Национална федерация
Техническа индустрия, Наука, Информатика
София 1000, ул. Ангел Кънчев №2 | nftini@abv.bg | www.NFTINI.org

до: **Божидар Божанов**, министър
МИНИСТЕРСТВО НА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ
гр. София

ПОЗИЦИЯ

от: **Адриан Н. Илиев**, председател
БРАНШОВ СИНДИКАТ „ИНФОРМАЦИОННИ ТЕХНОЛОГИИ"
на **НФТИНИ** при **КТ „Подкрепа"**
гр. София, ул. Ангел Кънчев №2

относно: Техническа спецификация за изграждане на мобилно приложение за електронна идентификация и електронно подписване – **BGID**

Уважаеми Г-дин МИНИСТЪР,

Като **национално представителна секторна организация на работещите** в областта на информационните технологии, от наше име и от името на нашите синдикални членове приветстваме новосформираното **Министерство на електронното управление** (МЕУ) за инициативата най-после да бъде започнат сериозен разговор относно българското Електронно управление – който разговор не може да не засегне още в самото си начало въпроса за **електронната идентификация** (и в частност – за **електронното подписване**). Без предварително разрешаване на този въпрос всеки делови процес в електронна среда е обречен или на липсата на гаранции за автентичност (и от там – липса на юридическа значимост); или на частични решения „на парче", които в крайна сметка правят Електронното управление разпокъсано, скъпо и неефективно.

В т. **3.1.** „Общи и специфични цели" от проекта на Спецификацията е посочено, че *„проектът е насочен към изграждане на удобно и достъпно средство за електронна идентификация на потребителите на електронни административни услуги, както и за електронно подписване на заявления за електронни административни услуги чрез мобилни устройства"*. По-детайлно се предлага и структура на проекта, където от Дейност **3.** „Разработване на мобилно приложение за потребители за **Android** и **iOS**"; и от Дейност **4.** „Разработване на служебно мобилно приложение за **Android** и **iOS**" научаваме, че се предвижда разработването на **мобилни приложения** (респективно **служебни мобилни приложения**) *„за най-популярните операционни системи, като минимум: **Android 9** и **Apple iOS 12**"*.

възражение: Защо само „мобилни устройства"?

Безспорно, включването на мобилни устройства (преди всичко „умни" телефони и отчасти – различни видове таблети, фаблети и т.н., осигуряващи **GSM**-свързаност), е стъпка в правилната посока – значителен брой лица използват такива устройства и практическите последици от включването им като възможност за електронна идентификация и електронно подписване са обнадеждаващи.

Същевременно обаче много граждани не ползват подобни устройства, но ползват напр. **стационарни или преносими компютри, които не са мобилни устройства** (не поддържат **GSM**-свързаност). Предимство при тях е, че настройването на операционната среда и приспособяването на системата към личните (а понякога и специфично професионални) нужди е много по-гъвкаво в сравнение с типичните

мобилни устройства; поради което често сред потенциално най-масовите потребители на електронни идентификационни и подписни услуги (счетоводители, одитори, адвокати, нотариуси, търговци и др.) стационарните и преносимите компютри са предпочитани. За разлика от тях, мобилните устройства в повечето случаи не се поддават на специфични настройки и не позволяват тяхното защитаване извън **фабрично заложените мерки за сигурност** – което поставя под въпрос надеждността им. Поставянето на мобилния телефон като единствена възможност за достъп до електронни административни услуги ограничава възможностите за работа в операционна среда, позволяваща приспособяване към личните (и професионалните) нужди на ползвателите. Не на последно място – съществуват отдалечени и слабо развити райони, където **GSM**-покритието е несигурно и това би направило услугите недостъпни.

► **Считаме**, че системите за електронна идентификация и електронно подписване на българското Електронно управление трябва още от самото начало да могат да работят на всякакви други устройства (освен мобилните), които осигуряват **internet**-свързаност или **GSM**-свързаност. В случай, че се настоява за включването на мобилния телефон като условие за обезпечаване на двуфакторност, достатъчна надеждност може да предостави напр. изпращането на обикновен **SMS** с код за потвърждаване (технология, достъпна и от телефони, които не са „умни").

възражение: Защо само несвободни операционни системи?

Безспорно е, че операционните системи **Android** и **iOS** са сред най-масовите алтернативи за софтуерно осигуряване на мобилни устройства – и разработването на приложения за тях ще обезпечи най-голяма добавена стойност за инициативата на **МЕУ**.

Далеч обаче тези операционни системи не са единствените. Много по-сериозни въпроси обаче повдига обстоятелството, че избраните операционни системи са **несвободен софтуер** (по см. на **Свободните софтуерни лицензи**[1]), където понятието „свобода" се възприема в своя морален и либерален смисъл, не в смисъла на дължима цена). Особеност на несвободния софтуерен код е това, че потребителят **нито може да знае, нито има право да знае** как точно функционира софтуерът и какво точно извършва на собственото му устройство. Като единствена алтернатива за потребителя остава да се довери „на сляпо" на разработващата софтуерна компания (която изначално му отказва каквото и да било доверие, лишавайки го от достъп до **изходния код**[2]). В допълнение – и двете най-масови операционни системи (**Android** и **iOS**) се разработват от софтуерни компании извън **ЕС**. Макар да не е на дневен ред, последното поставя под въпрос сигурността на българското Електронно управление, което при такова технологично разрешение би се оказало зависимо от трети страни извън юрисдикцията на Съюза. И не на последно място – такова технологично разрешение би „задължило" българските граждани, организации и административни органи „да бъдат клиенти" на чуждестранни частни компании, като условие за получаването на достъп до български електронни административни услуги; които чуждестранни частни компании имат право по всяко време и без предупреждение да променят както технологиите си, така и правилата за тяхното използване.

► **Считаме**, че системите за електронна идентификация и електронно подписване на българското Електронно управление трябва още от самото начало да бъдат базирани на свободни софтуерни технологии, които **не са зависими от трета разработваща страна**. Създаването на приложения за несвободни операционни системи (тук следва да включим напр. и **Windows Mobile**, кой знае защо изпусната от предложената версия на проекта) са допустими, но не препоръчителни – с оглед обезпечаване **дължимата на потребителите свобода** и защита на **националната сигурност**.

---

1 Вж. напр. американския **Общ публичен лиценз GNU (GNU General Public License)**, достъпен на този адрес: `https://www.gnu.org/licenses/gpl-3.0.en.html`
или напр. европейския **Публичен лиценз на ЕС (EU Public license)**, достъпен на този адрес: `https://joinup.ec.europa.eu/collection/eupl/eupl-text-eupl-12`

2 **Изходният код** позволява прочитане, анализ и промяна от човек; за разлика от **машинния (изпълнимия) код**, който се изпълнява от машината, но не се поддава на прочитане, анализ и промяна от човек (поне не без изключително трудоемки и ненадеждни работи, свързани с т.нар. **„обратно инженерство" (Reverse Engineering)**).

възражение: Софтуерът с отворен код не е достатъчен?

В т. **1.2.** „Технологични дефиниции" от проекта на Спецификацията е посочено, че под **софтуер с отворен код** ще се разбира *„компютърна програма, която се разпространява при условия, които осигуряват безплатен достъп до програмния код и позволяват: използването на програмата и производните на нея компютърни програми, без ограничения в целта; промени в програмния код и адаптирането на компютърната програма за нуждите на нейните ползватели; разпространението на производните компютърни програми при същите условия"*, като е приведен списък със **стандартни лицензионни споразумения**, предоставящи горните възможности (препратка към подзаконовата нормативна уредба към **ЗЕУ** и към списъка със софтуерни лицензи на **Инициативата за Отворен код**[3]).

Независимо, че между понятието за **Отворен код** и това за **Свободен код** няма кардинални технически разлики, следва да се отбележи един съществен риск за софтуера, разработван и разпространяван съгласно т.нар. **„отслабено свободни" софтуерни лицензи**. На пръв поглед такива лицензи дават „най-големи свободи" и много разработващи страни ги предпочита заради това – но в действителност те позволяват **„превземане" на софтуера**[4] от напълно несвободни проекти, които са се възползвали от така предоставените свободи. Следва да се вземат предвид т.нар. **„усилено свободни" софтуерни лицензи** (**CopyLeft**[5]), при които такова „превземане" на софтуера е забранено. Лишени от дължимата юридическа експертиза, много софтуерни и компютърни специалисти достигат до неправилен извод, че поради **забраната за отнемане на свободата** такъв вид лицензи са „по-несвободни" от други лицензи, при които такава забрана не съществува. В действителност именно тази забрана (и приведените в нейна защита юридически, технически и организационни гаранции) **защитава свободата на софтуерния код**.

Безспорно, въвеждането в българската нормативна уредба на понятието за **отворен софтуерен код**[6] е **стъпка в правилната посока, но не достатъчна**. Единствено „усилено свободните" софтуерни лицензи са в състояние да гарантират обществения интерес при разработването, поддържането, експлоатирането и надграждането на електронни системи за българската администрация (в т.ч. системи за електронна идентификация и електронно подписване). Този вид лицензи гарантират, че целият софтуер, без изключение, ще остане напълно отворен и достъпен както за независим технически одит, така и за отстраняване на слабости, ако такива бъдат установени; и за надграждане, ако такива нужди бъдат идентифицирани във времето; и гарантират, че това положение няма да бъде променено, изцяло или отчасти, поради технологично свързване на софтуера (технологично поставяне в зависимост на софтуера) от несвободни компоненти, без които на един по-късен етап този софтуер би се оказал неспособен да осъществява функциите си.

► **Считаме**, че системите за електронна идентификация и електронно подписване на българското Електронно управление трябва още от самото начало да бъдат базирани на гарантирано свободни

---

3 **Инициативата за Отворен код** (**Open Source Initiative; OSI**) възниква на **03.02.1998** г., като резултат от отделянето на част от привържениците на **Движението за Свободен софтуер** (**Free Software Movement**), което от **1985** г. се застъпва твърдо за свободата на потребителите и за отстояване на етичното споделяне и взаимопомощ (**Stallman 2009**). Привържениците на **OSI** намират този мотив за „недостатъчно прагматичен" (**Tiemann 2006**) и се съсредоточават в отварянето на кода с чисто техническа цел – за да бъде по този начин привлечен към усъвършенстването му по-широк кръг от специалисти и това да ускори развитието му – а от там и неговата добавена стойност и капитализация.

4 Подобно „превземане" на софтуера, свободен (отворен) по своята същност, се случва именно при операционната система **Android**, която е започната съгласно „отслабено свободния" софтуерен лиценз **Apache 2.0**, позволяващ вграждането на несвободни елементи в Linux-ядрото и **поставяне в зависимост** на операционната система от все повече и повече напълно несвободни софтуерни приложения, библиотеки, firmware и т.н. – без които към днешна дата тази операционна система изобщо не би могла да изпълнява функциите си.

5 Шеговита игра на думи от англоезичния израз **„право на копиране"** (**CopyRight**), където думата **„право"** може да се разбира и като **„надясно"**; съответно думата **„наляво"** (**Left**) следва да подскаже диаметралния подход при „усилено свободните" софтуерни лицензи, където правото на интелектуална собственост се използва не за ограничаване, а за защитаване неограничимостта на дадената свобода софтуерът да бъде (**0**) използван за всякакви цели, (**1**) споделян в първоначалния му вид, (**2**) проучван и променян според своите нужди, и (**3**) разпространяван в променения му вид.

6 Лични заслуги за това има министър **Божидар Божанов** като съветник по въпросите на Електронното управление на тогавашния вицепремиер **Румяна Бъчварова** във Второто правителство на **Бойко Борисов**.

софтуерни технологии, лицензирани съгласно **широко разпространени „усилено свободни" софтуерни лицензи**[7] – като надграждане на достигнатото нормативно понятие за „софтуер с отворен код" и като гаранция, че кодът ще продължи да бъде **прозрачен, достъпен, адаптируем** и **независим** от конкретна разработваща страна, **завинаги** в полза на цялото общество.

заключение: **Защо софтуерът с отворен код не е достатъчен?**

Инициативата разговорът за очакваното от всички ни българско Електронно управление да започне именно от въпроса за **електронната идентификация** (и в частност – за **електронното подписване**) е похвална и разкрива наистина професионално отношение към тази материя. Без разрешаването на този въпрос не може да се осигури нито участие на правните субекти в административния процес, нито стабилност на самия административен процес – което логично резултира в десетилетия изоставане на българската държавна администрация при управлението на поредица от предходни правителства.

Съществено безпокойство обаче поражда нагласата електронната идентификация и електронното подписване да бъдат ограничени до „мобилни устройства", работещи с несвободните операционни системи **Android** и **iOS**, които дори се разработват и са собственост на частни компании извън **ЕС**. Не можем да оправдаем a priori изключването на други широко разпространени в практиката устройства (напр. преносими и desktop компютри) и операционни системи (напр. **Windows**[8], **GNU/Linux**[9] и др.).

► **Считаме**, че поставянето още в самото начало на **широка основа за достъпност** до механизмите за електронна идентификация и подписване в българското Електронно управление е **критично условие** за ползваемостта на тези системи и от там – за успешността на Електронното управление. Това не може да стане, ако механизмите се ограничат само до мобилни устройства и само до две от възможните операционни системи. И не на последно място – евентуално базиране на механизмите за електронна идентификация и електронно подписване на **несвободен софтуер**, разработван от частни компании извън **ЕС** (каквито са фаворизираните две операционни системи) е уязвимост, която би снижила значително **сигурността** на тези механизми, **прозрачността** им и тяхната **независимост** от конкретни разработващи страни – диаметрално в противоречие със заявените цели и нагласи.

Благодарим за отделеното внимание!

24.02.2022 г.
гр. София

С уважение: **Адриан Н. Илиев**, председател
БРАНШОВ СИНДИКАТ „ИНФОРМАЦИОННИ ТЕХНОЛОГИИ"
на **НФТИНИ** при **КТ „Подкрепа"**

---

7 Сред най-широко разпространените „усилено свободни" лицензи могат да бъдат посочени: за софтуер – **GNU General Public License** (всички версии); **GNU Affero General Public License** (единствена версия); **Eclipse Public License** (версия **1.0**); **Mozilla Public License** (версия **2.0**); **European Union Public license** (версии **1.1** и **1.2**); **German Free Software License** (единствена версия); за бази с данни – **Open Database License** (единствена версия); за документация – **GNU Free Documentation License** (всички версии); за всякакво нетехническо съдържание – **Creative Commons** (**CC-BY-SA**); и др.

8 Независимо от множеството критики срещу технологичните достойнства на продуктите на **Microsoft**, със своя пазарен дял **75,5%** различните desktop версии на операционната система **Windows** (и със своя пазарен дял **32,11%** мобилната версия **Windows Mobile**) остават най-разпространените в световен мащаб, като България не прави изключение. Това прави нелогично изключването на тези системи от първоначалните планове на **МЕУ**. Вж. още на този адрес: `https://gs.statcounter.com/os-market-share/desktop/worldwide/`

9 Независимо от минималния пазарен дял на различните **GNU/Linux** дистрибуции (до **2,19%** при desktop версиите), следва да се отбележи, че те са предпочитани при сървърни системи (**77,4%** от системите), супер компютри (**81,4%** от **500**-те най-мощни системи) и др., където изискванията за **информационна сигурност** и **приспособимост към специфични задачи** са по-високи от обикновено. Това прави нелогично изключването им от първоначалните планове на **МЕУ**.