, доставчиците на удостоверителни услуги следва да спазват законодателството относно защитата на личните данни и личната неприкосновеност;

(25) Разпоредбите за използване на псевдоним в удостоверенията не следва да ограничават държавите членки да изискват идентификация на лицата съгласно правото на общността и националното право;

(26) Мерките, необходими за възприемането на тази директива, следва да бъдат приети съгласно Решение на Съвета на Европейския съюз 1999/486/ЕС от 28 юни 1999 г., определящо процедурите за упражняване на властта по приложението, предоставена на Комисията[7];

(27) Две години след въвеждането на директивата, Комисията ще направи преглед на директивата по такъв начин, *inter alia*, че да се установи дали напредналите технологии и промените в правната среда не са създали пречки за постигане на целите, залегнали в нея; следва да провери приложението на близки технически области и да предостави доклад на Европейския парламент и Съвета на Европейския съюз по този въпрос;

(28) В съответствие с принципите на субсидиарност и пропорционалност, както са посочени в чл. 5 от договора, целта за създаване на хармонизирана правна уредба за предоставяне на електронни подписи и свързани с тях услуги не може да бъде напълно постигната от държавите членки и може следователно да бъде по-добре постигната от общността; тази директива не отива извън необходимото за постигане на тази цел,

ПРИЕХА ТАЗИ ДИРЕКТИВА:

Член 1

Обхват

Целта на директивата е да улесни използването на електронните подписи и да подпомогне тяхното правно признаване. Директивата установява правната рамка на електронните подписи и на някои удостоверителни услуги, с цел да осигури правилното функциониране на вътрешния пазар.

Директивата не регламентира сключването и действителността на договорите или други правни задължения относно формата, предвидени в

[7] OJ L 184, 17.VII.1999, p. 23.

националното или европейското право, нито засяга нормите и ограниченията съгласно националното право или правото на общността относно използването на документи.

Член 2

Определения

За целите на настоящата директива:

(1) **„Електронен подпис“** (electronic signature) – информация в електронна форма, придружена или логически свързана с друга електронна информация и служеща като средство за автентификация;

(2) **„Усъвършенстван електронен подпис“** (advanced electronic signature) – електронен подпис, който отговаря на следните изисквания:
   1. свързан е по уникален начин с подписващото лице;
   2. способен е да идентифицира подписващото лице;
   3. създаден е със средства, които подписващото лице държи единствено под свой контрол; и
   4. е свързан с информацията по такъв начин, че всяка последваща промяна в нея може да бъде открита;

(3) **„Подписващо лице“** (signatory) – лице, притежаващо механизъм за създаване на подпис и действащо от свое име или от името на физическо или юридическо лице, което представлява;

(4) **„Данни за създаване на подписа“** (signature-creation data) – уникална информация като кодове или криптографски ключове, използвани от подписващото лице за създаване на електронен подпис;

(5) **„Механизъм за създаване на подписа“** (signature-creation device) – конфигуриран софтуер или хардуер, използван за въвеждане на данните за създаване на подписа;

(6) **„Защитен механизъм за създаване на подписа“** (secure-signature-creation device) – механизъм за създаване на подпис, който отговаря на изискванията на приложение III от директивата;

(7) **„Данни за проверка на подписа“** (signature-verification-data) – данни като кодове и публични криптографски ключове, използвани за проверка на електронния подпис;

(8) **„Механизъм за проверка на подписа** (signature-verification device) – конфигуриран софтуер или хардуер, използван за прилагане на данните за проверка на подписа;

(9) **Удостоверение“** (certificate) – електронна атестация, свързваща механизма за проверка на подписа с лицето и удостоверяваща идентичността на лицето;

(10) **„Квалифицирано удостоверение“** (qualified certificate) – удостоверение, отговарящо на изискванията, залегнали в приложение I и предоставено от доставчика на удостоверителни услуги, който отговаря на изискванията, залегнали в приложение II;

(11) **„Доставчик на удостоверителни услуги“** (certification-service-provider) – физическо или юридическо лице, което издава удостоверения или предлага други услуги, свързани с електронните подписи;

(12) **„Продукт на електронния подпис“** (electronic-signature-product) – хардуер или софтуер или други компоненти, предназначени да се използват от доставчиците на удостоверителни услуги за извършване на услуги с електронен подпис или предназначени да се използват за създаване или проверка на електронни подписи;

(13) **„Доброволна акредитация“** (voluntary accreditation) – разрешение, съдържащо права и задължения, специфични за извършването на удостоверителни услуги, което се издава по молба на заинтересования доставчик на удостоверителни услуги от публична или частна организация, на която е предоставен контрол за спазването на тези права и задължения, където доставчикът на удостоверителни услуги не е упълномощен да упражнява правата, произтичащи от разрешението, докато не го е получил от организацията.

Член 3

Достъп до пазара

1. Държавите членки следва да не поставят като условие за предоставянето на удостоверителни услуги предварителна оторизация.
2. Без да накърняват разпоредбите на ал. 1, държавите членки могат да въведат или поддържат доброволни схеми за акредитация, целящи по-високо ниво на предоставяне на удостоверителни услуги. Всички условия, свързани с такива схеми, следва да бъдат обективни, прозрачни, равнопоставени и недискримиращи. Държавите членки не могат да ограничават броя на лицата, предоставящи удостоверителни услуги, по причини, които попадат в обсега на тази директива.
3. Всяка държава следва да осигури функционирането на надеждна система, която да позволява наблюдение и контрол на доставчиците на удостоверителни услуги, установени на територията ѝ и издаващи квалифицирани удостоверения.
4. Съответствие на защитните механизми за създаване на подписа с изискванията, залегнали в приложение III на директивата се следят от съ-

ответните публични или частни организации, създадени в държавите членки. Комисията съгласно процедурата, залегнала в чл. 9, следва да определи критериите за това дали дадена организация ще може да прави такава оценка или не.

Прегледът на съответствието с изискванията, залегнали в приложение III, от организациите по ал. 1 ще се признава от всички държави членки.

5. Комисията може съгласно процедурата по чл. 9, да установи и публикува справочни/реферативни номера на общопризнати стандарти за продуктите на електронните подписи в „Официален вестник на Европейските общности". Държавите членки приемат, че има съответствие с изискванията на приложение II, буква „е", и приложение III, когато продуктът на електронния подпис отговаря на тези стандарти.
6. Държавите членки и Комисията ще работят заедно, за да поощрят развитието и използването на механизмите за доказване на подписа от гледна точка на препоръките за сигурно доказване на подписа, залегнали в приложение IV, и в интерес на потребителя.
7. Държавите членки могат да предвидят в законодателството си допълнителни изисквания относно използването на електронни подписи в публичния сектор. Такива изисквания следва да бъдат обективни, прозрачни, равнопоставени и недискриминиращи и да се отнасят само до специфичните характеристики на конкретното приложение. Тези изисквания не следва да представляват пречка за трансграничните услуги за гражданите.

Член 4

Принципи на вътрешния пазар

1. Държавите членки следва да прилагат разпоредбите на националното си законодателство, приети съгласно тази директива, относно доставчиците на удостоверителни услуги, установени на територията им, и относно услугите, които те предоставят. Държавите членки не могат да ограничават предоставянето на удостоверителни услуги, произтичащи от друга държава членка и попадащи в обсега на тази директива.
2. Държавите членки следва да предвидят продуктите на електронните подписи, които съответстват на изискванията, предвидени в тази директива, да се разпространяват свободно в рамките на вътрешния пазар.

Член 5

Правна сила на електронните подписи

1. Държавите членки следва да осигурят усъвършенствания електронен подпис, основан на квалифицирано удостоверение и създаден със защитен механизъм за създаване на подписа да:
   а) удовлетворява правните изисквания към подписа по отношение на електронните данни по същия начин, както и саморъчният подпис удовлетворява тези изисквания по отношение на данните на хартиен носител; и
   б) признаят подписа като доказателство в процеса.
2. Държавите членки следва да предвидят да не се отказва правно действие на електронния подпис и допустимост като доказателство в съдебен процес само на основание, че:
   - подписът е в електронна форма;
   - е основан на квалифицирано удостоверение;
   - не е основан на квалифицирано удостоверение, издадено от упълномощен доставчик на удостоверителни услуги; или
   - не е създаден чрез защитен механизъм за създаване на подписа.

Член 6

Отговорност

1. Като минимум държавите членки следва да предвидят/осигурят, че с издаването на удостоверението като квалифицирано удостоверение или гарантирайки такова удостоверение за обществеността, доставчикът на удостоверителни услуги носи отговорност за вреди, причинени на физически или юридически лица, които са разчитали на надеждността на това удостоверение:
   а) относно точността на информацията по време на издаване на квалифицираното удостоверение и относно факта дали удостоверението съдържа всички подробности, предвидени за квалифицираното удостоверение;
   б) да гарантира по време на издаване на удостоверението, че подписващото лице идентифицирано в удостоверението, е държало данни за създаване на подписа, които съответстват на данните за проверка на подписа, дадени или идентифицирани в удостоверението;
   в) да гарантира, че данните за създаване на подписа и данните за проверка на подписа могат да се използват като съвпадащи в случаите, когато доставчиците на удостоверителни услуги създават и двата вида данни; освен ако доставчикът на удостоверителни услуги не докаже, че не е проявил небрежност.
2. Като минимум държавите членки следва да предвидят, че доставчикът на удостоверителни услуги, издал квалифицирано удостоверение, е отговорен за вреди, причинени на физически или юридически лица, които са разчитали на удостоверението, за пропуски да се регистрира отмяната на удостоверението, освен ако дос-

тавчикът на удостоверителни услуги не докаже, че не е проявил небрежност.

3. Държавите членки следва да предвидят възможност доставчиците на удостоверителни услуги да въвеждат ограничения в използването на квалифицираните удостоверения, ако тези ограничения са признати от трети страни. Доставчиците на удостоверителни услуги не носят отговорност за вреди, причинени от използването на квалифицирано удостоверение при превишаване на ограниченията, наложени в него.
4. Държавите членки следва да осигурят възможност на доставчиците на удостоверителни услуги да предвидят при квалифицираните удостоверения лимит в размера на трансакцията, за която удостоверението може да бъде използвано, при условие че лимитът се признава от трети страни.

Доставчикът на удостоверителни услуги не носи отговорност за вреди, причинени при превишаване на този лимит.

5. Разпоредбите на ал. 1 – 4 не могат да накърняват разпоредбите на Директива на Съвета на Европейския съюз 93/13/ЕЕС от 5 април 1993 г. относно несправедливите условия в потребителските договори.

Член 7

Международни аспекти

1. Държавите членки следва да предвидят квалифицираните удостоверения, издадени от доставчици на удостоверителни услуги, регистрирани в трети държави, да им се признава еднаква правна сила с удостоверенията, издадени от доставчици, регистрирани в общността, при условие че:
   а) доставчикът на удостоверителни услуги отговаря на изискванията, залегнали в тази директива, и е бил упълномощен съгласно доброволна схема за акредитация, създадена в някоя от държавите членки; или
   б) доставчикът на удостоверителни услуги, който е установен в общността и отговаря на изискванията, залегнали в директивата, гарантира удостоверението; или
   в) удостоверението или доставчикът на удостоверителни услуги са признати по силата на двустранно или многостранно споразумение между общността и трети държави или международни организации.
2. За да се улесни трансграничното предоставяне на удостоверителни услуги с трети държави и правното признаване на усъвършенствани електронни подписи, произхождащи от трети държави, Комисията ще прави предложения там, където е необходимо, за постигане на ефективно прилагане на стандартите и международните споразумения с трети страни и международни организации. Съветът на Европейския съюз ще взема решения с квалифицирано мнозинство.
3. Когато Комисията е уведомена за трудности, които предприятията изпитват от гледна точка на достъпа до пазара на трети държави, тя може, ако е необходимо, да представи предложения до Съвета на Европейския съюз за придобиване на мандат за преговори за съответстващи права за предприятията на общността в тези трети държави. Съветът на Европейския съюз взема решения с квалифицирано мнозинство.

Мерките, предприети в тази връзка, не накърняват задълженията на общността и на държавите членки, произтичащи от международни споразумения.

Член 8

Защита на данните

1. Държавите членки следва да предвидят доставчиците на удостоверителни услуги и националните организации по акредитация и контрол да спазват изискванията, залегнали в Директива 95/46 на Европейския парламент и Съвета на Европейския съюз от 24 октомври 1995 г. за защита на индивидите при предаване на личните данни и свободното движение на такива данни.
2. Държавите членки следва да предвидят/осигурят, че доставчиците на удостоверителни услуги, които издават удостоверения за обществеността, могат да събират лични данни само пряко от субекта на данните или след неговото изрично съгласие и само доколкото е необходимо за целите по издаването и поддръжката на удостоверението. Данните не могат да се събират или обработват за никакви други цели, без да има изрично съгласие от страна на субекта на данните.
3. Без да се накърнява правният ефект, предоставен на псевдонима в националното законодателство, държавите членки не могат да забраняват доставчиците на удостоверителни услуги да използват в удостоверението псевдоним, вместо името на подписващия.

Член 9

Комитет

1. Комисията ще бъде подпомагана от „Комитет по електронния подпис“, наричан по-долу „Комитета“.
2. Когато се прави препращане към тази алинея, чл. 4 и 7 на Решение 1999/468/ЕС ще се прилагат, като се взема предвид чл. 8 от решението. Периодът, залегнал в чл. 4, ал. 3 от Решение 1999/468/ЕС, е три месеца.

3. Комитетът приема процедурни правила за своята работа.

Член 10

Задачи на Комитета

Комитетът разяснява изискванията, заложени в директивата и приложенията към нея, критериите, определени в чл. 3, ал. 4 и общопризнатите стандарти за продуктите на електронния подпис, установени и публикувани съгласно чл. 3, ал. 5 и в съответствие с процедурата на чл. 9, ал. 2.

Член 11

Уведомление

1. Държавите членки следва да уведомяват Комисията и другите държави членки за следното:
   а) информация относно националните доброволни схеми за акредитация, включително и всички други задължения по чл. 3, ал. 7;
   б) имената и адресите на националните организации, отговорни за акредитацията и контрола, както и организациите по чл. 3, ал. 4;
   в) имената и адресите на всички акредитирани национални доставчици на удостоверителни услуги.
2. За всяка информация, предоставена съгласно ал. 1 и промените, настъпили в нея, следва в най-кратък срок да се уведомяват Комисията и държавите членки.

Член 12

Преглед

1. Комисията следва да прегледа приложенията на тази директива и да докладва за резултатите от прегледа на Европейския парламент и на Съвета на Европейския съюз най-късно до 19 юли 2003 г.
2. Прегледът *inter alia* следва да оцени дали обсегът на директивата трябва да се промени, като се отчете технологичното, пазарното и правното развитие. Докладът по-конкретно следва да включва оценка, направена на базата на придобития опит, на аспектите на хармонизация. Докладът следва да бъде придружен, там, където е необходимо, от предложения за промени.

Член 13

Прилагане

1. Държавите членки следва да приемат закони, подзаконови актове и административни правила по приложение на тази директива най-късно до 19 юли 2001 г. Те следва да уведомят надлежно Комисията за това.

Когато държавите членки приемат в законодателството си тези мерки, те следва да съдържат препращане към тази директива или да бъдат придружени от такова препращане при официалното им обнародване. Начините за препращане се определят от държавите членки.

2. Държавите членки уведомяват Комисията относно текстовете на основните разпоредби, предвидени в националното им законодателство по приложение на тази директива.

Член 14

Влизане в сила

Директивата влиза в сила в деня на публикуването ѝ в „Официален вестник на Европейските общности“.

Член 15

Адресати

Тази директивата е адресирана към държавите членки.

Брюксел, 13 декември 1999 г.

За Европейския парламент
Президент: *Н. Фонтайн*

За Съвета на Европейския съюз
Председател: *С. Фаси*

Приложение I

Изисквания към квалифицираните удостоверения

Квалифицираните удостоверения следва да съдържат:

а) означение, че удостоверението е било издадено като квалифицирано удостоверение;

б) идентифициране на доставчика на удостоверителни услуги и държавата, в която е регистриран;

в) името на подписващото лице или псевдонима му, означен като такъв;

г) специфични особености на подписващото лице в случай на необходимост от гледна точка на целта, за която е създадено удостоверението;

д) данни за проверка на подписа, които съответстват на данните за създаване на подписа, намиращи се под контрола на подписващото лице;

е) означение на началото и края на срока на валидност на удостоверението;

ж) идентификационен код на удостоверението;

з) усъвършенствания електронен подпис на доставчика на удостоверителни услуги, който го е издал;

и) ограничения на обхвата на удостоверението, ако се предвиждат;

к) ограничения в цената на трансакциите, при които удостоверението може да се използва, ако се предвиждат.

Приложение II

Изисквания към доставчиците на удостоверителни услуги, издаващи квалифицирани удостоверения

Доставчиците на удостоверителни услуги са длъжни:

а) да демонстрират надеждност, необходима за предлагането на удостоверителни услуги;

б) да осигурят действието на точна и сигурна директория и сигурни и незабавни услуги във връзка с отменянето;

в) да осигурят възможност за точно определяне на времето и мястото на издаване и отмяна на удостоверението;

г) да проверяват чрез средствата, предоставени в националните им законодателства, самоличността и, ако е необходимо, специфичните особености на подписващото лице, на което е било издадено квалифицирано удостоверение;

д) да наберат персонал, притежаващ необходимите експертни знания, опит и квалификация, необходими за предоставяне на услугите, и по-специално компетентност на управленско ниво, експертни знания в областта на технологията на електронните подписи и добро познаване на процедурите за сигурност; да прилагат административни и управленски услуги, които са адекватни и съответстват на признатите стандарти;

е) да използват надеждни системи, които са защитени от изменения и осигуряват техническа и криптографска сигурност на процесите, поддържани чрез тях;

ж) да вземат мерки срещу подправяне на удостоверенията и в случаите, когато доставчикът на удостоверителни услуги събира данни за създаване на подписа и гарантира конфиденциалност по време на събирането на тези данни;

з) да поддържат достатъчно финансови средства, за да работят в съответствие с изискванията, залегнали в директивата, и по-специално да носят риска от отговорност за вреди, като например се сдобият със съответна застраховка;

и) да вписват цялата съответна информация относно квалифицираното удостоверение за определен период от време, и по-конкретно с цел да се предоставя като доказателство за удостоверяване при правен спор. Такива вписвания могат да се извършват по електронен път.

к) да не съхраняват или копират данни за създаване подписа на лицето, на което доставчикът на удостоверителни услуги е предоставял управленските услуги във връзка с ключа;

л) преди да влизат в договорни отношения с лицето, искащо удостоверение за неговия електронен подпис, да го информират чрез трайните средства за комуникация относно точните условия и изисквания за използване на удостоверението, включително и всички ограничения в използването му, упражняването на доброволни схеми за акредитация и процедури за жалби и решаване на спорове. Такава информация, която може да се предава по електронен път, трябва да бъде писмена и поднесена на разбираем език. Съответни части от тази информация следва да бъдат достъпни също по тяхна молба и на трети страни, които разчитат на удостоверението;

м) да използват надеждни системи за съхраняване на удостоверенията в такава форма, че:

- само оторизирани лица да имат достъп и да правят промени;
- автентичността на информацията да може да бъде проверена;
- удостоверенията да са обществено достъпни за извлечения само в тези случаи, в които съгласието на държателя на удостоверението е придобито, и
- всички технически промени, подлагащи на съмнение изискванията за сигурност, да бъдат известни на оператора.

Приложение III

Изисквания към защитения механизъм за създаване на подписа

1. Защитеният механизъм за създаване на подписа трябва чрез съответните технически и процедурни средства да осигури най-малко щото:
   а) данните за създаване на подписа, използвани за генерирането му, да могат практически да се намират/възпроизвеждат само веднъж и тяхната сигурност да бъде надеждно защитена;
   б) данните за създаване на подписа, с които той се генерира, да не могат с достатъчна сигурност да бъдат извлечени и подписът да е защитен срещу подправяне чрез използване на наличната сега технология;
   в) данните за създаване на подписа, използвани за генериране на подписа, да могат да бъдат надеждно защитени от легитимното подписващо лице срещу използването им от други лица;
2. Защитеният механизъм за създаване на подписа не трябва да изменя данните, които следва да се подпишат или да не пречи тези данни да бъдат представени на подписващото лице, преди началото на създаване на подписа.

Приложение IV

Предложения относно сигурното доказване на подписа

По време на процеса на проверка на подписа следва да се осигури с достатъчно ниво на сигурност, че:

а) данните, използвани за доказване на подписа, съответстват на данните, представени на доказващото лице;

б) подписът е надеждно проверен и резултатите от тази проверка са коректно изнесени;

в) доказващото лице може при необходимост надеждно да установи съдържанието на подписаните данни;

г) автентичността и валидността на удостоверението, необходими по времето на проверка на подписа, са надеждно проверени;

д) резултатите от проверката и самоличността на подписващото лице са коректно изнесени;

е) използването на псевдоним е ясно посочено; и

ж) всички промени във връзка със сигурността могат да бъдат открити.

Предложение на Европейската комисия до Европейския парламент и Съвета на Европейския съюз за директива относно правните аспекти на електронната търговия в Общия пазар

(Резюме)

http://europa.eu.int/eur-lex/en/com/dat/1998/en_598Pco586.htm

Community Preparatory Acts
COM (1998) 586 final
Document 598PC0586

I. Приложно поле

На 18 ноември 1998 г. Европейската комисия излиза с Предложение за директива относно правните аспекти на електронната търговия. Предложението е предадено за обсъждане на Съвета на Европейския съюз, на Европейския парламент, Икономическия и социален комитет и други заинтересовани организации. В резултат от проведените дискусии комисията прави ново изменено Предложение за директива, което в най-скоро време се очаква да бъде прието и да стане част от действащото европейско законодателство.

Предложението за Директива относно правните аспекти на електронната търговия има за цел да премахне пречките пред развитието на електронната търговия и да създаде законодателна рамка, която да осигури свободното движение на он-лайн услуги в общността. Предложената нормативна уредба цели да хармонизира националните разпоредби относно услугите на информационното общество, установяването на доставчиците на информационни услуги, търговската комуникация, електронните договори, отговорността на посредниците, извънсъдебното решаване на спорове и сътрудничеството между държавите членки.

Приложното поле на предложението за директива включва:

1. Установяване на доставчиците на информационни услуги (establishment of information society service providers)
2. Търговска комуникация (commercial communications)
3. Сключване на договори он-лайн (on-line conclusion of contracts)
4. Отговорност на посредниците (liability of intermediaries)
5. Приложение на директивата (implementation)

II. Определения

- **Услуги на информационното общество –** информационни услуги по смисъла на чл. 1, ал. 2 от Директива 98/34 от 22 юни 1998 г.[1], установяваща процедурата за предлагане на информация в областта на техническите стандарти и регламенти, изменена с Директива 98/48/ЕС от 20 юли 1998 г.[2]
- **Доставчик на услуги** (service provider) – физическо или юридическо лице, предоставящо услуги, свързани с информационното общество.
- **Установен доставчик на услуги**[3] – доставчик на услуги, ефективно извършващ икономическа дейност с установено място за неопределен срок. Само по себе си наличието и употребата на технически средства и технологии, необходими за предоставяне на услугата, не е критерий за определяне на установеното място на дейност на доставчика на услуги.
- **Получател на услугата** (recipient of the service) – физическо или юридическо лице, което с професионална или друга цел използва информационни услуги, и по-специално услуги за търсене и за достъп до информация.
- **Търговска комуникация** (commercial communication) – форма на комуникация, създадена с цел да представя пряко или косвено стоките, услугите или имиджа на компанията, организацията или личността, извършваща търговска, индустриална, занаятчийска дейност или упражняваща свободна професия. Не представлява търговска комуникация:
  - информацията, осигуряваща директен достъп до дейността на компанията, организа-

[1] Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations .

[2] Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations.

[3] Established service provider, по смисъла на чл. 52 и сл., Right of Establishment, EC Treaty.

цията или лицето и по-специално до електронната поща;
- комуникацията във връзка със стоки, услуги или имиджа на компанията, организацията или личността, извършена по безпристрастен начин без финансова престация.

- **Потребител –** физическо лице, действащо с цели, които са извън неговата търговия, бизнес или професия.
- **Област на координиране** (coordinated field) – хармонизиране на изискванията, приложими към услугите на информационното общество и доставчиците на тези услуги в държавите – членки на общността.

III. Основни положения

Установяване и информационни изисквания

Държавите членки се задължават да предвидят в законодателството си, че достъпът до дейността на доставчиците на информационни услуги не трябва да бъде предмет на разрешителен режим от страна на държавните им органи[4].

Без да се накърняват разпоредбите на Директива 97/7/ЕС, държавите членки предвиждат в законодателството си, че доставчиците на услуги, свързани с информационното общество, предоставят директно и постоянно на клиентите си следната информация:

1. име на доставчика на услугите;
2. адрес на доставчика на услугите;
3. други начини за връзка с доставчика (включително и електронната му поща), които дават възможност за бърза и ефективна връзка с него;
4. когато доставчикът е вписан в търговски регистър, указва се в кой регистър е извършено вписването и под кой номер;
5. когато дейността изисква разрешителен режим, предоставя се информация относно тази дейност и относно институцията, издала разрешението;
6. по отношение на регламентираните професии:
   - данни за професионалната организация или институция, където лицето е регистрирано;
   - професионалната титла, получена в държавата на регистрация и в държавата на извършване на търговска дейност;
7. данъчна регистрация и регистрация по ДДС, когато доставчикът извършва търговска дейност.

Държавите членки възприемат в законодателството си, че цените на услугите, свързани с информационното общество, всички допълнителни разходи и други съществени условия се определят ясно, точно и недвусмислено.

Търговска комуникация

Държавите членки възприемат в законодателството си, без да накърняват разпоредбите на Директива 97/7/ЕС, че търговската комуникация трябва да отговаря на следните изисквания:

1. да бъде ясно определена като такава;
2. физическите и юридическите лица, извършващи търговска комуникация, се определят ясно като такива;
3. промоционни оферти като отстъпки, премии и подаръци в случаите, когато са разрешени в държавите членки, в които е установен доставчикът на информационни услуги, се определят ясно като такива, а условията за достъп до тях се представят ясно, точно и недвусмислено;
4. промоционни състезания и игри в случаите, когато са разрешени в държавите членки, в които е установен доставчикът на информационни услуги, се определят ясно като такива с точно и недвусмислено представени условия за участие.

Спонтанна търговска комуникация

Държавите членки предвиждат в законодателството си, че спонтанната търговска комуникация (unsolicited commercial communication) чрез електронна поща трябва да бъде ясно и недвусмислено определена като такава веднага, щом е получена от получателя.

Сключване на договори по електронен път

Законодателството на държавите членки позволява сключването на договори по електронен път. Правните изисквания за сключване на електронни договори не трябва да ограничават правното им действие и валидност само на основание, че са сключени по електронен път. Държавите членки могат да предвидят този принцип да не се отнася за договорите, които се сключват по нотариален ред, договорите, които са валидни, само ако са регистрирани пред държавен орган, или договори в областта на семейното и наследственото право.

Условията за сключване на електронни договори се разясняват ясно и точно от доставчика на информационни услуги преди самото сключване на договора. Информацията включва отделните стадии на сключване на договора, дали сключеният договор трябва да бъде вписан и какви са средствата за корекции при грешки. Отделните стадии на сключване на договора по електронен път са ясно установени в законодателството на държавите членки с оглед постигането на пълно и информирано съгласие на страните.

[4] Principle excluding prior authorisation.

Моментът на сключване на договора се определя в чл. 11 на предложението за директива. Когато получателят на услугата трябва да даде съгласието си по електронен път чрез технологични средства (като например с кликване върху икона), договорът се смята сключен, ако получателят на услугата е получил от доставчика на услугата потвърждение за получаване на съгласието на получателя по електронен път.

Прилагат се следните принципи:

а) потвърждението на получаването се смята за получено, когато получателят на услугата има достъп до него;

б) доставчикът на услуги се задължава незабавно да изпрати потвърждение на получаването.

Отговорност на посредниците

Когато предлаганата информационна услуга включва прехвърляне в комуникационна мрежа на информация, предоставена от получателя на услугата, или предлагане на достъп до комуникационна мрежа, държавите членки предвиждат в законодателството си, че доставчиците на такива услуги не носят отговорност за прехвърлената информация, при условие че те:

а) не инициират прехвърлянето;

б) не избират получателя на прехвърлената информация; и

в) не избират или не изменят информацията, която се прехвърля.

Когато предлаганите услуги на информационното общество включват прехвърляне в комуникационната мрежа на информация, предоставена от доставчика на услугата, държавите членки предвиждат в законодателството си, че доставчикът не носи отговорност за временно и автоматично складиране на информацията при извършване на посредничеството, което се прави само с цел да направи по-ефективно прехвърлянето към други получатели на услугата по тяхна молба, при условие че:

а) доставчикът не изменя информацията;

б) доставчикът съблюдава изискванията за достъп до информацията;

в) доставчикът съблюдава правата относно осъвременяването на информацията по начин, който отговаря на индустриалните стандарти;

г) доставчикът не се намесва в технологии, съответстващи на индустриалните стандарти, използвани за придобиване на данни за употреба на информацията; и

е) доставчикът действа незабавно за отстраняване или установяване на забрана за достъпа до информацията при узнаване на следното:

- информацията при първоначалния източник на прехвърляне е била отстранена от мрежата;
- достъпът до информацията е бил забранен;
- компетентна организация е наредила такова отстраняване или забрана.

Складиране на информация

Когато предоставената услуга на информационното общество включва складиране на информация (hosting) на получателя на услугата, държавите членки предвиждат в законодателството си, че доставчикът не носи отговорност за складираната по молба на получателя на услугата информация, при условие че:

а) доставчикът не знае, че дейността е незаконна и във връзка с исковете за вреди не са му известни факти или обстоятелства, от които да произлиза, че дейността е незаконна;

б) доставчикът при узнаване на това действа незабавно за отстраняване или прекратяване на достъпа до информация.

Тази разпоредба не се прилага, ако получателят на услугата действа под властта или контрола на доставчика на услугата.

Отсъствие на задължение за наблюдение

Държавите членки не налагат общо задължение за доставчиците при предлагане на своите услуги да наблюдават информацията, която те прехвърлят или складират, нито общо задължение да следят за факти или обстоятелства, указващи наличие на незаконна дейност.

Това правило не се отнася до временни и нарочни дейности по наблюдение, инициирани от националните съдебни органи съгласно националното законодателство, с цел да се защити националната сигурност, обществения ред и с цел предотвратяване, разследване и разкриване на криминални престъпления.

Държавите членки и Комисията поощряват изработването на правила за поведение в общността на търговци, професионални и потребителски асоциации или други организации. Изработените правила за поведение на национално и европейско ниво се предоставят на Комисията, която преглежда съответствието им с правото на общността.

Извънсъдебно решаване на спорове

Държавите членки предвиждат, че при спор между доставчика на информационни услуги и получателя законодателството им позволява ефективно използване на извънсъдебни схеми за решаване на спорове, включително и чрез съответни електронни средства.

Държавите членки следва да осигурят тясно сътрудничество между компетентните организации, които да имат високо равнище на контрол и раз-

следване, необходимо за точното прилагане на директивата. От своя страна доставчиците на информационни услуги следва да им предоставят цялата изискуема от тях информация.

Държавите членки определят санкциите при нарушаване на националните правила, възприети на базата на директивата. Те следва да бъдат ефективни и пропорционални. Комисията се уведомява за възприетите национални мерки.

Предвидени са изключения, за които директивата не се прилага, а именно:

а) при финансови задължения/фиск;

б) в областта на приложение на Директива 95/46/ЕС и Директива 97/66/ЕС на Европейския парламент и Съвета на Европейския съюз;

в) дейностите на доставчиците на информационни услуги съгласно приложение I, което включва дейността на нотариуси, представителство и защита на интереси в съдебната система, както и хазарт с изключение на този, провеждан за търговска комуникация. Този списък от дейности може да бъде променян от Комисията.

При определени условия други ограничения в приложението на текстовете на директивата могат да бъдат наложени от компетентните органи в държавите членки за защита на обществения ред, здравето, сигурността и за защита на потребителя.

Европа

Кралски Указ-закон № 14 за електронния подпис от 17 септември 1999 г., Испания

На заседание на Съвета на министрите на телекомуникациите на Европейския съюз, проведено на 22 април 1999 г., се прие единно становище за проекта за директивата на Европейския парламент и Съвета на Европейския съюз, с която се въвежда обща уредба за електронния подпис.

Испания взе активно участие за постигането на единно становище, което улеснява придвижването на текста и включването на достатъчно елементи за защита на сигурността и неприкосновеността на телематичните комуникации, при които се използва електронният подпис. В Испания вече съществуват различни разпоредби за подаване на декларации за данък върху общия доход на физическите лица чрез телематични средства, определени от данъчната администрация. От своя страна Националната комисия за пазарите на ценни книжа прие и пусна в употреба система за кодиране и електронен подпис, която се използва за получаване на информация от наблюдаваните дружества. Чл. 81 от Закон № 66 за данъчните и административни средства и социалния ред от 30 декември 1997 г. посочва възможността да се представят посредством Националната монетарна и печатна фабрика – Кралска монетарница, технически и административни услуги за гарантиране сигурността, валидността и ефективността на емисията и получаване на комуникации чрез електронни, информационни и телематични методи и средства. Националната монетарна и печатна фабрика – Кралска монетарница, си сътрудничи с пощите и телеграфите.

По молба на Испания в проекта за директива е включено допълнение, съдържащо се в ал. „в“ на приложение II, в изискванията за доставчиците на услуги, които издават признати удостоверения. С това допълнение се разрешава удостоверението да съдържа датата и часа на извършване на удостоверяваното действие.

Освен това в Испания съществува предприемачески сектор, който би могъл да предостави услуга за удостоверяване на електронния подпис с необходимото качество. Счита се, че трябва да се въведе възможно най-бързо уредба, която позволява с необходимата правна сигурност използването на това технологично средство, съдействащо за развитието на т. нар. от Европейския съюз „информационно общество“. Незабавното приемане на тази уредба се дължи и на желанието за създаване на доверие у потребителите на нови услуги в системите, което улеснява тяхното въвеждане и бързо разпространение.

Кралският указ-закон има за цел, придържайки се към съдържанието на единното становище на Директивата за електронния подпис, установяване на ясна регулация за неговата употреба, правно действие и определяне на режима за доставчиците на удостоверителни услуги. По подобен начин кралският указ-закон регламентира регистъра, в който се записват доставчиците на удостоверителни услуги и режимът за административен контрол на тяхната дейност, регулира издаването и валидността на удостоверенията и определя нарушенията и санкциите, гарантиращи неговото изпълнение.

Настоящата уредба се подчинява на процедурите за получаване на информация съгласно нормативните актове и техническите разпоредби, предвидени в Директива 98/34/ЕС на Европейския парламент и Съвета на Европейския съюз от 20 юли 1998 г. и Кралския декрет № 1337 от 31 юли 1999 г.

По предложение на министъра на развитието, министъра на правосъдието, министъра на промишлеността и енергетиката, предварителния доклад на Генералния съвет на съдебната власт и Агенцията за защита на информацията след обсъждането от Съвета на министрите на заседание, проведено на 17 септември 1999 г., и по силата на дадените ми правомощия съгласно чл. 86 на Конституцията

ПОСТАНОВЯВАМ:

Раздел I
Общи разпоредби

Глава I
Общи разпоредби

Чл. 1. Сфера на приложение

(1) Настоящият кралски указ-закон регулира употребата на електронния подпис, признаването

на неговото правно действие и публичното предоставяне на удостоверителни услуги. Разпоредбите за този вид дейност се прилагат за доставчиците на услуги, установени в Испания.

(2) Разпоредбите, съдържащи се в настоящия кралски указ-закон, не противоречат на нормите, свързани със сключването, формалностите, валидността и действието на договорите и други юридически актове, нито на правния режим за задълженията.

Разпоредбите за предоставянето на услуги за удостоверяване на електронния подпис, съдържащи се в настоящия кралски указ-закон, не заменят и не отменят онези, които регулират дейностите, извършвани от упълномощените лица за гарантиране достоверността на подписа в документите или за намеса при неговото публично използване.

Чл. 2. Определения

Настоящият кралски указ-закон въвежда следните определения:

а) „**Електронен подпис**“. Сбор от данни в електронен вид, приложени към други електронни данни или свързани функционално с тях, използвани като средство за формално идентифициране на автора или авторите на документа.

б) „**Усъвършенстван електронен подпис**“. Електронен подпис, позволяващ разпознаването на подписания. Създаден е със средства и данни, съхранявани под изключителния му контрол и по начин, известен единствено на него. Това позволява разкриването на всякакви бъдещи изменения.

в) „**Подписан**“. Физическо лице, притежаващо механизъм за създаване на подпис и действащо от свое име или от името на физическо или юридическо лице, което представлява.

г) „**Данни за създаване на подписа**“ . Това са уникални данни като кодове или лични криптографски знаци, които участникът използва за създаване на електронния подпис.

д) „**Механизъм за създаване на подписа**“. Представлява програма или информационно устройство, което се използва за въвеждане на данните за създаване на подписа.

е) „**Защитен механизъм за създаване на подписа**“. Механизъм за създаване на подписа, който отговаря на изискванията, посочени в чл. 19.

ж) „**Данни за проверка/верификация на подписа**“. Уникални данни като кодове или лични криптографски знаци, които се използват за проверяване на електронния подпис.

з) „**Механизъм за проверка/верификация на подписа**“. Представлява програма или информационно устройство, което се използва за прилагане на данните за проверка на подписа.

и) „**Удостоверение**“. Електронно удостоверение, което съдържа всички данни за доказване достоверността на подписа на участника и потвърждава неговата идентичност.

к) „**Признато удостоверение**“. Удостоверение, което съдържа информацията, описана в чл. 8, и се издава от доставчик на удостоверителни услуги, както и отговаря на изброените в чл. 12 изисквания.

л) „**Доставчик на удостоверителни услуги**“. Физическо или юридическо лице, което издава удостоверения и може да оказва друг вид услуги, свързани с електронния подпис.

м) „**Продукт на електронния подпис**“. Програма или информационен уред или неговите специфични елементи, предназначени да бъдат използвани за оказването на услуги с електронен подпис от доставчика на удостоверителни услуги или за доказване на електронния подпис.

н) „**Доброволно упълномощаване на доставчика на удостоверителни услуги**“. Резолюция, която определя особените права и задължения за оказването на удостоверителни услуги. Постановява се от обществения орган, натоварен да наблюдава доставчика по негова собствена молба.

Чл. 3. Правни действия на електронния подпис

(1) Усъвършенстваният електронен подпис винаги когато се основава на признато удостоверение и е създаден със защитен механизъм, ще има по отношение на данните, съхранявани в електронен вид, същата правна сила като ръчния подпис, положен на хартиен документ, и се приема за доказателство пред съда, оценявайки се съгласно критериите, установени с процесуалните норми.

Предполага се, че усъвършенстваният електронен подпис съдържа всички необходими условия за пораждане на посочените в тази алинея действия, когато признатото удостоверение, на което се основава, е издадено от упълномощен доставчик на услуги, а защитният механизъм за създаване на подписа притежава удостоверение, съобразно предвиденото в чл. 21.

(2) Електронен подпис, който не съдържа елементите, посочени в предходната алинея, запазва правните действия и се приема за доказателство пред съда, поради самото обстоятелство, че се представя в електронен вид.

Раздел II
Предоставяне на удостоверителни услуги

Глава I
Общи принципи

Чл. 4. Режим на свободна конкуренция

(1) Предоставянето на удостоверителни услуги не се подчинява на предварително оторизиране и се осъществява в условията на свободна конкуренция, без да се въвеждат ограничения за удостоверителните услуги, произхождащи от някоя държава – членка на Европейския съюз.

(2) Предоставянето на удостоверителни услуги от администрацията или подчинените ѝ органи и организации се осъществява със съответното разпределение на отговорностите и съгласно принципите за обективност, прозрачност и недискриминация.

Чл. 5. Използване на електронния подпис от държавната администрация

(1) С държавен указ или в конкретния случай с вътрешни правила употребата на електронния подпис в сферата на държавната администрация и обществените учреждения и в отношенията, които те поддържат с частни лица, може да се подчинява на допълнителни условия, считани за необходими за гарантиране на защита при всяка процедура.

Допълнителните условия, които се въвеждат, могат да съдържат предоставянето на услуга за съхранение на датата и часа по отношение на електронните документи, включени в административния документ. Цитираната услуга се състои в удостоверяването от доставчика на услуги или от трето лице на датата и часа, в който даден електронен документ е изпратен от подписания или получен от получателя.

Държавните разпоредби, регулиращи допълнителните условия за употребата на електронния подпис, за които се отнася тази алинея, могат единствено да засягат особени характеристики на приложение и се приемат по предложение на Министерството на държавната администрация и предварителния доклад на Върховния съвет по информатика.

(2) Допълнителните условия, за които се отнася предходната алинея, трябва да гарантират изпълнението на предвиденото в чл. 45 на Закон № 30 за правния режим на държавната администрация и общите административни процедури от 26 ноември 1992 г. да бъдат обективни, прозрачни, справедливи и недискриминативни и да не възпрепятстват предоставянето на услуги на гражданите, когато се намесват различни национални или чужди държавни администрации.

(3) Използването на електронния подпис се подчинява на специфичен режим при комуникациите, засягащи класифицираната информация, държавната сигурност и защита. Министерството на финансите, спазвайки изискванията, предвидени в настоящия кралски указ-закон, може да въведе нормативен режим за гарантиране изпълнението на данъчните задължения, като определи по отношение събирането на данъците възможността участникът да бъде физическо или юридическо лице.

Чл. 6. Система за лицензиране на доставчици на удостоверителни услуги и на услуги за удостоверяване продуктите на електронния подпис

(1) Правителството чрез кралски указ може да въведе доброволни системи за упълномощаване доставчиците на услуги за удостоверяване на електронния подпис, определяйки режим, който позволява постигане на необходимата сигурност и защита правата на потребителите.

(2) Дейностите по удостоверяването, за които се отнася настоящият кралски указ-закон, се извършват от компетентните органи по отделните случаи, предвидени в Закон № 11 от 24 април 1998 г. – Общ закон за телекомуникациите, Закон № 21 за промишлеността от 16 юли 1992 г., и в останалата част от действащото в областта законодателство. Кралският указ, за който се отнася ал. 1, определя условията, разрешаващи координирането на системите за удостоверяване.

(3) Нормите, които регулират системите за лицензиране и удостоверяване, трябва да са обективни, справедливи и недискриминативни. Всички доставчици на услуги, подчиняващи им се доброволно, могат да получат съответното пълномощно за дейността си, или в конкретния случай – удостоверение за продукта на електронния подпис, който използват.

(4) Компетентните органи по изпълнение на дейностите, посочени в предходната алинея, разглеждат техническите доклади, издавани от лицензиращите организации, за доставчиците на услуги, помолили за получаване на пълномощно, или докладите за продуктите, за които е поискано удостоверение. За да бъде упълномощен доставчикът на услуги, под внимание се взима и изпълнението на установените с наредба изисквания.

(5) Съгласно настоящия кралски указ-закон лицензиращи организации могат да бъдат само онези, лицензирани от независим орган, придобил това право с кралския указ, за който се отнася ал. 1 на настоящия член.

Чл. 7. Регистър на доставчиците на удостоверителни услуги

(1) В Министерството на правосъдието се създава Регистър на доставчиците на удостоверителни услуги. Всички доставчици в Испания трябва да помолят да бъдат вписани предварително, преди да започнат своята дейност.

(2) Молбата за вписване се подава заедно с нормативно предвидената документация, с цел да се идентифицира доставчикът на удостоверителни услуги и да се установи дали отговаря на всички изисквания, за да осъществява дейността си. Предмет на бъдеща регистрация е и всяко обстоятелство съгласно настоящия кралски указ-закон, свързано с доставчика на удостоверителни услуги, като неговото упълномощаване или правото да издава признати удостоверения.

Включването в Регистъра на доставчиците на услуги е условие те да започнат или продължат своята дейност, без да се нарушава приложението на съответния режим на санкции.

(3) Регистърът на доставчиците на удостоверителни услуги е публичен и трябва да поддържа постоянно актуализирана и на разположение на всеки заинтересован информация за регистрираните, която съдържа име и търговска фирма, адрес на страницата в Интернет или адреса на електронната поща, данните за сравняване на техния електронен подпис и в конкретния случай положението на упълномощено лице или възможността да издава признати удостоверения. В споменатата информация се включват и всякакви други допълнителни сведения, които се определят от кралския указ.

Записаните данни в регистъра могат да се проверяват по телематичен път или чрез наличното регистрационно удостоверение. Подобна информация може да се получава срещу заплащане на определена такса, установена от закона.

Глава II
Удостоверения

Чл. 8. Изисквания за наличието на признато удостоверение

(1) Признатите удостоверения, описани в чл. 2, б. „к“ на настоящия кралски указ-закон, съдържат:

а) обозначение, че се издават като такива;

б) единен идентификационен код на удостоверението;

в) самоличността на доставчика на удостоверителни услуги, посочване на неговото наименование и правен статус, седалище, данъчен номер и регистрационните данни;

г) усъвършенстваният електронен подпис на доставчика на удостоверителни услуги, който издава удостоверението;

д) обозначаване на подписания, от което да стават ясно по недвусмислен начин неговото име и презимена или псевдоним; в удостоверението може да се обозначи всякаква друга лична особеност на титуляря, която е от значение за целите на удостоверението, когато той е дал своето съгласие;

е) при представителство посочване на документа, определящ правата на подписания да действа от името на физическото или юридическото лице, което представлява;

ж) данни за проверка на подписа, които съответстват на данните за създаване на подписа, намиращи се под контрола на подписания;

з) начало и край на срока на валидност на удостоверението;

и) ограничения за използване на удостоверението, ако се предвиждат;

к) ограниченията за цената на сделките, при които удостоверението може да се използва, ако се предвиждат;

(2) Включването в удостоверението на всяка друга информация, свързана с подписания, изисква неговото изрично съгласие.

Чл. 9. Валидност на удостоверението

(1) Удостоверенията за електронен подпис са невалидни при възникване на някои от следните обстоятелства:

а) изтичане срока на валидност на удостоверението. Когато се касае за признати удостоверения, този срок не може да превишава четири години, считано от датата на тяхното издаване;

б) анулиране от подписания, физическото или юридическото лице, което представлява, или от трето упълномощено лице;

в) загубване или невъзможност да се използва, поради нанесени повреди на удостоверението;

г) неправомерно използване от трето лице;

д) съдебно или административно решение, което го отменя;

е) смърт на подписания или на неговия представител, внезапна пълна или частична недееспособност, изтичане срока на представителството или заличаване на представляваното юридическо лице;

ж) преустановяване дейността на доставчика на удостоверителни услуги, освен когато с предварителното изрично съгласие на подписания издадените от него удостоверения са прехвърлени на друг доставчик на услуги;

з) големи неточности в данните, предоставени от подписания, за получаване на удостоверение.

(2) При изтичане срока на валидност и преустановяване дейността на доставчика на услуги правното действие на удостоверенията се прекратява от възникването на тези обстоятелства. Във всички останали случаи прекратяването на правното действие на дадено удостоверение поражда действия от деня, в който доставчикът на услуги разбере за възникването на посочените събития и го отбележи в своя регистър на удостоверенията, разгледан в чл. 11, б. „д".

(3) При всяко от посочените обстоятелства доставчикът на услуги трябва да отбележи заличаване на удостоверението в регистъра, за който се отнася чл. 11, б. „д", и ще отговаря за възможните щети, нанесени на подписания или на трети лица при закъснение на отбелязването. Доказателството, че третите лица са били запознати с обстоятелствата по невалидността на удостоверението, е в полза на доставчика на услуги.

(4) Доставчикът на услуги може да отмени действието на издадените удостоверения временно, по молба на подписания или на неговите представители, или по заповед на съдебен или административен орган. Отменянето поражда действията, предвидени в предходните две алинеи.

Чл. 10. Признаване на удостоверенията

Удостоверенията, издавани като признати от доставчиците на услуги, които са регистрирани в страна, нечленуваща в Европейския съюз, и съгласно нейното законодателство, се признават като издадени от доставчици, регистрирани в Испания, винаги когато са изпълнени някои от следните условия:

а) доставчикът на услуги да отговаря на изискванията на единните разпоредби за електронния подпис и да е упълномощен съгласно доброволна система, действаща в някоя от държавите – членки на Европейския съюз;

б) удостоверението да е гарантирано от доставчик на услуги от Европейския съюз, който да отговаря на изискванията, регламентирани в единните разпоредби за електронния подпис;

в) удостоверението или доставчикът на услуги да са признати по силата на двустранен или многостранен договор между Европейската общност и трети страни или международни организации.

Глава III
Изисквания за доставчиците на удостоверителни услуги

Чл. 11. Задължения на доставчиците на удостоверителни услуги

Всички доставчици на услуги се задължават:

а) да проверяват сами или чрез физическо или юридическо лице, което действа от тяхно име и за тяхна сметка, самоличността и всякакъв вид лични данни на желаещите да получат удостоверение за извършване на дейността си, като си служат с всички средства, предвидени от закона. От това задължение се освобождават доставчиците на услуги, които, издавайки удостоверения без статут на признати, се ограничават да проверят определени сведения за подалите молби;

б) да предоставят на разположение на подписания средствата за създаване и проверка на електронния подпис;

в) да не задържат и да не копират данните за създаване на подписа на лицето, на което са предоставили своите услуги, с изключение на случаите, когато то го изисква;

г) преди издаването на удостоверението да информират лицето, желаещо да ползва неговите услуги, за цената, точните условия за използване на удостоверението, ограниченията за употреба и начина, по който се гарантира неговата възможна имуществена отговорност;

д) да водят регистър с информация за издадените удостоверения и условията, при които се отменя или преустановява валидността им. Достъпът до регистъра става чрез телематични средства, а съдържанието му е на разположение на лицата, помолили за това, когато така е посочено от подписания;

е) в случай на преустановяване на дейността си доставчиците на услуги трябва да уведомят предварително съгласно предвиденото в § 1, чл. 13 титулярите на удостоверенията, издадени от самите тях, и ако са вписани – Регистъра на доставчици на услуги към Министерството на правосъдието;

ж) да вписват в регистъра доставчиците на удостоверителни услуги;

з) да изпълняват останалите предвидени разпоредби по отношение на тях в настоящия кралски указ-закон и изискванията за упражняване на дейността.

Чл. 12. Задължения на доставчиците на услуги, издаващи признати удостоверения

Освен задълженията, предвидени в чл. 7 и 11, доставчиците на услуги, които издават признати удостоверения, се задължават още:

а) да посочват датата и часа, в който е издадено удостоверението или е обявено за невалидно;

б) да доказват необходимата достоверност на своите услуги;

в) да гарантират бързината и сигурността на услугата. По-конкретно трябва да позволят използването на бърза и сигурна услуга за консултация с Регистъра на издадените удостоверения и да гарантират унищожаването или отменянето на действието им по незабавен и сигурен начин;

г) да използват квалифициран персонал с необходимия опит за оказване на предлаганите услуги в сферата на електронния подпис и съответните процедури и действия за сигурност;

д) да използват надеждни системи и продукти, защитени срещу всякаква външна намеса, и да гарантират техническа и криптографска сигурност на процесите по удостоверяването, за които се прилагат;

е) да вземат мерки срещу фалшифициране на удостоверенията, а в случай че доставчикът на услуги притежава данни за създаване на подпис, и да гарантират поверителност в процеса на създаването му;

ж) да разполагат с достатъчно икономически средства, за да действат съобразно предвиденото в настоящия кралски указ-закон и, в частност, за да посрещнат риска от отговорност за нанесени загуби и щети. Трябва да гарантират своята отговорност пред потребителите на услуги и трети лица, ощетени от тях. Учредителната гаранция може да бъде търговско поръчителство посредством кредитна институция или застрахователна полица.

Първоначално гаранцията покрива поне 4% от максимално допустимата стойността на сделките, при които може да се използва комплектът удостоверения, издавани от всеки доставчик на услуги. Имайки предвид развитието на пазара, правителството може да намали с кралски указ този процент до 2%.

В случай че няма ограничения за стойността на сделките, при които може да се използва комплектът от удостоверения, издавани от доставчика на услуги, учредителната гаранция покрива поне неговата отговорност с вноска от 1 000 000 000 песети (6 010 121.04 евро). С кралски указ правителството променя съответната стойност;

з) да съхраняват в продължение на петнадесет години цялата документация и информация, свързана с издадено признато удостоверение, което може да се осъществява и чрез електронни средства;

и) преди издаването на удостоверение да информират желаещия за цената и точните условия за използване на удостоверението. Информацията трябва да съдържа възможните ограничения за употреба, упълномощаване на доставчика на услуги и процедурите за рекламация и разрешаване на спорове, предвидени в законите, и е необходимо да бъде лесно разбираема. Тя е на разположение и на трети заинтересовани лица и се включва в документ, предоставящ се на всеки, който го поиска. За разпространяването на тази информация могат да се използват електронни средства, ако подписаният или заинтересованите трети лица са съгласни;

к) да използват надеждни системи за съхраняване на удостоверенията, така че:

1. само упълномощени лица да могат да се консултират с тях, ако те единствено са на разположение за проверка на електронни подписи;
2. единствено упълномощени лица да могат да внасят в тях забележки или изменения;
3. да може да се докаже автентичността на информацията;
4. подписаният или упълномощеното лице да може да разкрива всички технически промени, които не са съобразени с посочените изисквания за сигурност, за да достигне до удостоверенията;

л) да информират всички потребители на техните услуги за критериите, които се задължават да спазват, съобразявайки се с настоящия кралски указ-закон и неговите разпоредби за развитие и изпълнение на дейността им.

Чл. 13. Преустановяване на дейността

(1) Доставчикът на услуги, преустановяващ своята дейност, уведомява всички титуляри на издадени от него удостоверения и прехвърля с изричното им съгласие все още валидните към датата на преустановяването на друг доставчик, който ги приема или оставя без действие. Известието се прави предварително и най-малко два месеца преди окончателното преустановяване на дейността.

(2) Ако доставчикът на услуги е вписан в Регистъра на доставчиците на удостоверителни услуги към Министерството на правосъдието, уведомява министерството в срока, посочен в предходната алинея, за преустановяването на дейността си и за направлението, което ще даде на удостоверенията, посочвайки дали ще ги прехвърли и на кого, или ще ги остави без дейс-

твие. Посочва и всякакви други обстоятелства, които могат да попречат за продължаване на дейността му. По-точно съобщава за откриване на производство по несъстоятелност или преустановяване на плащания по отношение на него, когато научи за това.

(3) Регистрацията на доставчика на услуги в Регистъра на доставчиците на удостоверителни услуги се отменя официално от Министерството на правосъдието, когато той преустанови дейността си. Министерството на правосъдието отговаря за информацията относно удостоверенията, оставени без действие от доставчика на услуги, съгласно предвиденото в чл. 12, б. „з“.

Чл. 14. Отговорности на доставчиците на удостоверителни услуги

(1) Доставчиците на удостоверителни услуги отговарят за претърпените щети и загуби на всяко лице при извършване на дейността си, когато това се дължи на неизпълнение на задълженията, които им налага настоящият кралски указ-закон, или поради небрежност. При всички случаи доставчикът на услуги доказва, че е действал с необходимата добросъвестност.

(2) Доставчикът на удостоверителни услуги носи отговорност само за щетите и загубите, причинени от неправомерната употреба на признатото удостоверение, когато не е посочено в него по ясен за възприемане от трети лица начин ограничението за възможното му приложение или стойността на действителните сделки, които могат да се осъществяват чрез неговото използване.

(3) Отговорността се търси съобразно общите разпоредби за договорната и извъндоговорна отговорност, според нейното възникване и съгласно особеностите, предвидени в този член. Когато гаранцията, дадена от доставчиците на услуги не е достатъчна, за да покрие дължимото обезщетение, те отговарят за дълга с цялото си настоящо и бъдещо имущество.

(4) Тълкуването на разпоредбите на този член не може да противоречи на действащото законодателство за защита на потребителите.

Чл. 15. Защита на личните данни

(1) Подходът спрямо личните данни, които се събират от доставчиците на услуги за дейността им и прилагат в Регистъра на доставчиците на удостоверителни услуги, за който се отнася настоящият кралски указ-закон, се подчиняват на Основния закон № 5 за регулиране автоматичното използване на данни от личен характер от 29 октомври 1992 г. и разпоредбите за тяхното разработване. Същият режим се прилага спрямо личните данни, известни на органа, който при изпълнение на задълженията си наблюдава дейността на доставчиците на услуги и компетентното лице в областта на упълномощаването.

(2) Доставчиците на услуги, издаващи удостоверения на потребителите, могат единствено да получават лични данни от титулярите или с тяхното изрично съгласие. Могат да се искат само данни, необходими за издаване и използване на удостоверението.

(3) Доставчиците на услуги, отбелязали псевдоним в удостоверението по молба на подписания, установяват неговата идентичност и съхраняват документацията, която го легитимира. Тези доставчици на услуги са задължени да разкриват самоличността на титулярите на удостоверения, когато го изискват съдебните органи при изпълнение на задълженията си и съгласно предвиденото в чл. 11, ал. 2 на Основния закон № 5 от 29 октомври 1992 г. Настоящото се прилага, доколкото не противоречи на разпоредбите за идентифициране на лицата от специфичното законодателство в данъчната сфера, защитата на конкуренцията и обществената сигурност.

Във всички случаи се взема под внимание предвиденото в разпоредбите за защита на данните, посочени в ал. 1 на този член.

Глава IV
Проверка и контрол на дейността на доставчиците на удостоверителни услуги

Чл. 16. Наблюдение и контрол

(1) Министерството на развитието контролира посредством Главния секретариат за комуникации изпълнението от доставчиците на услуги, издаващи обществено признати удостоверения, на задълженията, посочени в настоящия кралски указ-закон и неговите разпоредби за приложение. Едновременно следи доставчиците на услуги да спазват задълженията си и да издават само признати удостоверения съгласно изискванията на чл. 11.

(2) При осъществяването на контрола Главният секретариат за комуникации действа официално чрез обосновано искане от Министерството на правосъдието, други административни органи или по настояване на заинтересованото лице. Служителите на Главния секретариат за комуникации, записани към Инспектората по телекомуникации, по силата на изпълнение на контролните им функции се считат за публична власт.

(3) Когато в резултат на проверка се установи несъответствие при употребата на данни с предвиденото в чл. 11, б. „в“, Главният секретариат

за комуникации уведомява Агенцията за защита на информацията. Тя от своя страна съгласно Основния закон № 5 от 1992 г. може да инициира наказателно производство съобразно със законодателството, регулиращо дейността ѝ.

Чл. 17. Задължение за сътрудничество

Доставчиците на услуги са задължени да предоставят на Главния секретариат за комуникации всякаква информация и необходимите средства за изпълнение на техните задължения. Позволяват на нейните служители или на личния инспектор достъп до оборудването и консултиране с какъвто и да е документ, свързан с проверката, която се отнася винаги за информация, засягаща доставчика на услуги.

Чл. 18. Решения на контролния орган

Главният секретариат за комуникации може да нареди на доставчиците на услуги вземането на целесъобразни мерки за спазването на настоящия кралски указ-закон и разпоредбите за неговото приложение.

Раздел III

Механизми на електронния подпис и оценка на съвместимостта с прилаганата нормативна уредба

Глава I

Механизми на електронния подпис и оценка на съвместимостта с прилаганите разпоредби

Чл. 19. Защитни механизми за създаване на електронния подпис

По силата на чл. 2, б. „е“, за да става ясно, че механизмът за създаване на даден електронен подпис е защитен, се изисква:

(1) Да гарантира, че използваните данни за генериране на подписа могат да се възпроизведат само веднъж и благоразумно да пази неговата тайна.

(2) Да съществува достатъчна сигурност, че споменатите данни не могат да се възпроизвеждат от тези за сравняване на подписа и от самия подпис, както и че подписът не може да бъде фалшифициран със съществуващите технологии по всяко време.

(3) Данните за създаване на подписа да са надеждно защитени от подписания срещу използване от други лица.

(4) Използваният механизъм да не повреждa данните и документа, който трябва да се подпише, както и да не пречи той да бъде показан на подписания преди създаването на подписа.

Чл. 20. Технически норми

(1) Предполага се, че продуктите на електронния подпис, съгласувани с техническите норми, чиито справочни номера са публикувани в „Официален вестник на Европейските общности“, са съгласувани с предвиденото в чл. 12, буква „е“ и в чл. 19.

(2) Справочните номера на тези норми се публикуват в „Държавния официален бюлетин“, без това да поражда някакви съмнения.

Чл. 21. Оценка на съвместимостта на защитните механизми за създаване на електронния подпис с нормативната уредба

(1) Удостоверяващите органи, за които се отнася чл. 6, могат да удостоверяват защитните механизми за създаване на електронния подпис и да получават предварителна оценка на техните технически доклади от акредитирани оценяващи организации.

При оценката на изпълнението на предвидените условия в чл. 19 оценителните организации прилагат техническите норми за продуктите на електронния подпис, за които се отнася предходният член и други, определени от упълномощаващите и удостоверяващи органи, чиито доклади се публикуват в „Държавния официален бюлетин“.

(2) Валидни са удостоверенията за защитните механизми за създаване на електронния подпис, издадени от определените за това органи от държавите – членки на Европейския съюз, когато оповестят, че механизмите отговарят на изискванията, съдържащи се в единната уредба за електронния подпис.

Чл. 22. Механизми за проверка на подписа

(1) Механизмите за сравняване на усъвършенствания електронен подпис трябва да гарантират следното:

а) подписът да се проверява по надежден начин и резултатът от тази проверка да бъде точно представен;

б) при необходимост проверяващият да може да установи по надежден начин съдържанието на подписаните данни и да провери дали не са променени;

в) да се посочва точно самоличността на подписания или ясно да се обозначи използването на псевдоним;

г) удостоверението да се потвърди по надежден начин;

д) разкриване на всякаква промяна, свързана с неговата сигурност.

(2) Кралският указ, за който се отнася чл. 6, може да определи сроковете, когато оценителните организации и удостоверяващите органи могат да

оценят и удостоверят дали средствата за проверяване на усъвършенствания електронен подпис отговарят на изискванията, установени в този член.

Раздел IV
Такса за признаване на пълномощни и удостоверения

Глава I
Такса за признаване на пълномощни и удостоверения

Чл. 23. Режим на заплащане

(1) Признаването на пълномощните и удостоверенията съобразно чл. 6, 21 и 22 от компетентните държавни органи се облага с такса, за която се прилага следният режим:
   а) задължително е признаването от посочените органи на пълномощното на доставчиците на услуги или удостоверението на средствата за създаване и проверяване на електронния подпис, за който се отнасят чл. 6, 21 и 22;
   б) пасивна страна е физическото или юридическото лице, което се облагодетелства от съответното пълномощно или удостоверение;
   в) квотата е 47 500 песети (285.48 евро) за всяко пълномощно или признато удостоверение; тази сума може да се актуализира чрез кралски указ;
   г) внася се при представяне на молбата за признаване на съответното пълномощно или удостоверение.

(2) Отмяната на таксата е нормативно установена.

Раздел V
Нарушения и санкции

Глава I
Нарушения и санкции

Чл. 24. Класификация на нарушенията

Нарушенията на регулативните разпоредби за електронния подпис и услугите за удостоверяване се разделят на много тежки, тежки и леки.

Чл. 25. Нарушения

(1) Много тежки нарушения са:
   а) неизпълнението от доставчиците на услуги, издаващи признати удостоверения, на задълженията, посочени в която и да е буква на чл. 11, с изключение на букви „в“, „ж“ и „з“.
   б) неизпълнението от доставчиците на услуги, издаващи признати удостоверения, на задълженията, наложени им в букви „в“ до „к“ на чл. 12, винаги когато се причиняват тежки щети на потребителите или на трети лица, или сериозно се застрашава сигурността на удостоверителните услуги;
   в) тежкото или повторно нарушение от доставчиците на услуги на решенията, взети от Главния секретариат по комуникации, за гарантиране спазването на настоящия кралски указ-закон.

(2) Тежки нарушения са:
   а) неизпълнението от доставчиците на услуги, които не издават признати удостоверения, на задълженията, предвидени във всички букви на чл. 11, с изключение на букви „в“, „ж“ и „з“, винаги когато се нанасят тежки щети на потребителите или на трети лица, или се засяга сериозно сигурността на удостоверителните услуги;
   б) неизпълнението от доставчиците на услуги, издаващи признати удостоверения, на предвидените задължения в букви „а“, „б“ и „л“ на чл. 12;
   в) неизпълнението от доставчиците на услуги, издаващи признати удостоверения, на задълженията в букви „в“ до „к“ на чл. 12, когато не са налице обстоятелствата, предвидени в ал. 1, буква „б“ на този член;
   г) липсата на връзка между доставчиците на услуги и Министерството на правосъдието в сроковете, предвидени в чл. 13, по отношение на преустановяване дейността или разкриване на процедура за преустановяване на плащанията или обявяване на фалит;
   д) съпротива, извинение или отказ на ревизия от упълномощените органи съобразно с настоящия кралски указ-закон;
   е) неизпълнението на решенията на Главния секретариат за комуникации, които гарантират, че доставчикът на услуги се съобразява с настоящия кралски указ-закон, когато не трябва да се счита за много тежко нарушение съгласно ал. 1, буква „в“ на този член.

(3) Леки нарушения са:
   а) неизпълнението от доставчиците на услуги, издаващи признати удостоверения, на посочените задължения в която и да е буква на чл. 11 с изключение на буква „в“, когато не трябва да се тълкува като тежко нарушение съгласно предвиденото в ал. 2, буква „а“ на този член;
   б) издаването на признати удостоверения, които не отговарят на някои от условията, посочени в чл. 8;
   в) непредоставянето на сведения, поискани от

Министерството на правосъдието или Главния секретариат за комуникации, за да проверят спазването на настоящия кралски указ-закон от доставчиците на удостоверителни услуги;

г) всякакъв друг вид неизпълнение на задълженията, наложени на доставчиците на услуги с настоящия кралски указ-закон, с изключение на посоченото в чл. 11, буква „в“ или това, което трябва да се счита за тежко или много тежко нарушение съгласно постановеното в предходните алинеи.

Чл. 26. Санкции

(1) Комисията налага следните санкции за нарушенията, включени в предходния член:

а) за много тежки нарушения, комисията налага на нарушителя глоба на стойност, не по-ниска от брутната печалба, нито по-висока от петорния размер, получена в резултат на действията или небрежността, в която се изразява нарушението. В случай че не може да се приложи този критерий или от приложението му се получава сума, по-ниска от най-високата от посочените по-нататък, най-високата стойност определя границата на паричната санкция. За тези цели се определят следните стойности: едно на сто от брутните годишни приходи, получени от организацията нарушител през последната бюджетна година, или при липса на такива – през текущата бюджетна година; 5 на сто от всички фондове, собствени и чужди, или 100 милиона песети (601 012.10 евро).

Повторението на две или повече много тежки нарушения за период от пет години води при съответните обстоятелства до налагане на санкция за забрана на упражняване на дейността в Испания за максимален срок от две години. Когато решението за тази санкция се потвърди, се известява Регистърът на доставчиците на удостоверителни услуги, за да заличи името на санкционирания доставчик на услуги;

б) за тежки нарушения комисията налага на нарушителя глоба, на стойност до два пъти брутната печалба, получена в резултат на действията или небрежността. В случай че този критерий не може да се приложи или след приложението му се получава стойност, по-малка от най-високата от посочените по-надолу, най-високата стойност определя границата на паричната санкция. За тези цели се определят следните стойности: 0.5 на сто от годишните брутни приходи, получени от организацията нарушител през последната бюджетна година, а в случай че няма такива – през актуалната бюджетна година; 2 на сто от всички фондове, собствени и чужди, или 50 милиона песети (300 506.04 евро);

в) за леки нарушения комисията налага на нарушителя глоба на стойност до два милиона песети (12020.23 евро).

(2) Решението за санкциите на тежките и много тежките нарушения се публикуват в „Държавния официален бюлетин“ и в два вестника с национален тираж, след като то бъде потвърдено.

(3) Стойността на глобите, които се налагат в посочените граници, нараства, като се взема под внимание предвиденото в чл. 131, ал. 3 на Закон № 30 от 1992 г. и следното:

а) тежестта на нарушенията, допуснати преди това от лицето, което се санкционира;

б) отражението на нарушението върху обществото;

в) нанесената щета, винаги когато не е взета под внимание за определяне на нарушението като леко, тежко и много тежко;

г) ползата за нарушителя от предмета на нарушението.

(4) В Регистъра на доставчиците на удостоверителни услуги се отбелязват наложените им санкции с потвърдено решение от комисията за всякакъв вид тежко или много тежко нарушение. Забележките относно санкциите се премахват след изтичане сроковете за давност на предвидените административни санкции в регулиращия Закон за общите административни процедури.

(5) Посочените в този член стойности се актуализират периодично от правителството с кралски указ, като се има предвид изменението на индексите на потребителските цени.

Чл. 27. Предпазни мерки

В наказателните процедури за тежки или много тежки нарушения могат да се предприемат съобразно Закон № 30 от 26 ноември 1992 г. предпазни мерки, които се считат за необходими за гарантиране ефективността на окончателното решение. Тези мерки се изразяват в заповед за временно преустановяване на дейността на доставчика на услуги, преустановяване валидността на издадените от него удостоверения или във вземането на други предохранителни действия, които се считат за необходими. При всички случаи се зачита принципът на пропорционалност на мерките, които се вземат, с цел да се приложи всяко взето решение.

Чл. 28. Наказателна процедура

(1) Упражняването на санкциониращата власт с настоящия кралски указ-закон се предоставя на Главния секретариат за комуникации към Министерството на развитието. Поради това Главният секретариат за комуникации се подчинява на действащите процедури от общ характер за изпълнението на санкциониращи правомощия от държавната администрация.

(2) Министерството на правосъдието и останалите органи, които съгласно този кралски указ-закон и неговите разпоредби имат права за приложение, могат да поискат откриване на наказателно производство с обоснована молба до Главния секретариат за комуникации.

Допълнителна разпоредба

Възможност за емисия от обществените организации за радиоразпространение от дадена автономна област на територията на други, с които имат общи гранични радиоелектронни пространства

Упълномощените автономни области съобразно закона за оказване услугата за цифрово териториално радиоразпространение могат да предават на територията на други автономни области, с които има съседни радиоелектронни пространства. Необходимо е споразумение между засегнатите автономни области и на всяка територия да се използват планираните честотни блокове в Националния технически план за звуково, цифрово и териториално радиоразпространение за автоматичната сфера.

Преходна разпоредба

Доставчици на удостоверителни услуги, регистрирани в Испания преди влизането в сила на настоящия кралски указ-закон

Доставчиците на услуги, регистрирани вече в Испания и чиято дейност се направлява от специална разпоредба, привеждат своята дейност в съответствие с настоящия кралски указ-закон за период от една година от влизането му в сила. Независимо от това удостоверенията, които вече са предизвикали действие, запазват своята валидност.

Заключителни разпоредби

§ 1. Конституционно основание

Настоящият кралски указ-закон се приема на основание на чл. 149, ал. 1, т. 8, чл. 18 и 21 на Конституцията, която дава изключителни правомощия на държавата в областта на гражданското законодателство въз основа на правния режим за държавната администрация и телекомуникациите.

§ 2. Упълномощаване на правителството

Правителството се упълномощава да прилага с наредби предвиденото в настоящия кралски указ-закон.

§ 3. Влизане в сила

Настоящият кралски указ-закон влиза в сила на следващия ден след неговото публикуване в „Държавния официален бюлетин“.

Закон за цифровия подпис, Федерална република Германия

(Резюме)

www.iid.de/iukdg/gesetz/iukdge.html

I. Нормативна уредба

Общата рамка на информационните и комуникационните услуги в Германия е уредена с пакет от закони за регулиране на рамковите условия за информационните и комуникационните услуги[1]. Пакетът включва Закон за телекомуникационните услуги, за защита на личните данни, за цифровия подпис, както и промени в някои действащи нормативни актове.

Законът за цифровия подпис регламентира общите условия, съгласно които цифровият подпис се смята за сигурен и всяко поправяне на цифрово подписани данни може да бъде надеждно установено.

II. Определения

- **Цифров подпис** (digital signature) – набор от електронни данни, създаден с частен ключ и установяващ притежателя на ключа и ненакърнеността на информацията с помощта на съответстващ му публичен ключ, който е предоставен с удостоверение за публичен ключ, издадено от удостоверяваща организация.
- **Удостоверяваща организация** (certification authority) – физическо или юридическо лице, което удостоверява издаването на публичен ключ на физически лица и притежава необходимата лицензия за това.
- **Удостоверение** (certificate) – снабдено с цифров подпис цифрово удостоверение за издаване на публичен ключ на физически лица (удостоверение за ключ) или специално цифрово удостоверение, което, недвусмислено свързано с удостоверението за ключ, съдържа и допълнителна информация (атрибутивно удостоверение).
- **Удостоверяване на време** (time stamp) – цифрово удостоверение, снабдено с цифров подпис, издадено от удостоверяващата организация и удостоверяващо, че определени електронни данни са ѝ били предоставени в даден момент от време.

[1] Законът е в сила от 1 август 1997 г. Правителството на ФРГ приема и Наредба по приложението на закона, която влиза в сила на 1 ноември с. г.

III. Основни положения

Компетентна организация

Издаването на лицензии и удостоверения и надзорът за съблюдаване на разпоредбите на този закон са предоставени на организацията по чл. 66 от Закона за телекомуникациите.

Лицензиране на удостоверяващи организации

За извършване на своята дейност удостоверяващите организации трябва да получат лицензия от компетентната организация. Лицензията се издава след подаване на заявление.

Лицензия може да бъде отказана, когато фактите водят до предположение, че кандидатът не притежава необходимата надеждност за ръководство на удостоверяваща организация или когато кандидатът не предоставя доказателства за това, че притежава специални познания в областта, или когато има основания да се вярва, че със започването на дейността другите изисквания към удостоверяващата организация няма да могат да бъдат изпълнени.

Ръководителите на удостоверяващата организация следва да гарантират спазването на законовите изисквания, регламентиращи дейността на организацията, и следва да притежават необходимата надеждност. Изискванията за специални познания в областта са спазени, когато лицата притежават необходимите знания, квалификация и опит. Другите изисквания относно ръководството на дейността на удостоверяващата организация се смятат спазени, когато компетентната организация е уведомена своевременно относно предприетите мерки и средствата за сигурност, предвидени в този закон и в актовете по приложението му и въвеждането им е било проверено от орган, признат от компетентната организация.

Към лицензията могат да се прикрепят допълнителни клаузи, с цел да се осигури спазване от страна на удостоверяващата организация на всички изисквания на този закон и на актовете по приложението му.

Компетентната организация издава удостовере-

ния за ключ за добавяне на подписа към удостоверението. Условията за издаване на удостоверения от удостоверяващите организации се прилагат съответно и относно компетентната организация. Компетентната организация следва да съхранява удостоверенията, издадени от нея, достъпни за всеки и по всяко време за проверка и отмяна чрез общодостъпни телекомуникационни връзки. Това се отнася също така и за адресите и телефонните номера на удостоверяващите организации, невалидните удостоверения, издадени от компетентната организация, спирането и забраната за извършване на дейност на удостоверяваща организация, както и отмяната и оттеглянето на издадените лицензии.

За публичните услуги, предоставяни по този закон, се дължат такси.

Издаване на удостоверения

Удостоверяващата организация следва да установи надлежно самоличността на лицата, подали заявление за удостоверение. Организацията потвърждава издаването на публичен ключ с удостоверение за ключ на идентифицираното лице. Удостоверението заедно с всички други атрибутивни удостоверения следва да бъде общодостъпно за проверка и при съгласие на притежателя на ключа за отменяне по всяко време чрез общодостъпни телекомуникационни връзки.

По молба на кандидата удостоверяващата организация може да включи в удостоверението за ключ или в атрибутивното удостоверение информация относно пълномощието му да представлява трети лица или относно професионалното му разрешение да практикува или друг вид разрешение дотолкова, доколкото надеждни доказателства са представени за съгласието на третите лица относно пълномощието, представителната власт и разрешението.

По молба на кандидата удостоверяващата организация посочва в удостоверението псевдоним вместо името на кандидата.

Удостоверяващата организация следва да вземе мерки за предотвратяване на подправяне на данните, предназначени за удостоверението. Организацията следва също така да вземе мерки за осигуряване на конфиденциалност на частните ключове. Съхраняването на частни ключове от удостоверяващата организация не се позволява.

Удостоверяващата организация следва да привлече надежден персонал за извършване на дейността си. Относно издаването на удостоверението и ключовете и във връзка с проверката на удостоверенията организацията следва да използва техническите компоненти, предвидени в закона.

Изискване за уведомление

Удостоверяващата организация следва да уведомява кандидатите относно мерките, необходими за поддръжката на сигурността на цифровия подпис и за неговата надеждна проверка и относно техническите компоненти, отговарящи на стандартите, предвидени в този закон.

Съдържание на удостоверението

Удостоверението за ключ трябва да съдържа следната информация:

1. името на притежателя на ключа, което може да съдържа и допълнителна информация в случай на опасност от объркване, или псевдоним, под който авторът е известен;
2. публичния ключ;
3. алгоритмите, с които се използва както публичния ключ на притежателя на ключа, така и публичният ключ на удостоверяващата организация;
4. сериен номер на удостоверението;
5. начало и край на срока на валидност на удостоверението;
6. име на удостоверяващата организация;
7. указания дали използването на публичния ключ е било ограничено по вид и обсег относно конкретни приложения.

Информация относно правото да се представлява трето лице, правото за професионални или други разрешения, да се упражнява определена професия може също да бъде включена в удостоверението или в атрибутивното удостоверение.

Друга информация не следва да се включва в удостоверението, освен ако страните не са дали своето съгласие за това.

Прекратяване на действието на удостоверението

Удостоверяващата организация следва да прекрати действието на удостоверението, ако притежателят на ключа или негов представител поиска това, когато удостоверението е било издадено въз основа на невярна информация, когато удостоверяващата организация престане да действа и нейната дейност не е продължена от друга удостоверяваща организация или когато прекратяването на удостоверението е обявено от компетентната организация. При прекратяването следва да се посочва точният момент, от който то влиза в сила. Прекратяване на удостоверението с обратно действие е недопустимо.

Когато удостоверението съдържа информация за трета страна, тя също има право да иска неговото

прекратяване.

Компетентната организация прекратява удостоверенията, издадени от нея, когато съответната удостоверяваща организация прекрати дейността си или лицензията ѝ е оттеглена или отменена.

Удостоверяване на време

При молба удостоверяващата организация следва да приложи печат към електронните данни за удостоверяване на времето.

Документация

Удостоверяващата организация следва да състави документация на мерките за сигурност по този закон, наредбата за приложението му и издадените удостоверенията по начин, по който данните и тяхната ненакърненост да могат да се проверяват по всяко време.

Преустановяване на дейността

При преустановяване на дейността си удостоверяващата организация съответно следва да уведоми компетентната организация в най-кратък срок и да осигури предаването на удостоверенията, валидни по време на прекратяване на организацията на друга удостоверяваща организация или да ги прекрати.

Удостоверяващата организация следва да изпрати документацията на съответната организация, която ще поеме дейността ѝ, или съответно на компетентната организация.

Компетентната организация трябва да бъде незабавно уведомена в случай на искане за обявяване в несъстоятелност или на помирително производство.

Защита на данните

Удостоверяващата организация може да събира лични данни само директно от съответното лице и само доколкото са необходими за целите на удостоверението. Събирането на данни от трети лица е позволено само при съгласие на лицето, за което се отнасят. Данните могат да бъдат използвани за цели, различни от посочените в първото изречение, ако това е позволено в този закон или в друга правна разпоредба или ако страната, за която те се отнасят, е дала своето съгласие.

В случай че притежателят на ключа използва псевдоним, удостоверяващата организация е задължена да предоставя на съответните институции информация за идентичността му, доколкото това е изискуемо за разкриване на престъпления и административни нарушения, за опасност от нарушаване на обществения ред или за изпълнение на законовите задължения на федералните и провинциалните служби за защита на Конституцията (Bundesnachrichtendienst), военните служби за разследване (Militaerischer Abschirmdienst) и митническите органи (Zollkriminalamt). Такова разкриване на информация следва да бъде документирано. Институцията, изискваща информация, следва да уведоми притежателя на ключа за разкриване на псевдонима му веднага, щом това не влиза в противоречие с изпълнението на законовите ѝ задължения или в случай, че има преобладаващ интерес за притежателя на ключа да получи тази информация.

Федералният Закон за защита на данните се прилага, доколкото е допустимо предприемането на проверки, когато няма данни за нарушаване на разпоредбите за защита на данните.

Контрол и прилагане на задълженията

Компетентната организация може да предприеме мерки спрямо удостоверяващите организации, за да осигури пълно прилагане на този закон и на правилника по приложението му. По-специално може да забрани използването на ненадеждни технически средства и може временно, изцяло или частично, да прекрати дейността на удостоверяващата организация.

За осъществяване на контролните си функции удостоверяващата организация следва да допуска компетентната организация да влиза в местата и офисите, в които се извършва дейността ѝ в рамките на нормалния работен ден, да предоставя цялата необходима документация и информация и да оказва необходимото съдействие. Лицата, задължени да предоставят информация, могат да откажат да отговарят на въпроси, които биха уличили тях или лица, с които са в кръвна връзка в нарушение на Закона за административните нарушения. Лицата, задължени да предоставят информация, следва да бъдат уведомени за това си право.

В случай че удостоверяващите организации не спазват изискванията, залегнали в този закон или в подзаконов акт, или в случай на наличие на основания за отнемане на лицензията, компетентната организация следва да отмени лицензията, ако се очаква, че прилагането на горепосочените мерки ще бъде неуспешно.

В случай на оттегляне или отмяна на лицензията или прекратяване на дейността на удостоверяващата организация компетентната организация следва да осигури прехвърляне на дейността ѝ към друга удостоверяваща организация или да прекрати договорите, сключени с притежателите на публични ключове. Това се отнася и за случаите, когато има искане за обявяване в несъстоятелност или помирително производство и лицензираната дейност не бъде продължена.

Правната валидност на удостоверенията, издадени от удостоверяващата организация, остава незасегната от оттеглянето или отмяната на лицензията. Компетентната организация може да обяви за недействителни удостоверенията, когато фактите сочат, че те са били подправени или не са били адекватно защитени срещу подправяне, или когато техническите средства, използвани за подписа, разкриват възможност цифровите подписи да бъдат подправени или подписаните данни манипулирани, без това да бъде разкрито.

Технически компоненти

Технически компоненти за защита са необходими за създаване и съхраняване на публични ключове и за генериране и проверка на цифрови подписи. Техническите компоненти надеждно разкриват подправените цифрови подписи и поправката на подписаните данни и осигуряват защита срещу неоторизирано използване на информацията.

За представяне на данни, които следва да се подпишат, са необходими технически компоненти за защита, които предварително и ясно установяват генерирането на цифровия подпис и позволяват идентифициране на данните, към които той се прикрепва. Те позволяват да се провери дали подписаните данни са непроменени, към кои данни се отнася цифровият подпис и на кой притежател на ключ принадлежи цифровият подпис.

При техническите компоненти, които позволяват отмяна, са необходими и предварителни мерки, които да предпазват регистрите на удостоверения от неправомерна промяна и отмяна.

Техническите компоненти следва да се тестват съгласно съвременните технически стандарти и съответствието им с тези стандарти трябва да се потвърди от организация, призната от компетентната организация.

Приема се, че техническите компоненти, валидно приети в страните от ЕС или в страните от ЕИП (Европейското икономическо пространство), осигуряващи същата степен на защита, съответстват на техническите компоненти за защита съгласно изискванията на този закон.

Удостоверения, издадени в други държави

Цифров подпис, подлежащ на проверка чрез публичен ключ, издаден в друга държава – членка на ЕС или на Европейското икономическо пространство, следва да има правната сила на цифровия подпис, издаден съгласно този закон, в случай че предвижда същото ниво на сигурност.

Това правило се отнася и за държавите, с които са сключени съответни международни споразумения.

Подзаконова уредба

Възлага се на федералното правителство да приеме подзаконова уредба относно:

1. подробностите във връзка с процедурите по издаване, оттегляне и отмяна на лицензията и процедурите относно прекратяване на дейността на удостоверяващата организация;
2. таксите за извършваните услуги и техния размер;
3. задълженията на удостоверяващата организация;
4. срока на действие на издадените удостоверения;
5. контрола върху удостоверяващите организации;
6. изискванията относно техническите компоненти, тестването им и потвърждаването, че установените изисквания са изпълнени;
7. периода на поставяне на нов цифров подпис и съответната за това процедура.

В закона са включени промени в съответните разпоредби на Наказателния кодекс и на Закона за административните нарушения, съгласно които базата данни, свързана с цифрови подписи и цифрови данни, се приравнява на писан документ.

Закон за електронните комуникации, Великобритания

(Резюме)

www. parliamentary.the stationery-office.co.uk

I. Приложно поле

Основна цел на закона е да изгради доверие в електронната търговия по пътя на правното признаване на електронния подпис и премахването на съществуващите в законодателството пречки относно използването на електронна комуникация и съхраняването на данни, както и чрез регламентиране на процедурите по одобряване на схеми на организации, предоставящи криптографски услуги.

Законът за електронните комуникации се състои от три части:

Част първа – регламентира регистрацията и дейността на доставчиците на криптографски услуги, например такива по създаване на електронни подписи.

Част втора – регламентира начините за улесняване на електронната търговия и съхраняването на данни. Съдържа разпоредби относно правното признаване на електронния подпис, улесняващо електронната комуникация и електронното съхраняване на данни като алтернатива на традиционните средства за комуникация и съхранение.

Част трета – посветена е на телекомуникационните лицензии и изменението им, съдържа общи тълкувателни разпоредби, дефиниции и териториално действие на закона.

II. Определения

- **Документ** (document) – понятие, което включва карта, план, дизайн, рисунка, снимка или други изображения.
- **Комуникация** (communication) – комуникация, включваща звуци, образи или и двете, както и комуникация за извършване на плащане.
- **Електронна комуникация** (electronic communication) – информация, предавана от едно лице на друго, от един механизъм към друг, от лице към механизъм или обратно чрез телекомуникационна система по смисъла на *Закона за телекомуникациите от 1984* г. или по всякакъв друг начин в електронна форма.
- **Криптографска услуга** (cryptography support services) – всяка услуга, извършена на изпращача или получателя на електронната комуникация или на лицата, съхраняващи електронни данни, и създадена, за да улесни използването на криптографски способи, както и с цел да гарантира, че:
  1. определена комуникация или данни са достъпни или могат да се трансформират в ясна и четлива форма само от определени лица;
  2. автентичността и ненакърнеността на комуникацията или данните могат да бъдат точно определени.
- **Електронният подпис** (electronic signature) по смисъла на този закон е изявление в електронна форма,
  1. включено или логически свързано с дадена електронна комуникация или електронни данни;
  2. инкорпорирано или асоциирано, с цел да бъде използвано за установяване на автентичността или ненакърнеността на комуникацията и данните или и на двете.
- **Изменение** (modification) – всяко изменение, добавяне или отпадане, както и включване на сродни изрази.
- **Запис** (record) – включва електронен запис.
- **Вторично законодателство** (subordinate legislation) – всяко вторично законодателство по смисъла на Закона за тълкуването от 1978 г., всеки акт, приет от Парламента на Шотландия, както и всяко законово правило, по смисъла на Наредбата за законовите правила на Северна Ирландия от 1979 г.
- **Автентификация на комуникацията или данните** (authenticity of communication or data) – е означение:
  1. дали определена комуникация или данни произлизат от определено лице или друг източник;
  2. дали правилно са означени датата и времето;
  3. дали са предназначени да имат правно действие.
- **Ненакърненост** (integrity) на комуникацията или данните е индикация относно това, дали е имало неправилна употреба или друго изменение на комуникацията или данните.
- **Четлива форма** (intelligible form) – възвръщане

в положението, съществуващо преди извършеното криптиране или сходно с него действие.

- **Ресорен министър** (the appropriate minister) – в част II на закона съответен е:
  1. държавният секретар (the Secretary of State) за всеки въпрос, свързан с Държавния секретариат;
  2. министърът на финансите за всеки въпрос, свързан с Министерството на финансите;
  3. ресорният министър за всеки друг въпрос, свързан с правителствена структура, която не е Държавният секретариат или Министерството на финансите.

III. Основни положения

Част първа. Доставчици на криптографски услуги

Държавният секретар създава и поддържа регистър на одобрените доставчици на криптографски услуги. Той следи регистърът да съдържа информация за всеки доставчик, получил одобрение и при вписването в регистъра да се отразява следната информация:

1. име и адрес на лицето;
2. услугите, за които лицето е получило одобрение;
3. условия за получаване на одобрението.

Държавният секретар следва да контролира валидността на издадените одобрения и да осигурява достъп на обществеността до регистъра. Всяко изменение в одобрението или оттегляне на одобрението следва да може да бъде достъпно за заинтересованите лица[1].

Издаване на одобрения

Държавният секретар отговаря за наличието на правила за издаване на одобрения, които:

1. осъществяват криптографски услуги във Великобритания или предлагат да започнат осъществяването им;
2. кандидатстват за издаване на одобрение за която и да е криптографска услуга, която те осъществяват или предлагат да започнат да осъществяват, в пределите или извън пределите на Великобритания.

Правилата за издаване на одобрение следва да:

1. позволяват издаване на одобрение за всички услуги, за които се иска одобрение, или само за част от тези услуги;
2. осигуряват възможност на лицето, което иска издаване на одобрение, да откаже одобрението, ако то съдържа различни условия от тези, искани от него;
3. позволяват издаване на одобрение по отношение на всички услуги само на лицата, които спазват техническите изисквания и са в състояние да спазват всички други изисквания, предписани от главния секретар като условия за издаване на одобрения;
4. включват правила относно обжалването на отказ за издаване на одобрения.

Делегиране на функциите по издаване на одобрения

Държавният секретар може да делегира функциите си по издаване на одобрения (без тези по издаване на правила) на друго лице. Делегирането се публикува, за да се доведе до знанието на заинтересованите лица. Всяка отмяна на извършено делегиране също се публикува.

Ограничения във връзка с разкриването на информация

Законът съдържа разпоредби за защита на личната и бизнес информация. Разкриването ѝ е оправдано само в определени случаи, като например при разследване на извършено престъпление. Законът предвижда и отговорност за лицата, неправомерно разкриващи информация.

Част втора. Улесняване на електронната търговия и електронния подпис

При правен спор:

1. електронният подпис, поставен или логически свързан с дадена електронна комуникация или електронни данни и
2. удостоверяване от всяко лице на електронен подпис се приемат за доказателство на всеки въпрос, свързан с автентификацията и ненакърнеността на комуникацията или данните[2].

Електронният подпис, включен или свързан с дадена електронна комуникация или електронни данни, е удостоверен от всяко лице, което преди или след извършване на комуникацията, е удостоверило или самия подпис, или начина на създаване на подписа или процедурата, приложена към него, като валидно средство за установяване на автентичността и/или ненакърнеността на комуникацията и данните.

[1] Целта на регистъра е да се осигури, че доставчиците на услуги са получили обективна оценка по отношение на изискваните стандарти за качество. Регистърът не е задължителен и доставчиците не са задължени да кандидатстват за одобрение и ако не са вписани в регистъра, те са свободни да извършват криптографски услуги (House of Commons – Explanatory Notes).

[2] Съдът решава във всеки конкретен случай дали електронният подпис е бил коректно използван и каква доказателствена стойност следва да има, напр. във връзка с автентичността и ненакърнеността на информацията спрямо други доказателства (House of Commons – Explanatory Notes).

Промяна в законодателството

Ресорният министър може да извърши промени във вторичното законодателство[3] и в съществуващите схеми, лицензии и оторизации, с цел да се установи или улесни използването на електронната комуникация или електронното съхранение на данни при постигането на следните цели:

1. извършване на всичко, което съгласно тези разпоредби може да се направи писмено или чрез съставяне на документ или известие;
2. извършване на всичко, което съгласно тези разпоредби може да се изпрати по пощенски път или чрез други средства за доставка;
3. извършване на всичко, което съгласно тези разпоредби следва или може да се удостовери с подписа на лицето или неговия печат, или изисква присъствие;
4. извършване на всичко, което съгласно тези разпоредби следва да бъде направено под клетва или да бъде включено в декларация;
5. събиране, съхраняване и публикуване съгласно тези разпоредби на всякаква информация;
6. извършване на всяко плащане, което следва и може да се направи съгласно тези разпоредби.

Актовете на министъра съгласно закона следва да се потвърдят или отхвърлят от двете камари на Английския парламент.

[3] Правомощието да променя законодателството, предоставено на министъра, цели премахването на всички пречки, съществуващи в законодателството, относно използването на електронната търговия и регулирането на електронната комуникация и съхранението на електронни данни там, където това е позволено, както и поради факта, че в законодателството съществуват много разпоредби, които изискват наличието на хартиена документация като случаите на комуникация между държавни органи и представители на бизнеса или между представители на бизнеса и отделния индивид и други законови изисквания комуникацията да е на хартиен носител. Правомощието следва да се използва селективно, за да се предостави възможност за електронна алтернатива на тези, които искат да я използват. От друга страна, има и много случаи, като например голяма част от договорите, в които няма изисквания за извършване на комуникация на хартиен носител. В тези случаи лицата са свободни да използват такава форма, каквато те пожелаят.

Законопроект за цифровия подпис, Дания

(Резюме)

www.mbc.com./ecommerce/legis/denmark.html

I. Цели и приложно поле

Като главни цели на законопроекта на Дания за цифровия подпис са посочени:

1. увеличаване на ефективното и сигурно използване на електронната комуникация;
2. осигуряване на еднакво третиране на възможностите за използване на цифрова комуникация и комуникация, извършвана на хартиен носител;
3. необходимост от създаване на условия за цифров обмен на информация между държавните органи и гражданите.

II. Определения

В законопроекта са дадени следните по-важни определения:

- **Двойка ключове** (key pair) за цифров подпис – частен и публичен криптографски ключ, независими по начина, по който цифровото съобщение, което може да бъде декодирано чрез общодостъпен ключ, може единствено да бъде закодирано чрез частен криптографски ключ.
- **Удостоверение** за двойка ключове (key certificate) – електронно удостоверение, в което се декларира, че общодостъпният криптографски ключ от дадена двойка принадлежи на определено физическо или юридическо лице.
- **Цифров подпис** (digital signature) – числова стойност, генерирана при закодиране на цифровото съобщение чрез система за цифров подпис и частен криптографски ключ.
- **Удостоверяваща организация** (certification authority) – физическо или юридическо лице, което издава и публикува удостоверения за цифров подпис.
- **Титуляр на ключа** (keyholder) – физическо или юридическо лице, сключило договор с удостоверяваща организация за издаване на удостоверение за ключ.
- **Удостоверяване на време** (time stamp) – изявление, удостоверяващо, че дадено електронно съобщение е съществувало в даден момент от време.
- **Оторизирана удостоверяваща организация** (authorized certification authority) – физическо или юридическо лице, което е оторизирано от Националната телекомуникационна агенция да:
  1. издава оторизирани удостоверения;
  2. издава удостоверения за оторизиран цифров подпис.
- **Оторизирано удостоверение за ключ** (authorized key certificate) – удостоверение, издадено от оторизирана удостоверяваща организация, което отговаря на минималните изисквания за оторизирано удостоверение, предвидени в този закон и в актовете по приложението му.
- **Удостоверение за оторизиран цифров подпис** (key certificate for authorized digital signature) – оторизирано удостоверение, при което криптографските ключове и системи за поставяне на цифров подпис отговарят на минималните изисквания за оторизиран цифров подпис.

III. Основни положения

Законопроектът предвижда три алтернативни метода, целящи осигуряване на еднаквото правно третиране на електронната комуникация с тази, осъществявана на хартиен носител, по отношение на формалните изисквания в нормативните и в индивидуални административни актове. Намерението е при обсъждане на закона да се постигне решение за възприемане на един от трите модела:

1. Модел на изключителност (The Exceptional Model)

В случай че нормативни актове, разпоредби или правилници изискват съобщението да бъде в писмена форма или да бъде подписано, то тя се смята за спазена, когато съобщението е оформено като електронно съобщение с оторизиран цифров подпис.

2. Модел на включване (The Inclusion Model)

По административен ред може да бъде установено, че там, където законовите и административните разпоредби съдържат изисквания съобщението да бъде в писмена форма или да бъде подписано, то тези изисквания се смятат за спазени от

електронното съобщение с оторизиран цифров подпис.

3. Комбиниран модел (The Combination Model)

Комбинация от модела на изключителност и модела на включване.

Титулярят на удостоверението може да се обърне към удостоверяващата организация да спре действието на удостоверението. Спирането влиза в сила след обявяването му от удостоверяващата организация и въз основа на него електронното съобщение и цифровият подпис не пораждат правни последици.

Удостоверението може да бъде валидно за определен срок от време. Електронно съобщение и цифров подпис, направени след изтичането на този срок, не пораждат правни последици.

Ако електронното съобщение излиза извън приложното поле, указано в удостоверението, то също не може да има правно валиден ефект.

Удостоверяващата организация по молба на адресата предоставя информация относно спирането на действието на удостоверението, срока на неговото действие и ограниченията в приложното поле на действие на удостоверението.

Удостоверяващата организация е задължена да предоставя информация на всеки желаещ относно условията и реда за издаване на удостоверения, правилата за установяване на самоличността на титуляря на ключа, вътрешните процедури за сигурност на удостоверяващата организация, начина на използване на цифров подпис, уведомления от страна на титуляря на ключа при неправомерно използване.

Удостоверяващата организация се задължава да не използва **личните данни**, предоставени ѝ от титуляря на ключа за цели, различни от дейността на организацията.

Надзор върху дейността на удостоверяващите организации се упражнява от Националната телекомуникационна агенция на Дания.

Жалби срещу решенията на Националната телекомуникационна агенция се подават пред Апелативния съвет, назначен от министъра на изследванията и информационните технологии. Апелативният съвет се състои от председател, който трябва да има квалификация на върховен съдия, и четирима членове, които да отговарят, респективно за техническите, финансовите въпроси и защитата на потребителя. Мандатът на членовете на Апелативния съвет е три години с възможност за преизбиране. Решенията на Съвета на Европейския съюз не могат да бъдат обжалвани пред друг административен орган, а само пред съдилищата в срок от 6 седмици от оповестяване на решението на страните.

Законопроект за електронния подпис[1], Чехия

(Превод със съкращения)

www.vip.fce.vutbr.cz/commerce/

Парламентът гласува следния закон на Република Чехия:

§ 1. Цел на закона

Целта на настоящия закон е да регулира използването на електронния подпис.

§ 2. Прецизиране на някои понятия

За целите на този закон се разбира:

1. „**Електронен подпис**“ – данни в електронен вид, които са присъединени към или логически свързани с електронно съобщение и които са използвани за установяване на идентичността на правоспособното лице във връзка с електронното съобщение.
2. „**Гарантиран електронен подпис**“ – електронен подпис, който изпълнява следните изисквания:
   а) по отношение собственика на подписа е еднозначен;
   б) дава възможност за идентификация на правоспособното лице във връзка с електронното съобщение;
   в) създаден е и е присъединен към електронното съобщение по начини, които са под контрола на правоспособното лице.
3. „**Електронно съобщение**“ – информация, която е създадена, пренесена, приета или запазена с електронни, оптични или други подобни средства, както и с други средства, позволяващи пренос на информация на разстояние.
4. „**Организация за електронни подписи**“ (нататък само организация) – орган на държавното управление, подчинен на Министерството на транспорта и съобщенията, натоварен с изпълнението на държавното управление в областта на електронните подписи и проверителите на информация съгласно този закон. Начело на организацията стои председател, назначаван и освобождаван от министъра на транспорта и съобщенията.
5. „**Правоспособно лице**“ – физическо лице, което е създало гарантиран електронен подпис.
6. „**Проверител на информация**“ – субект, който удостоверява връзката между гарантирания електронен подпис и правоспособното лице и е натоварен за това от организацията.
7. „**Удостоверяване**“ – електронно съобщение или друг запис, който е издаден от проверителя на информация и чиято цел е да установи идентичността на лицето, подписало електронното съобщение с гарантиран електронен подпис.

§ 3. Съответствие с изискванията към подписа

1. Електронното съобщение е подписано, в случай че е снабдено с електронен подпис.
2. Гарантираният електронен подпис гарантира, че електронното съобщение е подписано от правоспособно лице.

§ 4. Съответствие с изискванията към оригинала

Използването на гарантиран електронен подпис осигурява ненакърненост на съдържанието на електронното съобщение от момента, когато е било подписано.

§ 5. Гарантирани електронни подписи

Условията, които електронният подпис трябва да изпълнява, за да бъде гарантиран, се определят от Министерството на транспорта и съобщенията с нареждане.

§ 6

Страните могат да се договорят, че електронните подписи във взаимните им отношения се приемат за гарантирани електронни подписи.

§ 7. Задължения на правоспособното лице

1. Правоспособното лице е задължено:
   а) да използва електронния подпис с дължимата грижа така, че да не се стигне до неговото неправомерно използване;
   б) да уведоми незабавно проверителя на информация, в случай че има опасност от злоупотреба с неговия гарантиран електронен подпис;
   в) да осигури цялата информация във връзка с гарантирания електронен подпис, споделена от проверителя на информация или от друг субект като точна, истинна и пълна.
2. За нарушаване на задълженията по ал. 1 правоспособното лице отговаря според особените

[1] Вариант V от 18 септември 1999 г.

правила.[2] Отговорността обаче може да бъде снета, в случай че се докаже, че този, за когото са възникнали щети, не е извършил всички действия, необходими, за да се увери, че гарантираният електронен подпис е валиден и неговото удостоверение не е отнето.

§ 8. Задължения на проверителите на информация

1. Проверителят на информация е задължен:
   а) да предприеме действия, необходими за определяне самоличността на правоспособното лице и на всички други факти или данни, които проверителят на информация проверява;
   б) да осигури щото всеки да може да се увери в:
   - самоличността на проверителя на информация;
   - методиката, използвана за определяне самоличността на правоспособното лице;
   - условията, изключващи използването на гарантиран електронен подпис;
   - това, дали удостоверението не е било анулирано и дали с подписа не е злоупотребено;

   в) да съобщи на правоспособното лице начина, по който трябва да извести проверителя на информация при заплаха от злоупотреба с подписа;
   г) да осигури щото цялата информация, отнасяща се до отношенията, свързани с гарантирания електронен подпис, която ще съобщи на друг субект, да бъде точна, истинна и пълна.
2. При нарушаване на задълженията по ал. 1 проверителят на информацията отговоря според особените разпоредби.[3]

§ 9. Защита на личните данни на гражданите

Защитата на личните данни се определя в специален закон.[4]

§ 10. Организация

1. Издаването на разрешение за дейност като проверител на информация, както и надзорът върху спазването на този закон принадлежат на организацията.
2. Организацията:
   а) издава и отнема разрешението за дейност като проверител на информация, когато става дума за субект, действащ на територията на Република Чехия;
   б) наблюдава дейността на проверителите на информация, поставя задачи за корекции и налага глоби за нарушаване на задълженията от притежателите на разрешения;
   в) води регистър на издадените разрешения и на промените в тях;
   г) периодично публикува преглед на молбите за разрешения и преглед на издадените разрешения, като това става по начин, който позволява достъп до тях от разстояние.
3. С цел осъществяване на надзор проверителят на информация е задължен да позволи достъп на организацията до търговските и работните помещения, при поискване да предостави цялата документация, записи, документи, писмени материали и други изходни материали, да позволи достъп до информационната система на проверителя на информация и да предостави информация за цялата необходима съпътстваща дейност.
4. Ако не е определено друго в този закон, организацията се ръководи при извършването на надзора от специални норми.[5]

§ 11. Проверител на информация

1. Да извършва дейност като проверител на информация може само този, на когото е издадено разрешение от организацията.
2. Към молбата за разрешение по ал. 1 молителят трябва да приложи:
   а) търговското наименование и седалището на проверителя на информация;
   б) размера на основния капитал;
   в) предметни, персонални и организационни предпоставки за дейност като проверител на информация съгласно този закон;
   г) документи относно актуалното състояние на проверителя на информация[6], които не трябва да са по-стари от три месеца;
   д) свидетелство за съдимост на молителя физическо лице или представители на юридическо лице съгласно устава, не по-старо от три месеца;
   е) документация за безопасност съгласно този закон;
   ж) документ за платена такса.[7]
3. В случай че молбата не съдържа всички необходими реквизити, организацията поканва молителя да я допълни в определения за това срок. В случай че молителят не стори това в посочения срок, организацията спира разглеждането.

[2] Закон № 40 от 1964 г. от Сборник граждански закони, граждански кодекс по смисъла на последващото законодателство.
[3] Пак там.
[4] Закон № 256 от 1992 г. за защита на личните данни в информационните системи.
[5] Закон № 552 от 1991 г., закон за държавен контрол по смисъла на последващото законодателство.
[6] Разрешение за предприемаческа дейност, препис от търговския регистър или друг документ.
[7] Закон № 368 от 1992 г., закон за държавните такси по смисъла на последващото законодателство.

4. Организацията може да поиска от молителя да допълни молбата си и с други данни, необходими за определяне на способността му да извършва дейност като проверител на информация и евентуално да извършва проверки на място.
5. Проверителят на информация трябва да има седалище на територията на Република Чехия.
6. Освен дейностите, описани в настоящия закон, проверителят на информация може да извършва дейност без съгласието на организацията само като адвокат, нотариус или експерт.[8]
7. Съставна част на издаденото разрешение е заверката от организацията на гарантирания електронен подпис на проверителя на информация.
8. Министерството на транспорта и съобщенията издава разпореждане, в което определя детайлите относно предметните, персоналните и организационните предпоставки за осъществяване на дейност като проверител на информация и относно съдържанието на документацията за безопасност.

§ 12. Удостоверяване на гарантирания електронен подпис

1. Проверителят на информация издава на правоспособните лица удостоверение за техния гарантиран електронен подпис.
2. Преди издаването на удостоверението съгласно ал. 1 проверителят на информация трябва със сигурност да установи идентичността на правоспособното лице. Удостоверението трябва да бъде подписано с електронния подпис на проверителя на информация.
3. Проверителят на информация трябва да ограничи използването на неправилни данни за издаването на удостоверение. Той е задължен незабавно да преустанови валидността на удостоверението, в случай че правоспособно лице помоли за това или в случай че удостоверението е било издадено въз основа на неверни данни.
4. В случай на решение на организацията по § 14, ал. 2 проверителят на информация е задължен да получи описа на правоспособните лица.
5. Проверителят на информация е задължен да предприеме такива мерки, които да осигурят на правоспособното лице възможност по всяко време да блокира удостоверението или да прекрати неговата валидност. При това правоспособното лице трябва да се идентифицира по такъв начин, че да няма възможност за злоупотреба при блокирането или прекратяването на валидността на удостоверението от неправоспособно лице.
6. За всички дейности на проверителя на информация трябва да се води работна документация, която да съдържа следните данни:
   а) договор за издаване на удостоверение на правоспособно лице;
   б) издадени удостоверения;
   в) копие на представените лични документи за идентичност на правоспособното лице;
   г) потвърждение за приемане на гарантирания електронен подпис от правоспособно лице, включително времето на връчване;
   д) точно определяне периода на валидност на издаденото удостоверение;
   е) собствен гарантиран електронен подпис.
7. Записите, които се съхраняват в електронен вид, трябва да бъдат подписани с електронен подпис. Документацията трябва да бъде съхранявана за срок, не по-малък от пет години от времето на издаване на удостоверението и през цялото това време трябва да е съхранена по начин, че до нея да има достъп.
8. Проверителят на информация трябва да регистрира издадените удостоверения в обществено достъпен регистър, който да осигурява достъп от разстояние.
9. В случай на блокиране или прекратяване на валидността на удостоверението този факт трябва видимо да бъде отбелязан в регистъра на удостоверенията, включително и с точно времево обозначение (дата, час, минута) на осъществяване на съответния факт.
10. Техническите компоненти, които проверителят на информация може да използва за изпълнение на дейността си, се определят от Министерството на транспорта и съобщенията с нареждане.

§ 13. Съдържание на удостоверението

1. Удостоверението по § 12 трябва да съдържа следните данни:
   а) името на правоспособното лице, което в случай на възможна замяна трябва да бъде снабдено с добавка или с псевдоним, присъединен към правоспособното лице като незаменяем, който трябва да е обозначен като такъв;
   б) електронно съобщение, служещо за заверка на електронния подпис;
   в) означение на начина, по който е възможно да се завери гарантираният електронен подпис на правоспособното лице, както и гарантираният електронен подпис на проверителя на информация;

[8] Закон № 85 от 1996 г., закон за адвокатурата, Закон № 358 от 1992 г., закон за нотариусите и техните дейности (правилник за нотариусите) по смисъла на последващото законодателство, Закон № 36 от 1967 г., закон за експертите и преводачите.

г) номер на удостоверението – уникален при дадения проверител на информация;

д) начало и край на валидността на удостоверението;

е) името на проверителя на информация; и

ж) данни за това, дали ползването на гарантиран електронен подпис се ограничава според характера и обема само за конкретен случай.

2. Други данни удостоверението може да съдържа само с разрешението на правоспособното лице.

§ 14. Задължения на проверителя на информация при приключване на дейността

1. Проверителят на информация трябва да съобщи на организацията намерението да приключи дейността си най-малко три месеца преди планувaната дата и следва да положи всички възможни усилия за това валидните свидетелства да бъдат поети от друг проверител на информация. Проверителят на информация освен това трябва да информира всяко правоспособно лице за намерението си да приключи с дейността си най-малко два месеца предварително. Той трябва да съобщи името на проверителя на информация, който ще поеме управлението на неговото удостоверение за гарантиран електронен подпис. Във връзка с предаването на удостоверението на друг проверител на информация трябва да бъде предадена също съответната документация по § 13 от закона.
2. Ако проверителят на информация не може да осигури друг проверител на информация да поеме валидните удостоверения, то той е задължен своевременно да уведоми организацията за това. В такъв случай организацията решава кой проверител на информация ще приеме валидните удостоверения и съобщава това на правоспособните лица.

§ 15. Мерки за корекция

1. Ако организацията установи, че проверителят на информация нарушава задълженията, определени от настоящия закон или разрешението по § 11, му възлага в определен срок да извърши корекции и евентуално определя какви мерки е задължен да предприеме.
2. В случай на по-сериозни нарушения на задълженията организацията може изцяло или отчасти да забрани дейността на проверителя на информация за определен период или да му отнеме разрешението да извършва дейност като проверител на информация.
3. Ако организацията вземе решение за отнемане на разрешението, тя същевременно е задължена да осигури прехвърляне на извършената до този момент дейност от засегнатия проверител на информация към друг проверител на информация или по друг начин да осигури изпълнението на договора между проверителя на информация, който приключва дейността си, и правоспособното лице. Валидността на удостоверенията, издадени от проверителя на информация, който приключва дейността си, остава незасегната от отнемането на разрешението.

§ 16. Анулиране на удостоверението

1. Организацията може да нареди на проверителя на информация анулиране на удостоверението за гарантиран електронен подпис, в случай че съществува обосновано предположение, че удостоверението е било подправено, или в случай че е било издадено въз основа на неверни данни. До анулиране на удостоверението може да се стигне също, когато удостоверенията не са достатъчно сигурни или се ползват технически компоненти, показващи недостатъци в безопасността, които биха дали възможност за подправка на гарантирания електронен подпис или промяна на подписаните данни.
2. Регистърът на удостоверенията трябва да съдържа точни времеви обозначения откога удостоверението е било анулирано. Анулираните удостоверения не трябва да се пускат повторно в действие и да се ползват.

§ 17. Признаване на задгранични удостоверения

1. Удостоверения, издадени от чуждестранни проверители на информация, могат да бъдат използвани за целите на този закон, ако са признати от проверител на информация, действащ според този закон, като той гарантира в същия обем, както и в своите удостоверения правилността на удостоверението, също както и неговата правна валидност.
2. Удостоверенията, издадени от чуждестранен проверител на информация, се признават като удостоверения, издадени от проверител на информация, действащ съгласно този закон, в случай че обичайните методи на чуждестранните проверители на информация осигуряват ниво на надеждност, поне еквивалентно на това, което се изисква от проверителя на информация по този закон, и това произтича от решението на организацията или от международните договори или в случай, че между съответния задграничен орган или задграничен проверител на информация и Министерството на транспорта и съобщенията е сключен договор за взаимно признаване на удостоверенията.

§ 18. Технически и програмни компоненти

1. При използването на гарантирани електронни подписи могат да се ползват само такива технически и програмни компоненти, които надеждно ще гарантират, че е невъзможна неправомерна промяна на гарантирания електронен подпис или електронното съобщение, и имат дял в защитата от неправомерно ползване на гарантираните електронни подписи. Тези компоненти трябва еднозначно да разпознаят към какви данни и към кое правоспособно лице се отнася гарантираният електронен подпис.
2. За осигуряване на надеждност при използването на компонентите трябва да има достатъчен контрол. Техническите и програмните компоненти, които са създадени зад граница, за нуждите на този закон се подлагат на проверка и се признават, в случай че техническите им параметри изпълняват същата мярка за надеждност както техническите и програмните компоненти, определени от настоящия закон и правилника за приложението му.
3. Техническите и програмните компоненти, които позволяват да се провери или създаде гарантиран електронен подпис, трябва да съдържат в себе си такива мерки за безопасност, че да не е възможно да се стигне до злоупотреба.

§ 19. Глоби

1. С глоба в размер на 10 000 000 (десет милиона) чешки крони се наказва проверител на информация, който наруши задълженията, възложени му с този закон.
2. В случай че проверителят на информация в срок от една година от датата, когато е влязло в сила решението за глоба, наруши повторно задълженията, възложени му от този закон, може да му бъде наложена глоба в размер до 20 000 000 (двадесет милиона) чешки крони.
3. Проверител на информация, който пречи на контрола, извършван от организацията, може да бъде наказан с редовна глоба в размер до 1 000 000 (един милион) чешки крони, при това и повторно.
4. На лице, което, макар и от немарливост, не предостави на организацията при извършване на контрол необходимото съдействие, може да бъде наложена глоба в размер до 25 000 чешки крони, при това и повторно.
5. При определяне размера на глобата се обръща внимание преди всичко на начина на поведение, степента на вината и периода на продължителност на неправомерното поведение.
6. Глоба може да се наложи до една година от датата, когато съответният орган е установил нарушението на задълженията, но най-много до три години от датата, на която се е стигнало до нарушение на задълженията.
7. Глобата се събира от органа, който я е наложил, или от организацията за електронни подписи. Глобата се изисква от териториалния финансов орган според специални разпоредби.
8. Приходите от глоби постъпват в държавния бюджет.

§ 20

Ако не е определено друго, споровете по този закон се решават според общите норми за решаване на споровете.

§ 21. Промяна на гражданския кодекс

Закон № 40 от 1964 г.

. . . . . .

„§ 40, ал. 3 се изменя така:

„Писменото юридическо действие е валидно, ако е подписано от изпълнителното лице; ако юридическото действие се извършва от повече лица, не е необходимо техните подписи да присъстват на същия документ, освен ако юридическите разпоредби изискват друго. Подписът може да бъде заместен от механични средства в случаите, когато това е обичайно. Електронното съобщение може да бъде подписано с електронен подпис според специфични норми.“

§ 22. Промяна на Закон № 2 от 1969 г.

Закон № 2 от 1969 г. за устройството на министерствата и други централни органи на държавното управление на Република Чехия се изменя и допълва по следния начин:

„§ 17 (1) Министерството на транспорта и съобщенията е централен орган на държавното управление за делата на транспорта, телекомуникациите и пощите с изключение на управлението на честотния спектър, определен за радио- и телевизионно разпръскване и за електронните подписи.

(2) Министерството на транспорта и съобщенията ръководи организацията за електронни подписи.“

§ 23. Промяна на Закон № 368 от 1992 г. за държавните такси

„Приложение на Закон № 368 от 1992 г. „Размери на държавните такси“ се допълва, както следва:

„Част XI, точка 154

Разрешително за дейност като проверител на информация според специален закон – 100 000 чешки крони.“

Америка

Закон за цифровия подпис, щат Юта (САЩ)

(Резюме)

www.mbc.com/ecommerce/legis/utah.html

I. Приложно поле и цели

Законодателството на щата Юта е първото в света, което регламентира електронната търговия чрез използването на цифров подпис[1]. Законът на щата Юта регулира предоставянето на услуги от удостоверяващи организации и техните законови задължения и отговорности; определя задълженията на титуляря или подписващия, установява правната сила на цифровите подписи, улеснява системите за складиране и технологията на приложение на правно признатите цифрови подписи. Основните цели на закона са:

1. улесняване на търговията чрез надеждни електронни съобщения;
2. ограничаване в максимална степен на случаите на подправяне и измами в електронната търговия;
3. регламентиране на стандарти като X509 на Международния телекомуникационен съюз (International Telecommunication Union);
4. установяване на общи правила относно автентичността и надеждността на електронните съобщения.

II. Определения

- **Приемане на удостоверение** (accept a certificate):
  1. изразяване на одобрение относно удостоверението след запознаване със съдържанието му; или
  2. подаване на молба до удостоверяващата организация за издаване на удостоверение, в резултат на което организацията е издала удостоверението и заявителят не е отменил или анулирал молбата си.
- **Асиметрична криптосистема** (asymmetric cryptosystem) – алгоритъм или серия от алгоритми, осигуряващи надеждна двойка ключове.
- **Удостоверение** (certificate) – компютърен запис, който:
  а) указва издалата го удостоверяваща организация;
  б) именува или удостоверява титуляря на удостоверението;
  в) съдържа публичния ключ на титуляря;
  г) е цифрово подписан от издалата го удостоверяваща организация.
- **Удостоверяваща организация** (certification authority) – лице, което издава удостоверения.
- **Списък на удостоверяващата организация** (certification authority disclosure record) – он-лайн обществено достъпен списък, отнасящ се до удостоверяващата организация.
- **Заявление за удостоверителна практика** (certification practice statement) – декларация относно практиката, използвана от удостоверяващата организация при издаване на удостоверения.
- **Удостоверявам** (certify) – декларирам във връзка с удостоверението по начин, по който да се отразят и със задължение да се съобщят всички материални факти.
- **Потвърждавам** (confirm) – одобрявам след съответна проверка.
- **Съответства** (correspond) – (относно двойка ключове) означава принадлежност към определена двойка ключове.
- **Цифров подпис** (digital signature) – трансформация на съобщение чрез използване на асиметрична криптосистема по такъв начин, че лицето, съставило съобщението, и държателят на ключа могат да определят с точност:
  а) дали трансформацията е извършена чрез използването на частен ключ, който съответства на публичния ключ на подписващото лице;
  б) дали съобщението е било променено след настъпване на трансформацията.
- **Подправяне на цифров подпис** (forge a digital signature):
  а) създаване на цифров подпис без упълномощаване от страна на държателя на частния ключ;
  б) създаване на цифров подпис от титуляр, удостоверен от удостоверяващата организация, който или не съществува, или не се явява държател на частен ключ, съответстващ на публичния ключ, записан в удостоверението.

[1] Utah Digital Signature Act – Закон за цифровия подпис на щата Юта, приет на 27 февруари 1995 г., в сила от 1 май с. г.

- **Държане на частен ключ** (hold a private key) – възможност за използване на частен ключ.
- **Инкорпориране на съобщение** (incorporate by reference) – включване на съобщението след неговото идентифициране като част от друго съобщение и с изразено намерение за извършване на такова включване.
- **Издаване на удостоверение** (issue a certificate) – акт на удостоверяващата организация, с който се дава удостоверение и се уведомява титуляря, записан в удостоверението, относно неговото съдържание.
- **Двойка ключове** (key pair) – частен ключ и съответстващ му публичен ключ в асиметрична криптосистема, където публичният ключ удостоверява цифровия подпис, създаден с частния ключ.
- **Лицензирана удостоверяваща организация** (licensed certification authority) – организация, получила лицензия от специален орган (Division), който е в сила.
- **Съобщение** (message) – цифрово представяне на информация.
- **Частен ключ** (private key) – ключът от двойката с ключове, използван за създаване на цифров подпис.
- **Публичен ключ** (public key) – ключът от двойката с ключове, използван за удостоверяване на цифровия подпис.
- **Получател** (recipient) – лице, което получава или има цифров подпис и може да разчита на него.
- **Система за складиране** (repository) – система за складиране и извличане на данни, удостоверения и друга информация относно цифровите подписи.
- **Отмяна на удостоверение** (revoke a certificate) – признаване на удостоверението за невалидно от даден момент нататък. Отмяната е ефективна от момента на съобщаване или на вписване на удостоверението в списък с отменени удостоверения и не означава, че то е унищожено или нечетливо.
- **Правно валидно държане на частен ключ** (rightfully hold a private key) – означава използване на частен ключ, при което:
  а) държателят или негов служител не са разкрили информация в нарушение на чл. 305, ал. 1 от този закон;
  б) ключът не е получен от държателя чрез кражба, измама или по друг неправомерен начин.
- **Титуляр** (subscriber) – лице, което:
  а) е записано в удостоверението;
  б) е съгласно със съдържанието на удостоверението;
  в) държи частен ключ, съответстващ на публичния ключ, записан в удостоверението.
- **Спиране на действието на удостоверението** (suspend a certificate) – временно преустановяване на действието на удостоверението за точно определен период от време.
- **Удостоверяване на време** (time-stamp) – означава:
  а) приложение към съобщение, цифров подпис или удостоверение, указващо поне датата, времето и автора на приложението; или
  б) съобщение относно това приложение.
- **Удостоверение за сделка** (transactional certificate) – валидно удостоверение, съдържащо един или повече цифрови подписа.
- **Надеждна система** (trustworthy system) – компютърен хардуер и софтуер, който е:
  а) в достатъчна степен защитен от неправомерно използване;
  б) осигурява достатъчна степен на сигурност, достъпност и коректност на операциите;
  в) в достатъчна степен пригоден да осъществява специфичните функции.
- **Валидно удостоверение** (valid certificate) – удостоверение, което:
  а) е издадено от удостоверяваща организация;
  б) е прието от титуляря, записан в него;
  в) не е отменено или преустановено;
  г) не е изтекъл срокът на действие на удостоверението.
- **Потвърждаване на цифров подпис** (verify a digital signature) – във връзка с даден цифров подпис, съобщение и публичен ключ означава точно определяне на следните факти:
  а) цифровият подпис е създаден с частен ключ, съответстващ на публичен ключ; и
  б) съобщението не е променяно след създаването на цифровия подпис.

III. Основни положения

Права на лицензиращата организация (Division)

Лицензиращата удостоверяваща организация (Division) издава, спира или отменя удостоверения. Лицензиращата организация трябва да създаде и поддържа обществено достъпна база данни с лицензираните удостоверяващи организации. Лицензиращата организация следва да състави правила за:

1. управление на дейността, практиките и спиране на дейността на лицензираните удостоверяващи организации;
2. определяне на необходимите гаранции от глед-

на точка на тежестта, която пада върху удостоверяващите организации, и осигуряване на финансовата им отговорност към лицата, които разчитат на издадените удостоверения;
3. необходимите условия относно формата на удостоверението в съгласие с общоприетите стандарти, използвани за удостоверенията за цифров подпис;
4. необходимите условия за поддръжка на базите данни от удостоверяващите организации;
5. необходимите условия относно съдържанието, формата, източниците на информация в списъците на удостоверяващите организации, подновяването и срока на валидност на тази информация, както и определяне на условията за практиката на удостоверяващите организации за обявяване на данни.

Удостоверяващите организации следва да използват надеждни системи за издаване, отмяна и спиране на удостоверения, създаване на частни ключове и публикуване на необходимата информация.

Лицензиращата организация може да отмени или прекрати лицензия при неспазване на правилата за лицензиране.

Лицензиращата организация може да извършва разследвания и проверки относно спазване на материалните изисквания на закона от удостоверяващите организации, да издава нареждания в случаите на неизпълнение, да налага глоби, да спира или отменя удостоверения.

Лицензиране и права на удостоверяващата организация

За да получи лицензия, удостоверяващата организация трябва:
1. да бъде титуляр на удостоверение, публикувано в призната публична система за складиране;
2. да има служители с високи професионални качества, неосъждани за измама и подаване на декларация с невярно съдържание;
3. да предостави гаранции за наличие на оперативен капитал, достатъчен за осъществяване дейността на организацията;
4. да има надеждна система и средства за контрол при използването на частен ключ;
5. да отговаря на всички изисквания за лицензия, съставени от лицензиращата организация (Division);
6. да подаде молба и да заплати необходимата такса за регистрация.

Удостоверяващата организация има право да издава удостоверения при изпълнение на следните изисквания:
1. Удостоверяващата организация е получила молба от потенциалния титуляр;
2. Удостоверяващата организация е потвърдила, че:
   - потенциалният титуляр е лицето, вписано в удостоверението при издаване на удостоверението;
   - в случай че потенциалният титуляр действа чрез агенти, то титулярят е упълномощил агентите си да имат права над частния ключ и да подават молба за издаване на удостоверение, съдържащо съответстващ публичен ключ;
   - информацията в удостоверението е точна и проверена;
   - потенциалният титуляр на удостоверението е държател на частен ключ, съответстващ на публичен ключ;
   - потенциалният титуляр на удостоверението е правомерен държател на частен ключ, годен да създаде цифров подпис;
   - публичният ключ, записан в удостоверението, може да послужи като доказателство на цифров подпис, поставен чрез частен ключ, държан от потенциалния титуляр.
3. Изискванията на тази част от закона не могат да бъдат облекчени или отхвърлени от удостоверяващата организация, от титуляря или от двамата.

В случай че титулярят приеме издаденото удостоверение, удостоверяващата организация следва да публикува подписано копие от удостоверението в призната система за складиране на информация (repository), избрана със съгласието на удостоверяващата организация и титуляря на удостоверението, освен ако договорът между организацията и титуляря не предвижда друго.

В случай че титулярят не приема удостоверението, удостоверяващата организация не го публикува или отменя публикацията, ако такава вече е била извършена.

Гаранции на удостоверяващата организация при издаване на удостоверението

1. При издаване на удостоверението удостоверяващата организация гарантира на *титуляря* на удостоверението, че:
   а) удостоверението не съдържа информацията, за която организацията да знае, че е невярна;
   б) удостоверението е издадено при спазване на материалните изисквания на закона;
   в) удостоверяващата организация не е превишила правата си при издаване на удостоверението.
2. При издаване на удостоверението удостоверяващата организация гарантира на *всички заинтересовани лица*, че:

а) информацията в удостоверението е точна;
б) информацията, необходима за да бъде удостоверението надеждно, е достатъчно изчерпателна или включена в удостоверението чрез препратки;
в) титулярят е приел информацията в удостоверението;
г) удостоверяващата организация е издала удостоверението съгласно всички изисквания на законите на щата.

Удостоверяващата организация се смята, че действа като нелицензирана организация, в случай че издава удостоверения, излизащи извън рамките на правата, предоставени ѝ с лицензията.

Удостоверяващата организация следва да извършва работата си по такъв начин, че да не създава неоправдан риск или загуби за титуляря на удостоверението, за трети лица, разчитащи на удостоверението, или за лицата от системата за складиране (repository).

Титуляр на удостоверението

Титулярят на удостоверението се задължава да упражнява контрол над частния ключ, който е негова лична собственост, и да предотвратява разкриването му. С приемане на удостоверението той удостоверява на всички лица, разчитащи на информацията, записана в него, че:

1. държи частен ключ и съответстващ му публичен ключ, записан в удостоверението;
2. цялата информация, дадена от титуляря на удостоверяващата организация и потвърдена от нея при издаването на удостоверението, е вярна.

Агент, подал молба за издаване на удостоверение от името на титуляря, удостоверява, че притежава пълномощно от титуляря за подаване на молба за издаване на удостоверение с името на титуляря и е упълномощен да поставя цифров подпис от името на титуляря. В случай че упълномощаването е ограничено по някакъв начин, то агентът следва да представи достатъчни гаранции, че цифровият подпис не надвишава границите на упълномощаването.

Титулярят се задължава да обезщети удостоверяващата организация за претърпени загуби и вреди, в случай че той е подал невярна информация при издаване на удостоверението или е укрил факти в резултат на небрежност, или с цел да заблуди удостоверяващата организация или лице, разчитащо на информацията в удостоверението. В случай че удостоверението е издадено по молба на агент, той носи персонална отговорност за обезщетяване на организацията. Тази отговорност не може да бъде ограничена с договор между страните.

В случай че удостоверяващата организация държи частен ключ, съответстващ на публичния ключ на титуляря, издаден от тази организация, то тя го държи в качеството си на пълномощник и може да го използва само при писмено съгласие на титуляря, освен ако той не направи изрично изявление, че разрешава на удостоверяващата организация да държи ключа и да го използва съгласно нейните условия.

Спиране на удостоверението

Удостоверението се спира от удостоверяващата организация (за не повече от 48 часа) по молба на лицето, което се легитимира като титуляр на удостоверението, негов агент, служител, член от семейството. Спирането се извършва също така и в резултат на решение на лицензиращата организация или съда. Те имат право по тяхна преценка да откажат спирането и да проведат разследване на възможни закононарушения, извършени от лицето, искащо спирането.

Веднага след извършване на спирането удостоверяващата организация публикува съобщение за това в нарочен списък. Предвиждат се и алтернативни начини за спиране на удостоверението, които могат да се уговорят в договора между удостоверяващата организация и титуляря, но спирането в такива случаи е валидно от момента на вписването му в удостоверението.

Ефект на спирането е освобождаване на титуляря от задължение да пази сигурността на частния ключ за срока на спирането.

Отмяна на удостоверението

Удостоверяващата организация отменя удостоверението, издадено от нея:

а) по молба на титуляря;
б) след потвърждение, че лицето, искащо отмяната, е титуляр на удостоверението или е негов агент, упълномощен да извършва такава отмяна.

Удостоверението се отменя освен това и при смърт на титуляря или при потвърждение на неговото безследно изчезване.

Организацията може да отмени удостоверението при липса на надеждност, дори и без съгласието на титуляря и без значение на разпоредбите, записани в договора между титуляря и удостоверяващата организация.

Веднага след отмяна на удостоверението удостоверяващата организация следва да публикува съобщение за отмяната.

Ефект на отмяната е освобождаване на титуляря от задължение да пази сигурността на частния ключ. Удостоверяващата организация се освобождава от задълженията, свързани с издаването на удостоверението.

Изтичане на срока на валидност на удостоверението

Удостоверението следва да указва момента на изтичане срока на неговата валидност. След този момент титулярят и удостоверяващата организация престават да удостоверяват информацията в удостоверението и организацията се освобождава от всички задължения, свързани с издаване на удостоверението.

Писмена форма на съобщенията, подписани с цифров подпис

Съобщенията, подписани с цифров подпис, имат еднаква валидност и приложимост и следва да се третират така, както и документите в писмена форма, при условие:

1. че са подписани с цифров подпис;
2. че подписът е потвърден с публичен ключ, вписан в удостоверение, издадено от удостоверяваща организация и валидно в момента на подписване на документа.

Копие от документ, подписан с цифров подпис, има еднаква валидност и приложимост с оригинала, освен ако авторът не е определил, че част от съобщението следва да има уникалност. При това положение само тази част е валидна и има правна сила.

Система за складиране (repository)

Системата на складиране (repository) се признава от лицензиращата организация, при условие че:

1. оперира под наблюдението на удостоверяваща организация;
2. съдържа база данни с информация за:
   а) удостоверения, издадени от организацията;
   б) съобщения за прекратени и отменени удостоверения, издадени от удостоверяващата организация или от други лица, прекратили или отменили удостоверенията;
   в) данни за удостоверяваща организация;
   г) други документи, издадени от лицензиращата организация, относно регламентиране дейността на лицензираните удостоверяващи организации;
3. оперира в технически надеждна система;
4. не съдържа информация, която лицензиращата организация намира за неточна, неистинна или не в достатъчна степен надеждна;
5. съхранява архив с удостоверения, които са били прекратени или отменени или с изтекъл срок на валидност поне през последните три години;
6. отговаря на всички други изисквания, определени в правилата на лицензиращата организация.

Указ № 472 от 1998 г. на президента, Аржентина

(Резюме)

http://www.sfp.gov.ar/decree427.html http://mbc.com/legis/argentina.html

I. Приложно поле

С подписването на указа от президента на Аржентина на 16 април 1998 г. се създаде възможност за използване на публичен ключ в дейността на националната публична администрация на Аржентина. Указът постановява, че използването на публичен ключ е оторизирано за *срок от 2 години*, считано от деня на публикуване на процедурните сборници и стандарти на Подкомитета по криптография и електронни подписи, и има същия ефект, както и използването на саморъчен подпис при осъществяване дейността на националния публичен сектор. Разпоредбите на указа се отнасят до публичния сектор, включващ централни и местни органи на държавната администрация, държавни предприятия, предприятия, в които държавата е главен акционер, държавни банки и финансови институции и всички други организации, в които държавата има контролни функции.

Публичният сектор следва да мобилизира всички свои ресурси за използването на цифров подпис в изпълнение на дейността си.

Връзката между публичния ключ и титуляря се гарантира от удостоверение за публичен ключ, издадено от лицензираната удостоверяваща организация.

II. Определения

- **Лицензирана удостоверяваща организация** (licensed certification authority) – административен орган, издаващ удостоверения за публичен ключ.
- **Удостоверение или удостоверение за публичен ключ** (certificate or public key certificate) – цифров документ, издаден и подписан по електронен път от лицензирана удостоверяваща организация, свързващ публичния ключ с неговия титуляр за срока на действие на удостоверението и служещ за доказателство пред националния публичен сектор относно истинността на съдържанието на цифровия документ.
- **Частен ключ** (private key) – асиметрична криптосистема, ключ, използван за създаване на цифров подпис.
- **Публичен ключ** (public key) – асиметрична криптосистема, ключ, използван за потвърждаване на цифровия подпис.
- **Non-computer feasible** – компютърни математически изчисления, които поради изискващите се от тях времеви и компютърни ресурси превишават наличния капацитет.
- **Съответства** (to correspond) – думата се използва при двойка ключове, при която даден ключ принадлежи към определена двойка.
- **Асиметрична криптосистема** (asymmetric cryptosystem) – алгоритъм, използван за двойка ключове: частен ключ за създаване на цифров подпис и съответстващ му публичен ключ за проверка на цифровия подпис. За целите на този указ се подразбира, че асиметричната криптосистема е технически надеждна.
- **Резултат от хеширане** (hash result) – фиксирана последователност от цифри, която се получава при изпращане на цифровия документ.
- **Цифров документ** (digital document) – цифрово представяне на събития, факти и правно валидна информация.
- **Подписан цифров документ** (signed digital document) – цифров документ, към който е поставен цифров подпис.
- **Издаване на удостоверение** (to issue a certificate) – създаване на удостоверение от лицензирана удостоверяваща организация.
- **Одитираща организация** (auditing institution) – административен орган, компетентен да ревизира дейността на лицензиращата организация и лицензираните удостоверяващи организации.
- **Лицензираща организация** (licensing institution) – административен орган, компетентен да издава лицензия на удостоверяващите организации и да контролира дейността им.
- **Цифров подпис** (digital signature) – резултат от трансформация на цифров документ чрез използване на асиметрична криптосистема и резултат от хеширане по такъв начин, че лицето, което притежава цифровия документ и публичния ключ, е в състояние да определи следното:

1. дали трансформацията е настъпила в резултат от използването на частен 2.2.2. ключ, който съответства на публичния ключ на подписващото лице;
2. дали цифровият документ е бил изменян след настъпване на трансформацията.

Комбинацията от тези два фактора определя *ненакърнеността* и *неотменимостта* на подписа.

- **Хеширане** (hash result function) – математическа функция, която трансформира цифровия документ във фиксирана последователност от цифри/битове, наречена резултат от хеширане по такъв начин, че:
  1. една и съща последователност от битове се получава всеки път, когато функцията се изчислява за един и същ цифров документ;
  2. невъзможно е по компютърен път да се преустрои цифров документ от неговия хеш резултат;
  3. невъзможно е по компютърен път да се намерят два различни цифрови документа, които да произведат един и същ хеш резултат.
- **Ненакърненост** (integrity) – условие, при което документът не може да бъде променян по никакъв начин.
- **Списък на отменените удостоверения** (list of revoked certificates) – списък, публикуван от удостоверяващата организация, на удостоверения за публични ключове, издадени от нея, които са станали невалидни поради отмяна преди изтичане на определения в тях срок.
- **Неотменимост** (non-repudiation) – характеристика на цифровия подпис, при която авторът на подписа не може да се отрече от факта, че цифровият документ е бил електронно подписан от него.
- **Двойка ключове** (key pair) – частен ключ и съответстващ му публичен ключ в асиметрична криптосистема, при която публичният ключ удостоверява цифровия подпис, поставен чрез частния ключ.
- **Срок на валидност на удостоверението** (validity period of a certificate) – срок, в който титулярят може да подписва цифрови документи, използвайки частен ключ, съответстващ на публичния ключ в удостоверението, по такъв начин, че цифровият подпис не може да бъде оспорен. Срокът на действие започва да тече от деня и момента на издаване на удостоверението от лицензираната удостоверяваща организация или от по-късна дата и момент, ако това е указано в удостоверението, и спира да тече от датата на изтичането му или при отмяна на удостоверението.
- **Отмяна на удостоверението** (revocation of a certificate) – акт, анулиращ действието на удостоверението от конкретна дата нататък, в резултат на което удостоверението се вписва в списък с отменени удостоверения.
- **Удостоверяване на време** (digital time stamp) – акт на добавяне от удостоверяващата организация на датата, времето (минутите и секундите) на нейната интервенция в цифровия документ или в неговия хеш-резултат. Информацията от тази дейност е подписана по електронен път от удостоверяващата организация.
- **Надеждност на системата** (trustworthy system) – включва хардуер, софтуер и други, свързани с тях процедури, които:

1. са надеждно защитени от проникване и неправомерно използване;
2. осигуряват достатъчно високо ниво на достъпност, надеждност, конфиденциалност и оперативност;
3. са създадени технически надеждно да извършват специфичните за целта операции;
4. отговарят на общо възприетите стандарти за сигурност.

- **Титуляр** (subscriber) – лице, на името на което има издадено удостоверение и което е държател на частен ключ, съответстващ на публичен ключ, записан в удостоверението.
- **Технически надеждни** (technically trustworthy) – системи, които отговарят на техническите стандарти, издадени от Подкомитета по криптография и електронни подписи.
- **Трета страна** (third party) – всяко физическо или юридическо лице, което има субективни права и законни интереси.
- **Потвърждаване на цифров подпис** (verification of a digital signature) – възприемане на следните факти:
  1. Цифровият документ е подписан цифрово с частен ключ, съответстващ на публичния ключ, вписан в удостоверението.
  2. Цифровият документ не е променян от момента на поставяне на цифровия подпис.

  За документите, изискващи удостоверяване на конкретна дата или когато това е желателно с оглед на търсения от тях ефект, може да се иска допълнително потвърждаване, че документът е бил подписан с цифров подпис в срока на действие на съответстващото му удостоверение.

III. Основни положения

Използването на цифров подпис цели постигането на същия ефект, както и използването на саморъчен подпис в работата на държавните органи на централно и местно ниво.

Процедурните сборници и стандарти се изготвят от Подкомитета по криптография и електронни подписи – организация, натоварена с изпълнението на указа. Държавните органи предоставят на подкомитета доклади относно изпълнението на разпоредбите, заложени в указа. Подкомитетът по криптография и електронни подписи изпълнява функциите на лицензираща институция.

Лицензираща институция

Функции на лицензиращата институция

1. Издава лицензия, респективно удостоверения за публичен ключ на удостоверяващите организации, което позволява проверка/верификация на цифровите подписи;
2. Отказва издаването на лицензия на удостоверяваща организация, която не отговаря на необходимите изисквания;
3. Отменя издадена лицензия на удостоверяващи организации, които вече не отговарят на необходимите изисквания;
4. Контролира лицензираните удостоверяващи организации относно използването на технически надеждни системи;
5. Изучава и одобрява процедурните сборници и планове за секретност, предоставени от удостоверяващите организации;
6. Дава съгласие съвместно с одитиращите институции относно счетоводния план на лицензираните удостоверяващи организации;
7. Назначава *ex officio* счетоводни проверки;
8. Решава спорове, възникнали между титуляря на удостоверението и лицензираната удостоверяваща организация, издала удостоверението.
9. Решава други непредвидени случаи, възникнали в системата на цифровите подписи.

Задължения на лицензиращата институция

Задълженията ѝ са сходни с тези на удостоверяващите организации. Освен това лицензиращата организация трябва:

1. да се въздържа от генериране, изискване и получаване на информация по какъвто и да е друг начин относно частния ключ на титуляря, чието удостоверение издава.
2. да контролира своя собствен частен ключ и да избягва неговото разкриване;
3. да отменя собственото си удостоверение за публичен ключ, в случай че частният ключ е разкрит;
4. да осигурява постоянен достъп до удостоверенията за публичен ключ, издадени от лицензираните удостоверяващи организации, както и до списъка на отменените удостоверения, чрез публично достъпни телекомуникационни връзки. Това също се отнася до информацията относно адресите и телефонните номера на лицензираните удостоверяващи организации;
5. да дава пълна информация и оказва съдействие на одитиращите институции;
6. да публикува своето удостоверение за публичен ключ;
7. да отменя удостоверенията, издадени на лицензираните удостоверяващи организации, които са били закрити или където са настъпили основания за отмяна на лицензията;
8. да отменя удостоверенията, издадени от удостоверяващата организация, в случай че ключът се окаже технически ненадежден;
9. да осъществява контрол над плана за закриване на лицензирани удостоверяващи организации, в случай че те престанат да отговарят на изискванията;
10. да вписва подадените жалби заедно с подробна информация относно действията, предприети във всеки конкретен случай.

Удостоверяваща организация

Функции на лицензираната удостоверяваща организация

1. Удостоверяващата организация издава удостоверения за публичен ключ, като за целта трябва:
   а) да получи молба за издаване на удостоверение за публичен ключ от потенциалния титуляр, подписана с цифров подпис чрез частен ключ;
   б) да сравни и удостовери личната информация за титуляря, съдържаща се в удостоверението и всяка друга информация, която трябва да бъде потвърдена съгласно процедурните правила на удостоверяващата организация;
   в) да постави корелативно съответстващи номера на издадените удостоверения;
   г) да съхранява копия от всички издадени удостоверения и от датата на издаването им.

Лицензираната удостоверяваща организация може по своя преценка да включи в удостоверението и друга, неудостоверена от нея информация, но трябва изрично да посочи това в удостоверението.

Задължения на лицензираната удостоверяваща организация

Към задълженията, която лицензираната удостоверяваща организация има като титуляр на удостоверение, издадено от лицензиращата институция, тя трябва:

1. да се въздържа от събиране и изискване на информация, свързана с частния ключ на титуляря;
2. да контролира своя собствен частен ключ и да избягва неговото разкриване;
3. незабавно да поиска отмяна на собственото си удостоверение, в случай че частният ключ на организацията е бил разкрит;
4. да поиска от лицензиращата институция да отмени удостоверението, в случай че публичният ключ престане да бъде технически надежден;
5. незабавно да оповести лицензиращата институция за всяка промяна в информацията, съдържаща се в удостоверението, или за всеки факт от съществено значение за тази информация;
6. да използва технически надеждна система;
7. да информира титуляря за всички предпазни мерки, които той следва да съблюдава с оглед създаването на надежден цифров подпис, и за всички негови задължения;
8. да събира само тези лични данни за титуляря, които са абсолютно необходими за издаване на удостоверението. Титулярят може по своя преценка да предостави всякаква друга информация, която, ако не бъде включена в удостоверението, ще се съхранява от удостоверяващата организация по конфиденциален начин;
9. да предоставя на титуляря цялата информация относно удостоверението;
10. да пази цялата документация във връзка с издаваните удостоверения в срок от 10 години;
11. да осигури постоянен публичен достъп до издаваните удостоверения и до списъка с отменените удостоверения чрез публично достъпни телекомуникационни връзки;
12. да публикува адреса и телефонните си номера;
13. да осигурява достъп на одитиращите институции и да им предоставя цялата необходима за одита информация;
14. да вписва подадените жалби заедно с информация за мерките, предприети във всеки конкретен случай.

Отмяна на удостоверението от удостоверяващата организация

Лицензираната удостоверяваща организация може да отмени удостоверението и съответно публичния ключ:

1. по молба на титуляря;
2. по молба на трета страна;
3. когато установи, че удостоверението е издадено в резултат на невярна информация, която е трябвало да бъде проверена в момента на издаването;
4. ако се установи, че публичният ключ, съдържащ се в удостоверението, е престанал да бъде технически надежден;
5. ако трябва да се прекрати и да не се прехвърля издаденото удостоверение на друга лицензирана удостоверяваща организация.

Отмяната следва да определя момента, от който влиза в сила, и не може да има обратно действие или действие за в бъдеще. Отменението удостоверение следва да се включи незабавно в списъка с отменени удостоверения, който следва да се подпише от удостоверяващата организация. Обществеността трябва да има постоянен достъп до този списък чрез публично достъпни телекомуникационни връзки.

Лицензираната удостоверяваща организация издава документ за отмяна на удостоверението или по избор предоставя удостоверяване на времето на лицето, което желае отмяната.

Титуляр на удостоверението за публичен ключ

Задължения на титуляря

1. да предостави на удостоверяващата организация цялата необходима информация;
2. да контролира частния си ключ и да предотвратява неговото разкриване;
3. незабавно да информира удостоверяващата организация относно всяка промяна, която може да доведе до разкриване на частния ключ;
4. да подаде молба до удостоверяващата организация за отмяна на удостоверението, в случай че публичният ключ в удостоверението престане да бъде технически надежден;
5. незабавно да информира удостоверяващата организация относно всяка промяна в данните, записани в удостоверението.

Удостоверение за публичен ключ

Реквизити

1. име на титуляря на удостоверението;
2. вид и номер на документа за самоличност на титуляря или лицензионен номер, в случай на удостоверения, издадени на лицензирани удостоверяващи организации;
3. публичен ключ, издаден на титуляря;
4. име на алгоритъма на публичния ключ на удостоверението;
5. сериен номер на удостоверението;
6. срок на действие на удостоверението;
7. име на лицензираната удостоверяваща организация, издала удостоверението;
8. цифров подпис на лицензираната удостоверяваща организация, издала удостоверението, идентифициращо използвания алгоритъм;

9. всяка друга информация, необходима за удостоверението, съгласно процедурните изисквания на лицензираната удостоверяваща организация.

Условия за валидност на удостоверението
Удостоверението е валидно, когато:

1. е издадено от лицензирана удостоверяваща организация;
2. не е отменено;
3. не е изтекъл срокът на действие на удостоверението.

Закон за достъп и използване на електронни съобщения, електронна търговия и електронен подпис, Колумбия

(Резюме)

I. Приложно поле

Подготвеният законопроект се състои от 3 части – първите две следват до голяма степен Закона-модел на УНСИТРАЛ, като част първа се отнася за електронната търговия, част втора – за електронната търговия в някои специфични области и част трета – за електронните подписи, удостоверения и удостоверяващи организации. Приложното поле на законопроекта обхваща всяка информация във формата на електронно съобщение с изключение на задълженията, поети от държавата в резултат на международни споразумения или договори, както и писмените предупреждения, които по силата на правна норма трябва да бъдат задължително отпечатани върху определени продукти, при които съществува риск във връзка с тяхното разпространение, използване или консумиране.

II. Определения

В закона са дадени следните определения:

- **Електронно съобщение** (data massage) – информация, която е създадена, изпратена, получена, запазена или обменена чрез електронно, оптическо или друго такова средство, като например електронен обмен на данни (ЕОД), Интернет, електронна поща, телеграма или телекс.
- **Електронна търговия** (electronic trade) – включва въпросите, породени от всякакви отношения с търговски характер (договорни или недоговорни), които са структурирани на основата на използването на едно или повече електронни съобщения или други такива средства, като например търговски операции за снабдяване или обмен на стоки или услуги, дистрибуторски споразумения, финансови, борсови и застрахователни операции, консултантски услуги и др.
- **Електронен подпис** (digital signature) – цифров израз, прикрепен или добавен към електронно съобщение, който чрез използването на определена математическа процедура, свързана с паролата или с текста на самото съобщение на съставителя, позволява да се установи, че такъв израз може да бъде получен само чрез паролата на съставителя и че конкретното съобщение не е било променяно след извършване на съответната трансформация.
- **Удостоверяващ орган** (certifying entity) – лицето, което е овластено в съответствие с този закон да издава удостоверения във връзка с електронните подписи на лицата, да предлага или осигурява услуги по записването и хронологичното маркиране на предаването и получаването на електронни съобщения, както и да изпълнява други задължения във връзка с комуникацията чрез електронни съобщения.
- **Електронен обмен на данни** (data electronic exchange) – предаване на електронни съобщения от един компютър на друг, което е структурирано според съгласуваните за тази цел технически правила.
- **Информационна система** (information system) – всяка система, използвана за създаване, изпращане, получаване, записване или обработване на електронни съобщения независимо по какъв начин.

III. Основни принципи

Законът изрично забранява информацията да бъде лишавана от действителност, правно действие или задължителна сила само на основание, че е под формата на електронно съобщение.

Когато нормативен акт изисква писмена форма, това изискване се смята спазено, ако информацията е под формата на електронно съобщение, при условие че тази информация е достъпна за последващо използване.

Когато нормативен акт изисква наличието на подпис или предвижда определени последици при липсата на такъв, това изискване ще се счита спазено и чрез използването на електронно съобщение при следните условия:

- използван е метод, който позволява да се идентифицира съставителя на електронното съобщение и който показва, че неговото съдържание е било потвърдено от съставителя;
- методът е едновременно сигурен и удобен за целта, за която съобщението е било създадено или предадено.

Когато нормативен акт изисква информацията да бъде представена и съхранявана в оригинал, това изискване се смята за спазено чрез използване на електронно съобщение при следните условия:

- съществува сигурна гаранция, че ненакърнеността на информацията в електронното съобщение е запазена от момента, в който тя е била създадена за първи път в своя окончателен вид като електронно съобщение или друга форма;
- информацията може да бъде показана на лицето, на което трябва да бъде представена, ако е предназначена за това.

IV. Комуникация с електронни съобщения

При подготовката на договори, ако страните изрично не са уговорили друго, предложението и неговото приемане могат да бъдат във формата на електронни съобщения. Това не може да се отрази на действителността на договора и неговата задължителна сила. В отношенията между съставителя и адресата това важи за всички изявления, направени във формата на електронни съобщения.

Електронното съобщение се смята изпратено от съставителя, когато то е било изпратено от:

- самия съставител;
- всяко лице, овластено да действа от името на съставителя по отношение на това електронно съобщение;
- информационна система, програмирана от съставителя или от негово име да работи автоматично.

Електронното съобщение се предполага, че е било изпратено от съставителя, ако:

- предварително съгласуваната със съставителя процедура за установяване дали електронното съобщение действително е било изпратено от съставителя е била приложена;
- електронното съобщение, получено от адресата, е резултат от действието на лице, чиито отношения със съставителя или с негов пълномощник дават на това лице или на пълномощника достъп до методите, които съставителят използва за идентифициране на съобщенията като свои.

Във всички случаи, когато електронното съобщение е изпратено от съставителя или адресатът има право да го счита за изпратено от съставителя, в отношенията си със съставителя адресатът има право да приеме, че съдържанието на това съобщение съответства на намерението на съставителя, освен ако е знаел или е могъл да узнае чрез полагане на дължимата грижа или прилагане на съгласувания метод, че при предаването на електронното съобщение има грешка.

Всяко получено електронно съобщение се смята за отделно електронно съобщение, освен ако дублира друго електронно съобщение и адресатът знае или е могъл да узнае чрез полагане на дължимата грижа или прилагане на съгласувания метод, че новото съобщение е дубликат.

Ако по време на изпращането на електронното съобщение или преди това съставителят е поискал от адресата или се е споразумял с него за потвърждение на получаването, без да е уговорена определена форма или метод за това, такова потвърждаване може да бъде:

- всяко съобщение от адресата независимо дали е автоматично;
- всяко действие на адресата, достатъчно да покаже на съставителя, че електронното съобщение е било получено.

Ако съставителят е поискал от адресата или се е споразумял с него за потвърждение на получаването на електронното съобщение и е поставил това като условие за действителността на съобщението, това съобщение не може да се смята получено, докато не се получи потвърждението.

Ако съставителят получи потвърждение от адресата, предполага се, че електронното съобщение е получено.

Ако съставителят и адресатът не са уговорили друго, електронното съобщение се смята изпратено, когато постъпи в информационна система, която не се намира под контрола на съставителя или на лицето, изпратило съобщението от името на съставителя.

Ако не е уговорено друго, електронното съобщение се смята получено, както следва:

- ако адресатът е посочил информационна система за получаване на електронни съобщения – когато постъпи в посочената електронна система;
- ако електронното съобщение е изпратено в информационна система, различна от посочената – когато адресатът изтегли електронното съобщение;
- ако адресатът не е посочил информационна система – когато електронното съобщение постъпи в информационна система на адресата.

Ако не е уговорено друго между съставителя и адресата, електронното съобщение се смята изпратено от седалището на съставителя и получено в седалището на адресата. Ако съставителят или адресатът имат повече от едно седалище, за такова се смята това, което се намира в най-тясна връзка с извършваната операция, а когато такава връзка няма – главното седалище. Ако съставителят или адресатът нямат седалище, за такова се приема постоянното им пребиваване.

V. Електронен подпис

Използването на електронен подпис има същата сила, каквато има поставянето на саморъчен подпис, ако електронният подпис отговаря на следните изисквания:

- уникален е за лицето, което го използва;
- подлежи на удостоверяване;
- намира се под изключителния контрол на лицето, което го използва;
- свързан е с информацията или съобщението по такъв начин, че ако те бъдат променени, електронният подпис става недействителен;
- съответства на действащите нормативни актове.

VI. Удостоверяващи органи

Удостоверяващите органи получават разрешение от Агенцията за надзор върху промишлеността и търговията и трябва да отговарят на следните условия:

- да притежават достатъчно икономически и финансови възможности да предоставят услуги като удостоверяващи органи;
- да притежават технически възможности за създаването на електронни подписи, издаването на удостоверения за тяхната автентичност и обработката на електронни съобщения при условията, предвидени в този закон.

Удостоверяващите органи, получили разрешение от Агенцията за надзор върху промишлеността и търговията, могат да извършват следните дейности:

- издаване на удостоверения във връзка с електронните подписи на физически и юридически лица;
- издаване на удостоверения във връзка с установяването на промени, настъпили между изпращането и получаването на електронни съобщения;
- предоставяне на услуги по създаване на удостоверени електронни подписи;
- предоставяне на услуги по хронологичното регистриране или маркиране на създаването, предаването и получаването на електронни съобщения;
- съхраняване и обработване на електронни съобщения.

Заплащането на услугите, извършвани от удостоверяващите органи, се определя от самите тях.

Удостоверяващите органи имат следните задължения:

- да издават исканите или уговорени със съставителя удостоверения;
- да използват системи за сигурност с цел да се гарантират създаването и използването на електронните подписи, съхраняването и регистрирането на удостоверенията и другите документи към електронните съобщения;
- да гарантират сигурността, поверителността и използването по предназначение на информацията, предоставена от титуляря на електронния подпис;
- да гарантират непрекъснатото предоставяне на услугите;
- периодично да се запознават с исканията и жалбите на титулярите на електронни подписи;
- да извършват публикации и реклами в съответствие с нормите на закона;
- да предоставят информацията, поискана от административни или съдебни органи във връзка с електронните съобщения и издадените удостоверения;
- да допускат и съдействат при извършване на проверки от Агенцията за надзор върху промишлеността и търговията;
- да изготвят правилници във връзка с отношенията им с титулярите на електронни подписи и начина на предоставяне на услугите;
- да водят регистър на удостоверенията.

Ако не е уговорено друго, удостоверяващият орган може едностранно да прекрати съществуващо споразумение с титуляря на електронен подпис, като му изпрати съобщение за това не по-малко от 90 дни предварително. След този срок удостоверяващият орган отказва издаването на удостоверения. Титулярят може да прекрати едностранно съществуващо споразумение, като изпрати съобщение за това не по-малко от 30 дни предварително.

VII. Удостоверения

Удостоверенията, издавани от получилите разрешение удостоверяващи органи, трябва да носят електронния подпис на последните и да включват най-малко следното:

- името, адреса и местожителството на титуляря;
- идентификационния номер на титуляря, използван в удостоверението;
- името, адреса и мястото, където удостоверяващият орган осъществява дейността си;
- публичната парола на ползвателя;
- методологията, използвана за удостоверяване на електронния подпис на титуляря, поставен в електронно съобщение;
- серийния номер на удостоверението;
- датата на издаване и на прекратяване на действието на съответното удостоверение.

Титулярят на удостоверен електронен подпис може да иска от удостоверяващия орган да отмени удостоверението. Той е длъжен да поиска отмяна в следните случаи:

- загуба на частната парола;

- частната парола е или съществува риск да бъде неправилно използвана.

Ако титулярят не поиска отмяна на удостоверението в посочените случаи, той носи отговорността за вредите и загубите, настъпили за трети добросъвестни лица, които са се доверили на такова удостоверение.

Удостоверяващият орган отменя издадено удостоверение на следните основания:

- по искане на титуляря или на трето лице от името на титуляря;
- при смърт на титуляря;
- при прекратяване на титуляря, ако е юридическо лице;
- при установяване, че информация или факт в удостоверението са неистински;
- ако частната парола на удостоверяващия орган или системата му за сигурност е изложена на риск, засягащ годността на удостоверението;
- при прекратяване на дейността на удостоверяващия орган;
- при съдебна заповед или заповед от компетентен административен орган.

VIII. Титуляр на електронен подпис

Титулярят на електронен подпис има следните задължения:

- да получи електронен подпис от удостоверяващия орган или да създаде такъв при използване на метод, одобрен от този орган;
- да представя информация при поискване от удостоверяващия орган;
- да осъществява контрол върху електронния подпис;
- периодично да иска отмяна на удостоверения.

Титулярят на електронния подпис отговаря за неистинност, грешка или пропуск в информацията, представена на удостоверяващия орган, както и за неизпълнение на задълженията си като титуляр.

IX. Агенция за надзор върху промишлеността и търговията

Агенцията за надзор върху промишлеността и търговията има следните задължения:

- да разрешава извършването на дейност от удостоверяващи органи на територията на страната;
- да наблюдава дейността и предоставянето на услугите от удостоверяващите органи;
- да извършва проверки на удостоверяващите органи;
- да отменя или отказва издаването на разрешения за извършването на дейност като удостоверяващ орган;
- да изисква информация за изпълнението на задълженията от удостоверяващите органи;
- да налага санкции на удостоверяващите органи при неизпълнение на задълженията им във връзка с предоставяните услуги;
- да нарежда отмяната на удостоверения, които са издадени от удостоверяващите органи, без да са спазени нормативните изисквания;
- да издава удостоверения за електронните подписи на удостоверяващите органи;
- да следи за спазването на конституционните и други правни норми относно защитата на конкуренцията, ограниченията в търговската дейност, нелоялната конкуренция и закрилата на потребителите;
- да дава указания по спазването на нормативните актове, на които удостоверяващите органи са подчинени.

Агенцията за надзор върху промишлеността и търговията въз основа на съответните процедури и правото на защита може да налага в зависимост от характера и сериозността на нарушението следните санкции на удостоверяващите органи:

- предупреждение;
- имуществена санкции до определен максимален размер, както за удостоверяващите органи, така и за техните служители или представители;
- незабавно прекратяване на всички или някои дейности;
- забрана за предоставяне на услуги за определен период от време;
- окончателно отнемане на разрешението за осъществяване на дейност като удостоверяващ орган.

Азия

Закон за електронните трансакции, Сингапур

(Резюме)

www.cca.gov.sg/eta/index.html

I. Приложно поле

През 1998 г. в Сингапур се приема Закон за електронните трансакции. Законът регулира цифровите подписи, електронните договори, електронното вписване на данни и правата и задълженията на удостоверяващите организации.

Законът на Сингапур е възприел основните положения, залегнали в Закона-модел на УНСИТРАЛ за електронна търговия, в пакета закони за регулиране на рамковите условия за информационните и комуникационните услуги на ФРГ, закона на щата Юта и на щата Илинойс, САЩ.

II. Определения

- **Асиметрична криптосистема** (asymmetric cryptosystem) – система, способна да създава надеждна двойка ключове, състояща се от частен ключ за създаване на цифров подпис и публичен ключ за проверка на цифровия подпис.
- **Оторизиран служител** (authorized officer) – лице, оторизирано от контрольора съгласно разпоредбите на този закон.
- **Удостоверение** (certificate) – запис, издаден, за да поддържа цифровите подписи, който следва да потвърждава самоличността или други съществени характеристики на лицето, което държи определена двойка ключове.
- **Удостоверяваща организация** (certification authority) – лице или организация, които издават удостоверения.
- **Изявление за удостоверителна практика** (certification practice statement) – изявление, издадено от удостоверяваща организация, за конкретизиране на практиката, възприета от нея при издаването на удостоверения.
- **Контрольор** (controller) – назначеният съгласно разпоредбите на този закон контрольор на удостоверяващите организации, включително назначените заместник-контрольори и помощник-контрольори, които контролират удостоверяващите организации.
- **Съответства** (correspond) – принадлежи към една и съща двойка ключове (във връзка с частния и публичния ключ).
- **Цифров подпис** (digital signature) – електронен подпис, състоящ се от трансформация на електронен запис, с използване на асиметрична криптосистема и хеш функция по такъв начин, че лицето, което има първоначалния нетрансформиран електронен запис и публичния ключ на подписващото лице може със сигурност да определи:
  а) дали трансформацията е извършена чрез използване на частния ключ, който съответства на публичния ключ на подписващото лице; и
  б) дали първоначалният електронен запис е бил изменян след извършване на трансформацията.
- **Електронен запис** (electronic record) – запис, който е създаден, предаден, получен или съхранен по електронен, магнитен, оптичен или друг начин в информационна система или за трансформация от една информационна система в друга.
- **Електронен подпис** (electronic signature) – знаци, букви, числа или други символи в цифрова форма, прикрепени към или логически свързани с електронен запис и изпълнени и приети с намерение за автентификация или одобрение на електронния запис.
- **Хеш функция** (hash function) – алгоритъм, който превежда една последователност от битове в друга, по-малка (хеш резултат), по такъв начин, че:
  а) записът дава един и същ хеш резултат всеки път, когато алгоритъмът се използва при въвеждане на същия запис;
  б) невъзможно е чрез изчисляване записът да бъде извлечен и реконструиран от хеш резултата, произведен от алгоритъма; и
  в) невъзможно е чрез изчисления да се стигне до 2 записа, които водят до един и същ хеш резултат при използването на алгоритъма.
- **Информация** (information) – включва данни, текст, образи, звук, кодове, компютърни програми, софтуер и бази данни.
- **Двойка ключове** (key pair) – частен ключ и математически свързан с него публичен ключ, като с публичния ключ може да се провери цифров подпис, създаден с частния ключ (в аси-

метрична криптосистема).

- **Лицензирана удостоверяваща организация** (licenced cerification authority) – удостоверяваща организация, получила лицензия от контрольора съгласно разпоредбите на този закон.
- **Период на действие на удостоверението** (operational period of a certificate) – започва от датата и часа на издаване на удостоверението от удостоверяващата организация (или от по-късна дата и час, ако така е указано в удостоверението) и приключва на датата и часа, в който изтича съгласно записаното в удостоверението, или по-рано, ако то е било отменено или прекратено.
- **Частен ключ** (private key) – ключът от двойката ключове, използван за създаване на цифров подпис.
- **Публичен ключ** (public key) – ключът от двойката ключове, използван за проверка на цифровия подпис.
- **Запис** (record) – информация, която е записана, съхранена или фиксирана по друг начин в материална среда или която се съхранява в електронна или друга среда и може да бъде възстановена в годна за възприемане форма.
- **Система за съхранение** (repository) – система за съхраняване и възстановяване на удостоверения или друга информация във връзка с удостоверенията.
- **Отмяна на удостоверение** (revoke a certificate) – означава окончателно прекратяване на периода на действие на удостоверението от определен момент.
- **Процедура за сигурност** (security procedure) – процедура, която има за цел:
  а) установяване, че определен електронен запис е на определено лице;
  б) откриване на грешки или промени в предаването, съдържанието или съхраняването на електронен запис от определен момент, която може да изисква използване на алгоритми или кодове, идентифициране на думи или числа, кодиране, обратен отговор или процедури за приемане или подобни средства за сигурност.
- **Подписан** или **подпис** (signed or signature) и граматическите им разновидности включват всеки символ, използван или възприет, или всяка методология или процедура, прилагана или възприета от лице с намерение да автентифицира запис, включително електронни и цифрови методи.
- **Титуляр** (subscriber) – лицето, което е наименувано или идентифицирано в удостоверението, издадено на него, и което държи частния ключ, който съответства на публичния ключ, записан в удостоверението.
- **Прекратяване на действието на удостоверението** (suspend a certificate) – временно прекратяване на действието на удостоверението от определен момент.
- **Система за надеждност** (trustworthy system) – компютърен хардуер, софтуер и процедури, които:
  а) са достатъчно защитени от навлизане и неправомерно използване;
  б) осигуряват достатъчно ниво на достъпност, надеждност и коректна оперативност;
  в) са надеждно създадени да осъществяват предвидените функции;
  г) отговарят на общопризнатите процедури за сигурност.
- **Валидно удостоверение** (valid certificate) – удостоверение, издадено от удостоверяваща организация и прието от титуляря, записан в него.
- **Проверка на цифров подпис** (verify a digital signature) – (във връзка с определен цифров подпис, запис или публичен ключ) точно определяне дали:
  а) цифровият подпис е създаден чрез използване на частния ключ, съответстващ на публичния ключ, записан в удостоверението; и
  б) записът не е променян от създаването на цифровия подпис.

III. Общи правила

Информацията не може да бъде лишена от правно действие, действителност или правна сила само на основание, че е под формата на електронен запис. Когато законът изисква определена информация да бъде представена в писмена форма и предвижда определени последици, ако не е в такава форма, това изискване се смята изпълнено посредством електронен запис, ако информацията, съдържаща се в него, е достъпна за последващо използване.

Когато законът изисква подпис и предвижда определени последици, ако документът не е подписан, това изискване се смята спазено посредством електронен подпис. Електронният подпис може да бъде доказван по всякакъв начин, включително като се покаже, че съществува процедура, при която е необходимо страната, за да продължи с операцията, да изпълни определен символ или процедура за сигурност, с цел да се провери дали електронният запис принадлежи на тази страна.

Когато законът изисква определени документи, записи или информация да бъдат запазени, това изискване се смята изпълнено чрез запазването им под формата на електронни записи, ако са спазени следните изисквания:

а) съдържащата се в тях информация остава достъпна за последващо използване;
б) електронният запис е запазен в същия формат, в който е бил първоначално създаден, изпратен или получен, или във формат, в който може точно да демонстрира или представи първоначално създадената, изпратена или получена информация;
в) ако съществува и е била запазена информация, която позволява идентифициране на произхода и предназначението на електронния запис и датата и времето на неговото изпращане или получаване;
г) ако е получено съгласието на ведомството, министерството, държавния орган или организацията, които отговарят за изискванията относно запазването на такива записи.

IV. Електронни договори

Ако при сключването на договора страните не са уговорили друго, предложението и приемането на предложението могат да бъдат под формата на електронни записи. Когато при сключването на договора е използван електронен запис, такъв договор не може да бъде лишен от действителност или правна сила само на основание, че за целта е използван електронен запис.

Волеизявленията и другите изявления в отношенията между съставителя и адресата на електронния запис не могат да бъдат лишени от правно действие, действителност и правна сила само на основание, че са под формата на електронни съобщения.

Електронният запис е на съставителя, ако е бил изпратен от самия него.

В отношенията между съставителя и адресата електронният запис се смята за такъв на съставителя, ако е бил изпратен:

а) от лице, което е овластено да действа от името на съставителя във връзка с конкретния електронен запис; или
б) от информационна система, програмирана от съставителя или от негово име да работи автоматично.

В отношенията си със съставителя адресатът има право да смята електронния запис за такъв на съставителя и да действа в съответствие с това, ако:

а) с цел да установи дали електронният запис е на съставителя, адресатът точно е приложил предварително съгласувана с него процедура; или
б) полученото от адресата електронно съобщение е резултат от действията на лице, чиито отношения със съставителя или с негов представител му позволяват да получи достъп до използвания от него метод за идентифициране на електронните записи като свои.

Последното правило не се прилага:

а) от момента, когато адресатът е получил съобщение от съставителя, че електронният запис не е негов и е имал достатъчно време да действа в съответствие с това;
б) в случаите на подточка „б“ от предходното правило винаги когато адресатът е знаел или е трябвало да знае при полагане на дължимата грижа или прилагане на съгласуваната процедура, че електронният запис не е на съставителя; или
в) ако съобразно всички обстоятелства по случая е неестествено адресатът да смята електронният запис за такъв на съставителя и да действа в съответствие с това.

Когато електронният запис е на съставителя, смята се за негов или адресатът има право да го смята за негов, в отношенията си със съставителя адресатът има право да смята, че полученият електронен запис отговаря на намерението на съставителя, и да действа в съответствие с това. Адресатът няма това право, ако е знаел или е трябвало да знае при полагане на дължимата грижа или прилагане на съгласуваната процедура, че е налице грешка при предаването на електронния запис.

Адресатът има право да смята всеки получен електронен запис за самостоятелен и да действа в съответствие с това, с изключение на случаите, когато дублира друг електронен запис или когато е знаел или е трябвало да знае при полагане на дължимата грижа или прилагане на съгласуваната процедура, че електронният запис е дубликат.

Съставителят може да поиска от адресата или да се договори с него за потвърждаване на получаването на електронния запис. Когато съставителят и адресатът не са уговорили определена форма или определен метод за получаване на потвърждението, то може да бъде направено посредством:

а) всяко автоматично или друго съобщение от адресата; или
б) всяко действие на адресата, достатъчно да му покаже, че електронният запис е бил получен.

Ако съставителят е поставил получаването на потвърждение като условие, електронният запис се смята за неизпратен, докато се получи потвърждението.

Ако съставителят не е поставил получаването на потвърждение като условие и потвърждението не е било получено в определения или уговорен срок или в разумен срок, ако такъв не е бил определен или уговорен, съставителят може:

а) да уведоми адресата, че потвърждение не е по-

лучено, и да определи срок за неговото получаване; и

б) ако потвърждението не бъде получено в така определения срок, да смята електронният запис за неизпратен и да упражни другите си права, като уведоми за това адресата.

Ако съставителят получи потвърждение от адресата, предполага се, освен ако има доказателства за противното, че електронният запис е получен, но не се предполага, че съдържанието на получения електронен запис съответства на изпратения.

Ако според полученото потвърждение електронният запис отговаря на уговорените или установени в приложимите стандарти технически изисквания, предполага се, освен ако има доказателства за противното, че тези изисквания са били изпълнени.

Ако друго не е уговорено между съставителя и адресата, електронният запис се смята изпратен, когато постъпи в електронна система извън контрола на съставителя или на лицето, което е изпратило електронния запис от името на съставителя.

Ако друго не е уговорено между съставителя и адресата, електронният запис се смята приет, както следва:

а) ако адресатът е посочил информационна система за получаване на електронни записи, електронният запис се смята получен:
   - в момента на постъпването му в посочената информационна система; или
   - ако е изпратен в друга информационна система, различна от посочената, в момента на изтеглянето му от адресата;

б) ако адресатът не е посочил информационна система, електронният запис се смята получен в момента на постъпването му в информационна система на адресата.

Ако не е уговорено друго между съставителя и адресата, електронният запис се смята изпратен от мястото на дейност на съставителя и получен в мястото на дейност на адресата. Ако съставителят или адресатът имат повече от едно място на дейност, за такова се приема това, което се намира в най-тясна връзка със съответния договор, или ако няма такова – основното място на дейност. Ако съставителят или адресатът нямат място на дейност, за такова се приема мястото на обичайното им пребиваване. Мястото на обичайно пребиваване на юридическите лица е мястото, където те са регистрирани или по друг начин правно установени.

V. Сигурни електронни записи и подписи

Ако предписаната или търговски целесъобразната процедура за сигурност, договорена от заинтересованите страни, е била надлежно приложена спрямо определен електронен запис, с цел да бъде установено, че той не е бил променян след определен момент, този електронен запис се приема за сигурен електронен запис от този определен момент до момента на проверката.

Ако посредством прилагането на предписаната или търговски целесъобразната процедура за сигурност, договорена от заинтересованите страни, може да се установи, че определен електронен подпис е:

а) уникален за лицето, което го използва;

б) годен да идентифицира това лице;

в) създаден по начин или със средство под контрола на лицето, което го използва; и

г) прикрепен към електронния запис, с който е свързан по такъв начин, че ако записът беше променен, електронният подпис щеше да стане невалиден, такъв подпис се приема за сигурен електронен подпис.

С оглед определянето на електронните записи и електронните подписи за сигурни определена процедура за сигурност се приема за търговски целесъобразна, като се отчитат целите на процедурата и обстоятелствата от търговски характер към момента на нейното използване, включително характера на сделката, познанията на страните, броя подобни сделки, в които са участвали страните или някоя от тях, наличието на предложени, но отказани от насрещната страна алтернативи, цената на алтернативните процедури, както и процедурите, които по принцип се използват при подобни сделки.

При всички действия, свързани със сигурен електронен запис, се предполага до доказване на противното, че сигурният електронен запис не е бил променян от определения момент до момента, с който се свързва статутът на сигурност.

При всички действия, свързани със сигурен електронен подпис, се предполага до доказване на противното, че:

а) сигурният електронен подпис е подписът на лицето, с което той се свързва; и

б) сигурният електронен подпис е бил поставен от лицето с намерение да бъде подписан или одобрен електронният запис.

Ако не е налице сигурен електронен запис или сигурен електронен подпис, не съществува презумпция във връзка с автентичността и верността на електронния запис или електронния подпис.

VI. Действие на цифровите подписи

Всяка част от електронен запис, която е подписана с цифров подпис, се смята за сигурен електронен запис, ако цифровият подпис е сигурен електронен подпис съгласно изискванията на този закон.

Ако част от електронен запис е подписана с цифров подпис, този цифров подпис се смята за сигурен, ако:

а) е създаден в рамките на периода на действие на валидно удостоверение и е проверен посредством публичния ключ, вписан в това удостоверение; и

б) удостоверението се приема за надеждно и точно показва връзката на публичния ключ със самоличността на лицето, защото:
   - удостоверението е издадено от лицензирана удостоверяваща организация, действаща в съответствие с този закон;
   - удостоверението е издадено от удостоверяваща организация извън Сингапур, призната за тази цел от контрольора съгласно този закон;
   - удостоверението е издадено от ведомство, министерство, държавен орган или организация, утвърдени от министъра да действат като удостоверяващи организации при посочените или определени от него условия; или
   - страните (изпращач и получател) са се споразумели помежду си да използват цифрови подписи като процедура за сигурност и цифровият подпис е бил надлежно проверен посредством публичния ключ на изпращача.

Предполага се до доказване на противното, че информацията (освен информацията, определена като информация на титуляря, която не е била проверена), вписана в издаденото от лицензираната удостоверяваща организация удостоверение, е вярна, ако то е прието от титуляря.

VII. Общи задължения относно цифровите подписи

Приема се, че лице, което се доверява на цифров подпис, се доверява и на удостоверението, съдържащо публичния ключ, с който цифровият подпис може да бъде проверен.

Никой няма право да публикува удостоверение или по друг начин да го прави достъпно за лице, за което знае, че се доверява на удостоверението или на цифров подпис, който подлежи на проверка посредством публичния ключ, вписан в удостоверението, ако знае, че:

а) удостоверяващата организация, посочена в удостоверението, не го е издала;

б) титулярят, вписан в удостоверението, не го е приел; или

в) удостоверението е било отменено или прекратено, освен ако това публикуване е с цел проверка на цифров подпис, създаден преди отмяната или прекратяването.

Който съзнателно създаде, публикува или по друг начин направи достъпно удостоверение с измамна или противозаконна цел, подлежи на наказание глоба в размер до 20 000 щ. д. и/или лишаване от свобода до 2 години.

Който съзнателно представи на удостоверяващата организация неверни данни за своята самоличност или овластяване във връзка с искане на удостоверение или с отмяна или прекратяване на удостоверение, подлежи на наказание глоба в размер до 10 000 щ. д. и/или лишаване от свобода до 6 месеца.

VIII. Задължения на удостоверяващата организация

Всяка удостоверяваща организация е длъжна да използва системи за надеждност при осъществяване на услугите.

Удостоверяващите организации трябва да огласят:

а) своето удостоверение, което съдържа публичния ключ, съответстващ на частния ключ, използван от удостоверяващата организация при цифрово подписване на други удостоверения (наричано в тази част удостоверение на удостоверяващата организация);

б) всяко ново изявление за удостоверяваща практика;

в) съобщение за отмяната или прекратяването на действието на удостоверението на удостоверяващата организация; и

г) всеки друг факт, който оказва влияние върху надеждността на издадено от организацията удостоверение или върху нейната способност да осъществява съответните услуги.

Ако възникне обстоятелство, което засяга системите за надеждност или удостоверението на удостоверяващата организация, последната е длъжна да направи необходимото, за да уведоми всички лица, за които е известно или се предполага, че ще бъдат засегнати от това обстоятелство, както и да действа в съответствие с процедурите, предвидени за такива обстоятелства в нейните изявления за удостоверителна практика.

Удостоверяващата организация може да издаде удостоверение на бъдещ титуляр само въз основа на направено искане от този титуляр. Ако удостоверяващата организация има изявление за удос-

товерителна практика, тя трябва да се съобрази с практиките и процедурите, предвидени в него, включително процедурите за идентификация на бъдещия титуляр.

Ако удостоверяващата организация няма такова изявление, тя трябва лично или чрез овластен представител да потвърди:

а) че бъдещият титуляр е лицето, което ще бъде вписано в удостоверението, което ще бъде издадено;

б) че титулярят е овластил представителя да има достъп до частния ключ на титуляря и да направи искане за издаване на удостоверение, съдържащо съответния публичен ключ, ако бъдещият титуляр действа чрез един или повече представители;

в) че информацията в удостоверението, което ще бъде издадено, е точна;

г) че бъдещият титуляр правомерно притежава частния ключ, съответстващ на публичния ключ, който ще се впише в удостоверението;

д) че титулярят притежава частен ключ, годен да създаде цифров подпис; и

е) че публичният ключ, който ще бъде вписан в удостоверението, може да бъде използван за проверка на цифровия подпис, създаден чрез частния ключ на бъдещия титуляр.

Посредством издаването на удостоверение удостоверяващата организация декларира пред всяко трето лице, което добросъвестно се доверява на удостоверението или на цифров подпис, подлежащ на проверка чрез публичния ключ, вписан в удостоверението, че е издала удостоверението в съответствие с всички приложими изявления за удостоверителна практика, които са включени в удостоверението чрез препращане или за които третото лице е било уведомено.

Ако липсва такова изявление за удостоверяваща практика, удостоверяващата организация декларира, че потвърждава:

а) че се е съобразила с всички изисквания на този закон относно издаване на удостоверението, а ако е публикувала удостоверението или по друг начин го е огласила на трето лице – че титулярят, вписан в удостоверението, го е приел;

б) че идентифицираният в удостоверението титуляр притежава частния ключ, съответстващ на вписания в удостоверението публичен ключ;

в) че публичният и частният ключ на титуляря образуват функциониращa двойка ключове;

г) че цялата информация в удостоверението е точна, освен ако удостоверяващата организация е посочила в удостоверението или в изявление, включено в удостоверението чрез препращане, че точността на определена информация не е потвърдена; и

д) че на удостоверяващата организация не са известни факти, включването на които в удостоверението би се отразило върху декларираното по букви от „а“ до „г“.

Посочените правила се прилагат и когато е налице приложимо изявление за удостоверителна практика, което е включено в удостоверението чрез препращане или за което третото лице е било уведомено, но само доколкото не му противоречат.

Ако удостоверяващата организация и титулярят не са уговорили нещо различно, удостоверяващата организация, издала удостоверението, е длъжна възможно най-бързо да го прекрати, ако е постъпило искане за това от лице, за което удостоверяващата организация добросъвестно смята, че е:

а) титулярят, вписан в удостоверението;

б) лице, надлежно упълномощено да извършва действия за титуляря; или

в) лице, което извършва действия от името на отсъстващия титуляр.

Удостоверяващата организация отменя издаденото от нея удостоверение:

а) при получаване на искане за отмяна от страна на вписания в удостоверението титуляр и след като бъде потвърдено, че лицето, поискало отмяната, е титулярят или негов представител, овластен с правото да поиска отмяна;

б) при получаване на заверено копие от акта за смърт на титуляря или при потвърждаване чрез други доказателства, че титулярят е починал; или

в) при представяне на документи, установяващи прекратяването дейността на титуляря, или при потвърждаване чрез други доказателства, че титулярят е прекратил дейността си или е престанал да съществува.

Удостоверяващата организация отменя удостоверението независимо от съгласието на вписания в него титуляр, ако се потвърди, че:

а) посочен в удостоверението факт е неверен;

б) не са спазени изискванията за издаване на удостоверението;

в) частният ключ или надеждната система на удостоверяващата организация са засегнати по начин, който засяга надеждността на удостоверението;

г) конкретният титуляр е починал; или

д) титулярят е прекратил дейността си или поради други причини е престанал да съществува.

При отмяна на удостоверението с изключение на случаите по букви „г“ и „д“ удостоверяващата организация незабавно уведомява титуляря, вписан в отменното удостоверение.

При прекратяване или отмяна на удостоверение-

то от страна на удостоверяващата организация последната публикува подписано съобщение за прекратяването или отмяната в системата за съхранение, определена в удостоверението за публикуване на такива съобщения. Ако има определени повече от една системи за съхранение, удостоверяващата организация публикува подписаното съобщение за прекратяване или отмяна във всички такива системи.

IX. Задължения на титуляря

Ако титулярят генерира двойката ключове, чийто публичен ключ предстои да бъде вписан в издаденото от удостоверяващата организация и прието от титуляря удостоверение, той трябва да генерира тази двойка, като използва система за надеждност. Това правило не намира приложение, ако титулярят генерира двойката ключове, използвайки система, одобрена от удостоверяващата организация.

Всичко, декларирано от титуляря пред удостоверяващата организация с цел получаване на удостоверението, включително цялата информация, известна на титуляря и включена в удостоверението, трябва да бъде максимално точна и пълна, независимо дали декларираното е потвърдено от удостоверяващата организация.

Удостоверението се смята за прието от титуляря, ако той:

а) публикува или разреши публикуването на удостоверението пред едно или повече лица или в система за съхранение;

б) демонстрира по друг начин одобрението на удостоверението, след като знае или е бил уведомен за неговото съдържание.

Титулярят, вписан в удостоверението, посредством приемане на удостоверението, издадено от него или от удостоверяваща организация, удостоверява пред всички, които добросъвестно се доверяват на съдържащата се в него информация, че:

а) титулярят правомерно притежава частния ключ, съответстващ на вписания в удостоверението публичен ключ;

б) всичко, декларирано от титуляря пред удостоверяващата организация, и информацията, вписана в удостоверението, са верни; и

в) цялата информация в удостоверението, която е известна на титуляря, е вярна.

С приемане на издаденото от удостоверяващата организация удостоверение титулярят, идентифициран в него, поема задължението да полага дължимата грижа за упражняване на контрол върху частния ключ, съответстващ на вписания в това удостоверение публичен ключ, и за предотвратяване на узнаването му от друго лице, което не е овластено да генерира цифровия подпис на титуляря. Това задължение съществува през целия период на действие на удостоверението и през всички периоди, през които удостоверението е било прекратено.

Приелият удостоверението титуляр е длъжен възможно най-бързо да поиска то да бъде прекратено или отменено от издалата го удостоверяваща организация, ако е засегнат частният ключ, съответстващ на вписания в удостоверението публичен ключ.

Електронна търговия и електронен подпис: правни аспекти

Авторски колектив

Българска
Първо издание

Редактор *Людмила Димова*
Художник на корицата *Стефан Касъров*
Технически редактор *Мирослава Карпузова*
Коректор *Цветана Маринова*

ISBN 954-9791-33-5

Дадена за набор на 16 март 2000 г.
Подписана за печат на 28 март 2000 г.
Обем 12 п. к.
Формат 210 x 297
Тираж 500 бр.
Предпечатна подготовка: отдел „Печатни издания на БНБ“
Печат и подвързия: Полиграфична база на БНБ