

---

## **ПРОТОКОЛ № 2**

от заседание на Съвет за електронно управление при Министерския съвет

**Дата:** 01.04.2015 г.

**Начален час:** 16:00

**Краен час:** 17:30

**Място:** Министерски съвет, заседателна зала, ет. 3

### Дневен ред:

1. Представяне на становища от Асоциацията банките в България и Министерство на правосъдието относно идеята за замяна на квалифициран е-подпис (КЕП) с ПИК/ПИН по решение на СЕУ от 28.01.2015 г..
2. Представяне на проектозакона за електронната идентичност.
3. Представяне на предложението на Оракъл България за предоставяне на неограничено лицензионно споразумения за нуждите на държавната администрация
4. Преместване на Интернет възела, договора за доставка на Интернет за Държавната администрация и закупените IPv4 адреси от Администрацията на Министерски съвет в Изпълнителна агенция „Електронни съобщителни мрежи и информационни системи“;
5. Представяне на проекта за Единна входна точка
6. Представяне на ЗИД на ЗДОИ с отразени коментари вследствие на общественото обсъждане
7. Представяне на статистика от ИСПОДСА за броя реално използвани лицензи за продукти на Майкрософт и информиране за процедурата

### Списък на присъстващите:

Име	Институция	Длъжност
Румяна Бъчварова	МС	Заместник министър-председател по коалиционна политика и държавна администрация и председател на Съвета за електронно управление
Томислав Дончев	МС	Заместник министър-председател по европейските фондове и икономическата политика и член на СЕУ
Ивайло Калфин	МС/МТСП	Заместник министър-председател по демографската и социалната политика и министър на труда и социалната политика и член на СЕУ
Антон Герунов	МС	Началник на политическия кабинет на заместник министър-председателя по коалиционна политика и държавна администрация
Васил Величков	МС	Съветник към заместник министър-председател по коалиционна политика и държавна администрация
Владислав Горанов	МФ	Министър на финансите и член на СЕУ
Валери Борисов	МТИТС	Заместник-министър на транспорта, информационните технологии и съобщенията и Секретар на Съвета за електронно управление
Петър Иванов	БАИТ	Председател на УС на Българска асоциация по информационни технологии, член на СЕУ и член на Бизнес съвета към СЕУ
Стамен Кочков	БАСКОМ	Председател на УС на БАСКОМ и член на Бизнес съвета към СЕУ
Жанет Захариева	ICT Cluster	Председател на Бизнес съвета към СЕУ
Диана Янчева	НСИ	Заместник-председател на НСИ
Сергей Цветарски	НСИ	Председател на НСИ
Леончия Сеизова	АМС	Началник отдел „Информационно обслужване“ в Администрацията на Министерския съвет

Заседанието на Съвета за електронно управление бе открита от неговия председател – заместник министър-председателя г-жа Р. Бъчварова. След кратки встъпителни думи тя даде

думата на секретаря на Съвета – В. Борисов. Същият информира присъстващите, че е налице кворум и Съвета може да взема решения. По т. 1 от дневния ред председателя на съвета даде думата на В. Борисов.

**1. Представяне на становища от Асоциацията банките в България и Министерство на правосъдието относно идеята за замяна на квалифициран е-подпис (КЕП) с ПИК/ПИН по решение на СЕУ от 28.01.2015 г.**

**Докладва:** Валери Борисов – заместник-министър на транспорта, информационните технологии и съобщенията и секретар на Съвета.

В. Борисов припомни на присъстващите решението, взето от СЕУ на свое заседание на 28.01.2015 г. – да се изпратят официални запитвания до Асоциацията на банките в България и до Министерството на правосъдието относно потенциалната възможност за заменяне на квалифициран електронен подпис с пин, пик и други такива номера, издавани от различни институции. Той цитира и няколко важни пасажа от официалните отговори както следва:

**Асоциация на банките в България:**

*Смятаме, че прилагането на квалифицирания електронен подпис за електронна идентификация е най-сигурно и достатъчно надеждно от гледна точка на възможността за гарантиране на неотменимостта и интегритета в сравнение с използването на пин или пик, поради което не бихме могли да подкрепим извършването на описаната замяна. Квалифицираният електронен подпис е законово признат електронен инструмент за идентификации и има сила на саморъчно поставен подпис, съгласно изискванията на чл. 13, ал. 4 от Закона за електронни документи и електронния подпис...*

*Предвид изложеното, налице са съществени разлики в съдържанието и нормативната уредба на административните услуги, които ще бъдат предлагани в рамките на електронното управление и платежните услуги, предлагани от банките по електронен път. С оглед на това, използването на едни и същи средства за идентификация може да бъде обсъждано само и единствено в случаите, когато идентификаторите се издават по процедура, утвърдена на европейско ниво и въз основа на това националното и европейското законодателство признават средството като важещо пред всички правни субекти. На тези изисквания понастоящем отговаря единствено квалифицираният електронен подпис, по смисъла на ЗЕДЕП.*

**Министерство на правосъдието:**

*Във връзка с решение на Съвета за електронно управление, съгласно Протокол № 1 от 2015 г., Министерството на правосъдието изготви настоящото становище относно заменянето на квалифицирания електронен подпис (КЕП) с ПИК, ПИН, издаван от различни институции – НОИ, НЗОК, НАП, общини.*

*Към настоящия момент КЕП е законово признат инструмент за електронно волеизявление и същевременно средства за електронна идентификация, КЕП е еквивалент на собственоръчно поставен подпис и съответно, има доказателствена стойност в съда.*

*Съгласно Регламент ЕС910/2014 г, прилаганите средства за електронна идентификация следва да се определят, в зависимост от тяхното предназначение и изискванията за ниво на сигурност и защита на личните данни на потребителите. С оглед постигане на трансгранична оперативна съвместимост и сигурност на транзакциите, в разпоредбите на § 14 от Регламента е уредено, че признаването на електронната идентичност между държавите-членки е задължително само когато нивото на осигуреност е „значително“ или „високо“, които нива на сигурност, по смисъла на § 16, са приравнени на ниво 3 и 4, съгласно ISO 29 115. Тези разпоредби изключват възможността средствата за електронна идентификация, като ПИК и ПИН да бъдат признати по смисъла на Регламента.*



*Използването на ПИК или ПИН, както и други по-прости и удобни средства за електронна идентификация (като например саморегистрация на потребители) е допустимо в случаите, когато се касае за електронни транзакции, които не изискват електронно волеизявление и/или от които не произтича риск за сигурността на личните данни на потребителите.*

*Всеки администратор на първични данни би следвало да оцени потенциалните рискове за всеки вид транзакция и да определи адекватни методи за достъп до всяка конкретна административна услуга.*

*За удостоверителни услуги в електронна форма задължително е използването на КЕП за доказване на тяхното авторство, както и автентичността на информацията. Като пример: заявяването на електронно свидетелство за съдимост. Извършва се с електронен подпис на заявителя, а издаденото електронно свидетелство за съдимост е подписано с квалифицирания електронен подпис на министъра на правосъдието. Така са спазени нормативните изисквания електронната форма има стойност на официален документ.*

С това решението на Съвета за електронно управление е изпълнено – налице са становищата на АББ и на МП. И двете институции са на мнение, че квалифицираният електронен подпис не би трябвало да бъде заменян от ПИК или ПИН, когато става дума за волеизявления и транзакции, свързани с лични данни. Това в никакъв случай не означава, че ПИН и ПИК, издавани от различни институции, не бива и не може да бъдат използвани за справочни услуги. Напротив, това е едно улеснение за всички потребители на електронни услуги, предоставяни от различни администрации.

Неудобството е, че е налице набор от ПИН-ове и ПИК-ове, които са несъвместими помежду си. След влизане в сила на електронния идентификатор, би било логично съответните администрации да си преработят системите така, че да позволяват идентификация с ЕИД и постепенно да отпада тази хетерогенност в средствата за идентификация.

След изложението на В. Борисов, председателят на СЕУ даде думата за коментари и мнения.

Министърът на финансите В. Горанов призова секретаря на СЕУ да предоставя предварително материалите за заседанията на съвета. В. Борисов прие критиката и обясни, че по независещи от него причини се е наложило да запознае Съвета с постъпилите становища на място, а не предварително. Той пое ангажимент това да не се повтаря като практика.

Р. Бъчварова постави въпроса за това как ще се съвместяват ПИК и ПИН с новия електронен идентификатор? Ще има ли преходен период, през който съвместно ще работят ПИК, ПИН и еИД?

В. Борисов увери членовете на Съвета, че ще има преходен период, защото няма как от следващия ден след влизане в сила на Закона за електронна идентификация, да отпаднат всички системи, които са използвали ПИК и ПИН.

Р. Бъчварова уточни, че новият електронен идентификатор няма да е задължителен и потребителите ще могат да продължат да се идентифицират с ПИН и ПИК, но само за справочни услуги.

Петър Иванов (БАИТ): Имам следния коментар. По регламент, ако в България се въведе електронна услуга, която изисква идентификация на ниско ниво, да речем, само с ПИК или ПИН, тя трябва да може, първо, да допуска чужденци, които имат идентификация на по-високо ниво да се възползват от тази услуга. Тоест, в България, ще трябва да осигурим услугата да работи задължително и с други идентификатори, включително и с електронната идентификация – тази, която е по смисъла на Закона за електронната. Няма от това да спестим пари. Само правя коментар и забележка какво трябва да се случи.

В същото време тези българи, които имат ПИК или ПИН, четейки регламента, на практика с него извън България няма да могат да правят абсолютно нищо. Извън България ПИК и ПИН няма да работят, защото те не влизат в ниво 3 и ниво 4 по ISO 29115.

Другото, което в момента се опитвам да се сетя, но не мога да го кажа абсолютно еднозначно, може ли да въвеждаме различни електронни идентификатори, тоест по регламента дава ли ни възможност един човек, да речем, един електронен идентификатор по смисъла на закона и още четири пика за четири други различни услуги? Това е нещо, което леко ме притеснява. Надявам се тук да има някой, който да може да отговори на този въпрос.

**След края на разискванията по първа точка Съветът за електронно управление прие за сведение представените становища на АББ и на МП.**

## **2. Представяне на проектозакона за електронната идентичност**

**Докладва:** проф. д-р Георги Димитров, член на междуведомствената работна група, изготвила проекта на закон

Проф. Димитров запозна накратко членовете на СЕУ с основните постановки на Закона за електронната идентификация и даде някои разяснения относно разликата между електронен подпис и електронен идентификатор.

Подпис се полага тогава, когато едно лице е съгласно с едно изявление и затова го подписва – първо. Второ, по подписа може да се идентифицира лицето, защото при анализ чрез графологична експертиза може да се установи дали той го е подписал. Трето, понеже подписът е под документа, той слага край на документа, тоест, осигурява интегритета на документа, че нищо не може да промени волята му оттук насетне.

Самият подпис отдолу под документа нищо не ни казва, освен ако няма име и ако аз трябва да докажа, че аз съм подписал документа, трябва офлайн да се идентифицирам, трябва да си покажа личната карта, която е документът ми за самоличност. Тогава проверяващият ме идентифицира, тоест, извършва проверка на идентификация дали аз съм аз, гледайки снимката ми – това е идентификацията и след като я идентифицира и вярва, че това е моят документ за самоличност, вярва на удостоверените в него факти от МВР чрез издаването на този документ. А законът, който казва, че трябва да се вярва на МВР за този документ, е Законът за българските документи за самоличност. Така че, така се удостоверява моята самоличност и се идентифицира, че аз съм този, който се явявам с този документ, а подписът е само изявление, тоест само белег за авторство върху документ, върху документ и върху нищо друго. Само върху документ. Аз подписвам документ, когато съм съгласен с него и искам да настъпят някакви последици и слагам край на документа.

Така че, подписът доказва авторство, съгласие, неотменимост и интегритет; нищо друго. Той не служи за идентификация на лицето, защото, първо, няма такъв механизъм, с който чрез подписа се идентифицира едно лице – имам предвид електронния подпис. Няма такъв механизъм и второ, никъде в закон – тоест аз поне не познавам такъв закон нито в България, нито в чужбина, който да казва, че чрез електронния подпис се удостоверява самоличността на лицето, няма никакви данни, няма такъв закон. Това е първото.

Във всички държави законодателствата, тоест националните юрисдикции са се чудили как да осигурят вариант, при който да може да се обезпечат тези две проверки - идентичност и самоличност. И след дълги обсъждания в крайна сметка до момента нямаме единна визия как това трябва да стане на ниво Европейския съюз. Затова европейският Регламент 910, който е факт от юли миналата година казва: всяка държава си го решава само на национално ниво, а когато реши задачата на национално ниво тя трябва да привърже, да нотифицира Европейската комисия за своята национална схема за електронна идентификация и да я привърже с един специален конектор, който да позволява ба граждани от една държава със своя идентификатор да се идентифицира пред българския орган и на български граждани със своя идентификатор пред чужд орган. Това трябва да се случи и това казва Регламент 910. Той казва, че когато страните членки изработят такъв национален модел и той е за нуждите



на публични услуги и за осигуряване на трансгранично удостоверяване в рамките на единния пазар, тогава това, което казва В. Борисов е вярно - че трябва да има ниво на сигурност 3 или 4, което изисква допълнителни технологични, организационни и други мерки. Те, съгласно стандарта ISO 29115 осигуряват това ниво на сигурност. Така че регламентът не установява единен модел, той просто казва, че страните-членки, за нуждите на онлайн идентификация трябва да обезпечат такъв инструмент, който да бъде един. Той трябва да се използва за нуждите на публичните услуги онлайн. Моделът, който е заимстван при разписването на проекта за електронна идентификация не е оригинален български. Това е модел, който работи в Австрия от много години, всъщност цялата австрийска концепция за електронно управление почива върху тези два инструмента – електронния подпис и електронната идентификация като удостоверяване на това кой е от другата страна, каква е самоличността на лицето. Той почива върху следното нещо, залегнало и в нашия модел - създава се един електронен документ, който се нарича удостоверение за електронна идентичност. На практика това е аналога на личната карта в електронната среда и има много по-малко атрибути. Само пет – имената на кирилица на човека, имената на латиница, ЕГН, дата на раждане, когато няма ЕГН, примерно има ЛНЧ, и електронен идентификатор, който представлява криптирано ЕГН. За да не може този документ просто да се копира и да се използва, той винаги трябва да се привърже към конкретно устройство, върху което може да бъде записан. На практика без това устройство този документ не може да бъде използван. Затова привързването на този електронен документ с конкретно устройство става чрез второ удостоверение, като подписа на първия документ се прикачва към уникалния номер, идентифициращ конкретното устройство. И така записан веднъж документа върху това устройство се постига невъзможност за копиране. Така че, за да се идентифицираме по електронен път, трябва задължително да държим този инструмент в ръцете си. Това, което трябва да се подчертае е, че законът почива върху плурализъм на използване на устройствата. Стига едно устройство да е разпознато от Европейската комисия, която ще обяви съответния стандарт за устройство за сигурно създаване на подписи. То може да бъде същото каквото се използва за квалифициран електронен подпис, смарт карта, токън, криптомодул, смартфон. Тоест електронният идентификатор може да бъде записан включително върху смартфон стига да има такъв чип в него. Второто позитивно нещо, което се въвежда със закона е да имаме възможност за повече от едно удостоверение за електронна идентичност - върху различните устройства е възможно да има различни удостоверения. Това е така, защото самото удостоверение е едно. То съдържа едни и същи данни с подписа на МВР, но е привързано към различни устройства посредством второто удостоверение, което позволява едно лице да има няколко удостоверения.

Преди няколко години, когато се създаваше основата на този модел обсъждахме, че за да не се товари МВР с допълнителна административна тежест, изискваща и много познания във връзка с персонализирането, използване на устройства и т.н., допускаме възможността МВР да се подпомага от особени категории лица, които се наричат администратори на електронна идентичност. Това са специализирани лица, които чрез своеобразна регистрация в МВР доказват, че имат необходимата техническа инфраструктура, знания, квалифициран персонал и могат да действат като проверяващи от името на МВР. Това могат да бъдат банки, доставчици на удостоверителни услуги, мобилни оператори, нотариуси, всеки, който може да обезпечи съответната инфраструктура и сигурност. Така гражданинът ще може да влезе в първия клон на банката (или друг офис на администратор на електронна идентичност) и да каже „искам удостоверение“, а не да ходи в МВР да се реди на опашки и да товари МВР с излишна работа. Администраторът идентифицира лицето чрез личната му карта и подава една електронна заявка до МВР. Всичко това се случва в реално време. В МВР се проверява дали представения от гражданина документ е валиден, а в ГРАО дали човекът е жив? При успешни проверки МВР генерира удостоверението и чрез администратора то се записва на съответното устройство. Затова тези лица ще подлежат на регистрационен режим и трябва да отговарят на определени изисквания. Тези изисквания са много тежки и подлежат на контрол от страна на държавата. За издаването на удостоверение за електронна идентичност се дължи държавна такса.

Как работи електронната идентификация като процес? Гражданинът със своето устройство, било лична карта с чип, върху която е записана или върху смартфона или другото устройство, влиза в системата на съответна институция, било държавна, било частна, и към системата отива само неговия електронен идентификатор, само неговото криптирано ЕГН. Оттам насетне институцията, предоставяща услугата все още не знае кой е той и дали той наистина е той, дали в интернет наистина той е седнал пред компютъра? Организацията, която предоставя услугата пита един специален център за електронна идентификация, който се създава към министъра на транспорта, информационните технологии и съобщенията, който извършва тези две проверки. Първо, влиза в картата на човека, изчита двете удостоверения, проверява дали се използва от точно тази карта; второ, пита МВР дали това удостоверение е валидно издадено, дали не е прекратено предварително и тогава центърът за електронна идентификация връща към съответната институция, предоставяща услугата, личните данни изчетени от удостоверението. Едва тук се получават личните данни, примерно три имена и ЕГН.

Центърът за електронна идентификация преценява какви лични данни да пусне към администрацията предоставяща услугата, защото ако институцията няма право да те идентифицира по закон, тоест по закон няма задължение и право да те идентифицира, да кажем може да се подаде сигнал за малтретиране на дете, за него не се изисква да се идентифицира лицето. Тогава се подава само факта „да, удостоверението е валидно“. А може да се подаде информация само „да, лицето е над 18 години“, което е извършило операцията, примерно справка. Или само трите имена, или само ЕГН-то. Тоест каква комбинация от лични данни ще се върне към доставчика на услугата от центъра за електронна идентификация зависи от това по закон този орган какви данни има право да получи. Ако е частно лице, той трябва да се регистрира като администратор на лични данни в Комисията за защита на личните данни, за да обработва тези лични данни. Хубавото нещо е, че законът дава възможност такива центрове за електронна идентификация да се създават и от частни лица, те също преминават на особен регистрационен режим. Възможно е да има браншови такива, примерно банките решават да си създадат свой център.

Всички центрове за електронна идентификация се регистрират в регистър в МВР като задължително има един държавен, който е към министъра на транспорта, информационните технологии и съобщенията. Проверките на електронната идентичност за държавните органи са безплатни, а за частни лица не са.

Каква информация може да се връща като лични данни към проверяващия услугата, се вписва в административен регистър, който доколкото разбирам, тепърва ще се изпълнява подобен проект по. В него ще се укаже какви лични данни органът, който предоставя административни услуги има право да получи по закон.

Това, което въвежда законът и е много оригинално и е изключително революционно, е една втора фигура, която се нарича регистър на овластяванията. Това е своего рода регистър на пълномощните. Когато едно лице иска да се представлява от друго лице пред някакъв държавен орган, примерно пред НАП или Агенцията по вписванията, за да подаде и да извърши изявление от мое име, това лице като пълномощник влиза в този регистър идентифицира се, подписва овластително изявление, с което казва „упълномощавам Васил с еди какво си ЕГН да ме представлява за еди кои си действия пред еди кои си органи“. И тогава какво става? Тогава Васил, когато с неговото удостоверение за електронна идентичност влиза пред съответния орган, казва „подавам данъчна декларация от името на Георги Димитров“, НАП веднага автоматизирано пита регистъра „Васил представлява ли ме мен за тези действия“, представлява ме, и така се прави автоматична проверка и пуска Васил да подаде декларацията от мое име. Нещо като електронен нотариат, електронно пълномощно. Аз ако реша да си оттегля пълномощното мога да го направя веднага, влизам в регистъра, изтривам записа, с който съм го овластил и той престава да ме представлява, той вече не може да ме представлява, защото тази проверка ще бъде отрицателна. Така се решава проблемът с носенето на пълномощните в електронната среда.

Това е горе-долу моделът на закона. Този модел на практика е единственият, който е идентифициран след задълбочена работа, който извършва истинска идентификация в реално



време. Защото моделите, които са свързани с ПИК/ПИН, за да работят гражданинът трябва преди това да отиде да се идентифицира с личните си документи за самоличност и се надява, че веднъж като се идентифицира му се генерира ПИК и му се даде, оттук насетне вече той ще си пази ПИН-а и няма да го дава на никого. Но на практика в момента, в който той подава ПИН-а и го пуска, няма сигурност, че той го държи. Може някой друг да му го е видял. Тоест в този процес липсва моментът на онлайн идентификация или проверката на идентичността. Това е, което липсва. Това не означава, че в една държава не може да има и пет схеми за идентификация, може да има и десет, и четиридесет. Регламентът не ограничава колко схеми ще има в държавата. Така че може да има ПИН, ПИК, ПУК, каквото искаме. Но ако има национален модел, който да се използва за публични услуги и за осигуряване на трансграничен достъп до услуги, каквото е едно от изискванията на „Европа 2020“, тогава вече трябва да имаме такава схема. Тя може да се добави към съществуващите, разбира се, и да си работи независимо от тях. А дали старите трябва в някакъв момент да спрат да се ползват или ще продължават да съществуват, е въпрос на управленско решение. Двете неща не се конкурират. Ако се възприеме такъв национален модел и се нотифицира комисията по начин, по който тя ще каже през месец юли 2015 г., той ще бъде разпознаваем като достатъчно ниво на сигурност и достатъчно сигурен за нуждите на трансгранично предоставяне на онлайн административни услуги.

С това приключи представянето на проекта на закон за електронната идентификация.

Председателят на СЕУ даде думата за въпроси и мнения.

ПЕТЪР ИВАНОВ: /БАИТ/: Два въпроса. Единият е, наличието на електронна идентификация по този закон трябва да дава право на човек да се идентифицира във всяка една система, нали така? Тоест ако системата предвижда някакви алтернативни методи за идентификация, тя трябва задължително да дава възможност за достъп и с електронен идентификатор.

И втори въпрос, ако допуснем, че утре този закон бъде гласуван, според сроковете, които са предвидени в него, кога може да бъде издаден първият електронен идентификатор?

Проф. д-р Г. Димитров - На практика първите електронни идентификатори бяха генерирани тестово преди две години. Тогава бяха издадени пет хиляди карти, които бяха раздадени. Но те така или иначе без закон не могат да работят.

Това, което законът е предвидил е да се даде достатъчно време, за да може организационно и МВР, и МТИТС, и всички лица да мога да добавят този начин като универсален за цялата държава - и в частния и в публичния сектор. В този срок ще се регистрират администратори на електронна идентичност, центровете за електронна идентификация, МВР ще се подготви и т.н., ще се създаде регистър, проверки и т.н. Този срок е година и половина, тоест юли 2016 г., когато влиза в пълна сила и регламентът. С други думи едновременно с влизането в сила на регламента влиза и в сила и нашия закон. Така с влизането в сила на регламента България ще има готовност за национален модел.

Р. Бъчварова постави въпроса за възможността за стартиране на издаването на електронни идентификатори преди изтичането на този 18 месечен срок.

Отговорът бе, че няма проблем сроковете да се скъсят. Всичко е въпрос на организационна и технологична готовност, а и на финансова възможност.

Р. Бъчварова обобщи възможността за запис на удостоверение за електронна идентичност върху новите лични карти, които ще съдържат чип. Подмяната на личните карти предстои да започне през следващата година.

Проф. Димитров изрази становище, че няма никакъв проблем да се запише удостоверение за електронна идентификация върху лична карта с чип. Проблемът би възникнал ако човек отиде със смарт телефона си в МВР и поиска там да му се запише идентификатора.

Р. Бъчварова сподели, че в МВР ще се персонализират само личните карти с чип, а всички останали възможности – при администраторите на електронна идентичност.

В. Величков добави, че и понастоящем от общо 23 вида лични документи, които издава МВР, 2 от тях всъщност са чип карти, които съдържат практически електронна идентификация. Най-известни са сините карти, които са разрешение за работа за чужди



граждани. Чисто технологично и настоящата система, която се използва би могла да издава и да персонализира върху носители, които общо взето отговарят на същия стандарт като тези, които са на пилотната система за електронна идентификация. Тук вече е въпрос на ангажменти и бизнес процес в МВР, дали това може да се случва преди юли 2016 г.

Р. Бъчварова: Има работна група, която точно сега разработва този въпрос и скоро ще го решим как да стане. За мен най-големите въпросителни са около тези, които се явяват доставчик на тази услуга от страни и самия процес на тяхното лицензиране или регистриране, тук може да се спънем.

Г. Димитров: Изискванията към тези лица ще бъдат същите и по-тежки, като към доставчик на удостоверителни услуги, който издава удостоверение за електронен подпис. На практика той трябва да притежава квалифициран персонал; да докаже, че има квалифициран персонал, сигурни системи, система за информационна сигурност, която работи в съответното ниво, да има застраховка, отговорност за вреди. Той действа на практика, като лице, осъществяващо публична функция, като доставчик на удостоверителна услуга.

Ст. Кочев: Бизнесът по принцип обсъди проекта на закона и подкрепя улесняването и повишаване сигурността на въвеждането на нови електронни услуги, въобще за работата на електронното управление, както и за интегрирането ни в Европейския съюз. Има коментар към тези ПИК, ПУК, ПИН и т.н. Според нас трябва да се въведе някакъв период на валидност, за което време тези ПИН, ПУК и ПИК и т.н. да изчезнат постепенно. Това е чисто от гледна точка на граждани, институции и пр. Процесът на работа сигурно ще се улесни. Освен това ще се избегне объркване около идентификации кое е валидно, кога е валидно, къде е валидно и пр., както и това, което колегата каза - извън страната, в Европейския съюз тези неща не важат. В тази връзка също в момента, в който влезе в сила законът би било добре да се ограничи въобще създаването и генерирането на такива ПИН-ове, кодове въобще, за да може в крайна сметка в някакъв момент да се излезе само с един, какъвто и да било той носител и електронна идентичност, било то електронен подпис или каквото и да е там.

С. Цветарски: Надявам се, че ние не нарушаваме протокола, но исках да коментирам това, че електронната идентификация за статистиката е изключително важна и полезна. И ще дам един пример за едно бъдещо преброяване и то ще реши страшно много от въпросите и усилията, които влагаме, за да контролираме обхвата на нашето преброяване. Това по отношение на физическите лица. Но въпросът ми е, как стои въпроса с юридическите лица? Как те биха могли да бъдат идентифицирани така, че ние да можем да получаваме съответните отчетности? В момента върви кампанията за годишно отчитане и съответните отчети да бъдат подписани и идентифицирани електронно, посредством тези средства.

Проф. д-р Г. Димитров - Системата, която е предложена, освен самия електронен идентификатор, въз основа на него могат да се генерират секторни електронни идентификатори. Те позволяват допълнителното криптиране на вече създадения електронен идентификатор и разделянето му, така че в определен сектор едно лице, ако се идентифицира от този сектор да не може по никакъв начин друго лице, което е извън този сектор да го идентифицира. Примерно за нуждите на електронното гласуване този инструмент може прекрасно да се използва, защото той може да раздели самоличността на лицето от факта, че е гласувало. Този инструмент го позволява чрез т.нар. секторни електронни идентификатори. Предвидено е Министерският съвет, съвместно с Комисия за защита на личните данни, министърът на вътрешните работи, министърът на транспорта, информационните технологии и съобщенията да определят секторите, които имат нужда от секторни електронни идентификатори. Това е, когато трябва да има капсулиране на възможността отвън някой, по какъвто и начин, да идентифицира лице вътре в сектора.

Р. Бъчварова – А за здравен статус?

Проф. д-р Г. Димитров - Категорично. Здравен статус, съдебна система, електронно гласуване, много, много сектори. Освен за електронна идентификация се дава решение за идентификация само на физически лица, защото само такива лица се идентифицират в електронния свят. Когато има нужда едно лице да представлява юридическо лице, примерно аз представлявам търговеца Х, тогава проверката ни става чрез електронния идентификатор,

а фактът дали представлявам търговеца X става чрез проверка при първичния администратор на данни – Агенцията по вписванията. Тоест, пита се Агенцията по вписвания – този представляват ли те по закон, представлява те. Когато юридическо лице трябва да упълномощи физическо лице това става в регистъра на овластяванията. Там едно юридическо лице, един търговец може да си овласти търговски пълномощник и той да извършва действията от негово име.

Д. Янчева: Хубаво е, че ще може онлайн да се провери дали дадено лице е упълномощено и овластено да представлява определено юридическо лице. Но дали то има право самостоятелно да извършва действия от името на фирмата или на предприятието на юридическото лице и да гарантира за достоверността на това, което е записано? Говорим за счетоводни и данъчни документи. Това е въпросът.

Проф. д-р Г. Димитров - когато говорим за представителство по закон проблем няма. Защото в държавно-организиран регистър винаги се вписва факта как едно физическо лице представлява едно юридическо лице. В Търговският регистър пише кой, как представлява – заедно, поотделно, всеки, до и т.н. Когато говорим за овластяване, което произтича от пълномощно, тогава влиза в сила Регистър на овластяване и там е въпрос на реализация как човек ще каже това лице как ме представлява – заедно с някого, самостоятелно и т.н. Всичко вече е въпрос на конкретна реализация на самия регистър на овластяванията, но да – този механизъм ще позволява да се определя особен начин на упражняване на представител, тоест – на определяне на обема на представителната власт и начина на представляване.

### **След края на разискванията по първа точка Съветът за електронно управление прие за сведение представения проект на закон за електронна идентификация.**

По предложение на председателя на СЕУ следващите точки от дневния ред бяха разместени.

#### **7. Представяне на статистика от ИСПОДСА за броя реално използвани лицензи за продукти на Майкрософт и информирание за процедурата**

**Докладва:** Л. Сеизова – началник отдел „Информационно обслужване“ в Администрацията на Министерския съвет

Л. Сеизова представи накратко данните от предварително раздадения доклад, съдържащ статистика ИСПОДСА за броя реално използвани лицензи за продукти на Майкрософт. По данни, отчетени в системата, от 576 административни структури броят на лицензиите за операционни системи е 120 961. Разпределени по версии на операционна система, представям на вашето внимание следните данни: 58 470 или 50% ползват „Windows 7“. На второ място следва „Windows\_XP“, почти 36% и около 10% са използващите, според отчетните данни „Windows 8“ и „Windows 8.1“. Съгласно отчетните данни се вижда, че използваните в доклада за състоянието на администрацията лицензии за операционни системи са 24 961 повече от това, което държавата е закупила централизирано за нуждите на държавната администрация по корпоративния договор за продукти на „Microsoft“, именно 96 000 лиценза. Искам да ви обърна внимание, че от тези 96 000 закупени централизирано лицензии с безсрочно право на ползване 12 455 през годините са раздадени на структурите на съдебната власт. По този начин общият брой на използваните по договора за нуждите на държавната администрация са със 37 416 по-малко от отчетените в доклада данни. Трябва да споменем, че когато са закупувани лицензите някои административни структури не са прилагали Закона за администрацията. При обявяване на последната обществена поръчка през 2012 година Законът за администрацията не се прилагаше по отношение на Националната здравноосигурителна каса, НОИ, Държавен фонд „Земеделие“, Комисията за финансов надзор. Тези структури в момента отчитат използвани лицензии и те са в тази обща бройка 120 000 лиценза, но реално не са обезпечени с лицензии от корпоративния договор. Има други административни структури, които са получили лицензии по корпоративния договор, но сега в доклада за състоянието на администрацията отчитат по-голямо количество брой операционни системи. Това означава, че те са провели обществени поръчки и със собствен бюджет са закупили допълнително необходими лицензии. Такива са например НАП, която има раздадени 6 200 лиценза по корпоративния договор, а реално



отчита в доклада за състоянието 9 300, Агенция за социално подпомагане – 3 700 раздадени централизирано, отчитат 5 010, Агенция по заетостта – 1 900 раздадени, отчита използвани лицензи 3 600, Министерство на вътрешните работи при раздадени 12 600 отчита 13 100.

По втората точка относно информацията за предстоящата процедура, мога да ви кажа следното. На предходното заседание бяха обсъждани два варианта за техническа спецификация на продуктите на „Microsoft“. Преобладаващо беше мнението, че трябва да се работи по Вариант 2, тъй като той отговаря в по-голяма пълнота на Стратегията за електронно управление, както и на целите на Оперативна програма „Добро управление“. Процедурата е приключила, документацията е изготвена, предстои нейното обявяване до края на тази седмица по варианта, който Съветът за електронно управление приоритетно одобри и миналия път, именно Вариант 2. Ще се предоставят и услуги от типа „Premier Support“ и „Atap“ в досегашния обем – 3 600 часа за „Premier Support“ и 3 000 часа за услугата „Atap“. Тези услуги по предходния договор са изразходени изцяло. Показали са своята ефективност при внедряване на технологични решения на Microsoft платформи.

Р. Бъчварова – и стойността на поръчката е колкото при предишната процедура?

Л. Сеизова – Да, точно така.

**След края на разискванията по точка 7 Съветът за електронно управление прие за сведение представения доклад.**

#### **4. Преместване на Интернет възела, договора за доставка на Интернет за Държавната администрация и закупените IPv4 адреси от Администрацията на Министерски съвет в Изпълнителна агенция Електронни съобщителни мрежи и информационни системи**

**Докладва:** В. Величков – Съветник към заместник министър-председател по коалиционна политика и държавна администрация

Това е една неособено сложна мярка, която има за цел нещата да си дойдат по местата по отношение на доста съществена част от базовата инфраструктура, която обслужва голяма част от онлайн административните услуги и е-услугите на администрациите. Понастоящем администрацията на Министерския съвет се явява централизиран доставчик на интернет за държавната администрация. Това на практика не се получава така, тъй като поради непрекъснатите спирания, бавната скорост на услугата, липсата на адекватна възможност за защита на тази връзка всички администрации си пазаруват – всеки, както може, откъдето може интернет и се оправят със собствените си бюджети. Горедолу Министерският съвет купува 500 Mbps, по същите статистики от системата се оказва, че сумарно администрациите пазаруват отделно около 27 000 Mbps капацитет. Особено когато разгледаме общинското ниво там положението е много лошо. Има общини, които харчат повече за интернет, отколкото Министерство на финансите или Министерство на вътрешните работи и същевременно има такива общини, които въобще нямат връзка с интернет.

Другото важно нещо е, че IP адресите версия 4 от две години вече са изчерпани. Преди години държавата си е купила 8 700 бр., които се държат от Министерския съвет и около 512 бр. са в рамките на Министерство на транспорта, информационните технологии и съобщенията. Тези адреси се раздават на различните администрации, по неясно какъв начин. В момента има остра липса на адреси. Тоест, ако трябва да се пускат нови услуги, нови портали, нови сайтове, се оказва, че държавата няма IP адреси. Целта на преместването, което предлагаме, е да се промени схемата - интернетът да се доставя в резервираните интернет възли на Изпълнителна агенция „ЕСМИС“, която държи цялата национална мрежа на държавната администрация. Министерският съвет да си стане потребител на интернет, а „ЕСМИС“ да осигури 24-часова поддръжка и ясно ниво на обслужване.

И същевременно скоростта да се вдигне чрез свързване на интернет възела в ЕСМИС с няколко точки в българското интернет пространство, в което абсолютно всички български телекоми са се свързали. И горедолу за около 700 евро на месец получават 10 000 Mbps, Икономииите от мащаба биха били доста сериозни. Същевременно ще се прехвърлят всички раздадени IP адреси за управление от ЕСМИС. Така ще се направи инвентаризация и ще се

види кои администрации реално ги ползват, кои не ги ползват. Тъй като вървим в посока държавен облак за по-голямата част от администрациите, без може би осемте най-големи, това ще спести огромно количество заети в момента IP адреси.

Според грубите статистики от ИСПОДСА за разходите за комуникации на държавната администрация се харчат около 35 милиона на година. Това е една силно подценена цифра. Конкретно за пренос на данни горе-долу 90 % от администрациите са подали нулеви данни. Тук интересният ред е сумата за фиксирана телефония - 18 милиона на година. Давайки възможност на администрациите да се свържат към мрежата на ЕСМИС, не само директно физически, но и през криптирани канали през интернет, и ако има и бърз и стабилен интернет в самата агенция ЕСМИС, ще бъде възможно да се въведе IP телефония и всякакви други форми на IP комуникация. Това ще обезсмисли наличието на множество фиксирани телефонни линии. МВР вече използват IP телефония от няколко години и са спестили доста милиони на година от фиксирани телефони. Предлагаме да се започне с една инвентаризация на това какво има в администрацията на Министерски съвет, да се направи един бърз план за едно такова прехвърляне към ЕСМИС, което ще включва прехвърляне на договори, евентуално някаква промяна в правила, процедури, подзаконови актове. ЕСМИС да предложат едни общи условия, така че да е ясно на администрацията какво ниво на обслужване получава и следващата крачка е поетапното преместване на нещата. Мисля, че с МТИТС сме на общо мнение, че това е изключително важно, тъй като в момента е парадоксално ЕСМИС да отговаря за поддръжката на хиляди километри оптична мрежа и да пренася данни, всичко да е много резервирано, всичко да е в бункери, а интернета на държавата да минава през мазето на Министерски съвет. Цялото това упражнение няма да коства нищо на държавата.

Председателят на СЕУ даде думата за коментари и обсъждания

В. Борисов: Аз искам формално да предложа за следващото заседание на Съвета за електронно управление да подготвим пакет документи, които да улеснят прехвърлянето на тази дейност от администрация на Министерския съвет към Изпълнителната агенция ЕСМИС и да представим пакета документи с анализи и т.н. Чисто формално го предлагам като решение на съвета, съветът да натовари мен като представител на Министерството на транспорта, информационните технологии и съобщенията, което е принципал на агенцията, да изготви такъв пакет на документи, който разбира се ще ви бъде изпратен.

Р. Бъчварова: Аз съм съгласна с това. Предлагам ви да го подкрепите или да изразите мнение. Но не виждам какъв е смисълът да изчакаме следващото заседание на Съвета за електронно управление, за да се разглеждат. Това са документи, които са свързани с вътрешни технологични решения и процеси, за да можем по-бързо да го приемем.

**След края на разискванията по точка 4 Съветът за електронно управление възложи на секретаря на СЕУ в качеството му на представител на МТИТС да подготви пакета документи за прехвърляне на цялостната дейност по преместване на Интернет възела, договора за доставка на Интернет за Държавната администрация и закупените IPv4 адреси от Администрацията на Министерски съвет в Изпълнителна агенция Електронни съобщителни мрежи и информационни системи.**

## **5. Представяне на проекта за Единна входна точка**

Председателят на СЕУ даде думата на Д. Янчева (НСИ)

Д. Янчева направи кратка ретроспекция на проекта за единна входна точка за подаване на ГФО (годишните финансови отчети) от бизнеса. Преди отчетната 2007 г. предприятията предоставяха един екземпляр от отчета за дейността си в НСИ. В офиса на НАП или по пощата на хартия и съответно в Агенцията по вписванията, по различни закони предприятията бяха задължени, и сега са задължени, да представят една и съща информация.

За отчетната 2008 г., тоест 2009 г. от 1 януари започна да работи тази единна входна точка и всичко всъщност се свежда до склада от данни (data warehouse), който се получава



през информационна система “Бизнес статистика“, която НСИ е разработил и тези, които не могат да я използват, предават в НАП заедно с годишната данъчна декларация този отчет и съответно той се въвежда, за да стане пълна базата данни.

Днес (01.04.2015 г) завърши една част от кампанията, имаме още един месец и мога да ви кажа, че тези от юридическите лица, които прилагат двустранни счетоводни записвания вече сме достигнали 85 % онлайн въвеждане на отчетите. Предложенията ни беше и Агенцията по вписванията да се включи, но по една или друга причина досега това не става. Вече имаме и европейски нормативни документи, които позволяват това нещо. Само с едно допълнение към Закона за статистиката това може да стане нормативен факт. Говоря за нормативни документи, които изискват съответно решение, тоест приемане в Народно събрание. Не говоря за вътрешно нормативни уредби, които сравнително лесно се коригират, когато има добра воля.

Идеята е този склад за данни освен от нас и от НАП да бъде споделен и от Агенцията по вписванията. Самата система „Бизнес статистика“ ще позволява генериране на PDF документи, които ще бъдат електронно подписвани. Поне за сега това е изричното изискване на Агенцията по вписванията. Заедно с докладите, които са необходими, един от двата доклада, които по нормативна уредба трябва да бъдат прикачени към този пакет, да бъдат подписани с два електронни подписа вместо с три и да бъдат изпратени в Агенцията по вписванията. В техническото задание е разписано какви допълнителни функционалности трябва да реализираме в нашата система. Ще разработим и консолидираните отчети, които ще могат да се подават до 30 юни, защото такъв е срокът сега за Агенцията по вписванията. Иначе с НАП сме уеднаквили сроковете до 30 април. Целта е да имаме по-бърза, качествена и навременна информация, а не в различните държавни администрации да има различни данни за едно и също юридическо лице.

Това е същността на Единната входна точка. Това, което може би господин Горанов очаква като предварителна оценка, е около един милион лева заедно със софтуер, хардуер, лицензии и съответно това, което ще се изисква като различни допълнения към инфраструктура и мрежови елементи в НСИ и в НАП.

Може би трябва да кажа, че нямаме този един милион в нашия бюджет, защото общо взето толкова са ни по бюджет всичките капиталови разходи за цяла година. Ако решим, че трябва го направим по някоя от оперативните програми, например „Добро управление“, съгласно европейското законодателство, мога да кажа, че имаме опасения да не нарушим и европейското и нашето законодателство по отношение на статистическа конфиденциалност. Ако разработката изцяло отговаря или тоест много пунктуално отговаря на условията за такива продукти по ОПДУ. Защото имаме два регламента - 223 и 557, които по един или друг начин са транспонирани в нашия Закон за статистиката, което не ни позволява публичност на това, което събираме като информация. Едно от тези изисквания по ОПДУ е точно това.

В. Величков - Само един бърз коментар. Става въпрос за отваряне на данните, които така или иначе в момента са публично достъпни, става въпрос за годишните финансови отчети.

Д. Янчева - Това, за което сме получили съгласие от собственика на отчета, няма никакъв проблем. Но другите, които не са дали съгласие, просто няма как да го направим публично.

В. Величков - Това е въпрос на прецизиране при реализацията, тъй като в досега действащото законодателство когато търговците публикуват годишните си финансови отчети и те се вписват в Търговския регистър. Много ясно е разчетено какво всъщност е публично и достъпа до тези документи става след регистрация и идентификация с електронен подпис на лицата, които искат да получат достъп до тези документи. Така че, по същество нищо не променяме в тази част.

Ст. Кочков - Един коментар от бизнес съвета. Честно казано като документация за нас беше малко объркващо, иначе и по принцип концепцията за Единна входна точка, да, правилно, но от бизнес гледна точка не стана ясно какво е облекчението за бизнеса? Тоест за нас какви биха били ползите, колко пъти трябва да ги вкарваме тези документи било то и онлайн?

Д. Янчева - Само веднъж и да „качвате“ доклада когато мине акционерното събрание или когато мине одита. Това е второто влизане, с което да оформите целия пакет, който да заминете за Агенцията за вписванията.

Ст. Кочков - Не става ясно. Тук препоръката е да се осъвремени заданието, защото най-малкото от 2011 г. досега поне в нашия бизнес е остаряло.

Д. Янчева - Това е задание, за да може да бъде избран разработчик. Затова е 2011 г.

Ст. Кочков - За разработчика коментара е, че в момента както е написана документацията говорим за ограничена обществена поръчка, срещу което ние сме силно против. Тоест искаме да е отворена обществената поръчка.

Д. Янчева - Няма проблем, ние сме я заявили още в началото на годината на сайта на Агенцията за обществени поръчки, че би могло такова нещо да се появи като задание.

**След края на разискванията по точка 5 Съветът за електронно управление прие за сведение представения проект.**

#### **6. Представяне на ЗИД на Закона за достъп до обществена информация, с отразени коментари след обществено обсъждане**

**Докладва:** В. Величков – Съветник към заместник министър-председател по коалиционна политика и държавна администрация

След приключване на общественото обсъждане на закона, имаше доста забележки както от страна на НПО сектора, така и от бизнеса за това, че има прекалено много пожелателни неща. Този ЗИД е с цел транспониране на европейска директива.

По време на междуведомствената съгласувателна процедура бяха отразени допълнителни забележки, които много накратко, са в посока премахване на някои пожелателни елементи по това кога и къде администрациите да могат да публикуват, както отговори на заявления за достъп до обществена информация, така и по отношение на отварянето на данни в машинночетим формат. Въведен е проактивен принцип, при който администрациите да отварят по годишни планове наборите от данни, които те така или иначе събират и съхраняват във връзка с изпълнение на обществената си функция. Въведена е концепция за това да има единен централизиран портал, през който да могат да се отправят запитвания до съответните администрации за достъп до обществена информация, заявления и съответно там да могат да се получава отговорите, за да може на едно място да се трупат и отговорите и да не се налага да питат хората едни и същи неща по много пъти. Същевременно са прецизирани санкциите при неизпълнение и персоналната отговорност.

Ив. Калфин: Може ли само един коментар по тази точка? Много е ограничен кръгът, който се определя от документите, които могат да се ползват за повторна информация. Идеята на тази директива е да се прави публично и то на ниска цена на себестойност с цялата информация, която не е лични данни и не е класифицирана информация. Тук има един изключително рестриктивен режим какво точно да се дава, което е много далеко от идеята на директивата. Цялата информация, която събира администрацията, би трябвало да е публична по принцип, без лични данни и без класифицирана информация, включително и това, което се събира в НСИ.

С. Цветарски: Извинявам се, но само преди три месеца приключи една проверка от ЕВРОСТАТ, която основно това проверяваше - спазването на Кодекса на добрата статистическа практика, където влиза и този въпрос. Той е неотменим. В момента се ревизира Закона за статистиката, европейската статистика - регламент № 223 и той е



абсолютно категоричен. Ние самите страдаме от това. Защото искаме нашата информация да достигне до всеки. Ние сме доволни, когато тя се ползва, но тези ограничения имат други цели. Да запазят доверието в статистическата институция и информацията, която ние събираме. Иначе ще се лишим от нашите контрагенти.

Готови сме и търсим варианти максимално да отваряме нашата информация без да издаваме, разбира се, конфиденциална информация.

Р. Бъчварова - Господин Калфин, да ни представите коментарите и предложенията и ще ги разгледаме преди да ги внесем.

Ив. Калфин - Ще ви ги дам, аз не знам на този етап дали е възможно, казвам ви го, защото като се приемаше директивата бях докладчик по нея и съм преговарял и със страните членки, и с Парламента и парламентарните групи.

Идеята е да се смени концепцията. Вие казвате „извадихме още данни“, точно обратна е концепцията. Всичко трябва да е извадено, но въпроса е кое не се вади, кое е забранено действително да се извади, а не че още някоя информация е решила администрацията да предостави публично. Това е точно обратното.

Вл. Горанов - Ако спазваме принципа на активното предоставяне?

Р. Бъчварова - Принципът е на активното предоставяне на информация. Мисля, че докато преминем към пълното предоставяне ще мине време

Вл. Горанов – На етапи. Доработваме идеята, иначе цялата информация, която я създаваме ще я представим.

**След края на разискванията по точка 6 Съветът за електронно управление прие за сведение представената информация.**


Поради изчерпване на предвиденото време председателя на СЕУ Р. Бъчварова предложи да се отложи за следващо заседание разглеждането на т. 3 от дневния ред. Съветът прие това предложение.

Поради изчерпване на дневния ред заседанието на СЕУ беше закрито.


**Приложения към протокола от заседание на СЕУ:**

1. Становища от Асоциацията банките в България и Министерство на правосъдието;
2. Презентация на тема „Проектозакон за електронната идентичност“;
3. Презентация на тема „Преместване на Интернет възела, договора за доставка на Интернет за Държавната администрация и закупените IPv4 адреси от Администрацията на Министерски съвет“;
4. Презентация на тема „Проект за Единна входна точка“

**Председател на Съвета за електронно управление:**

  
/РУМЯНА БЪЧВАРОВА/  
Заместник министър-председател  
по коалиционна политика и държавна  
администрация

**Секретар на Съвета за електронно управление:**

  
/ВАЛЕРИ БОРИСОВ/  
Заместник-министър на транспорта,  
информационните технологии и съобщенията