Р Е П У Б Л И К А Б Ъ Л Г А Р И Я
МИНИСТЕРСТВО НА ТРАНСПОРТА,
ИНФОРМАЦИОННИТЕ ТЕХНОЛОГИИ И СЪОБЩЕНИЯТА

ПРОТОКОЛ № 3

от работата на комисия, назначена със Заповед № РД-14-94/04.12.2018 г. на министъра на транспорта, информационните технологии и съобщенията за разглеждане и оценяване на постъпилите оферти за участие в обществена поръчка с предмет: „Надграждане на поддържаните от Изпълнителна агенция „Автомобилна администрация" регистри и бази данни. Изграждане на нов модел на контролната дейност, основан на оценка на риска", в състав:

Председател:

1. **Дамян Войновски** – заместник изпълнителен директор на Изпълнителна агенция „Автомобилна администрация"

и членове:

2. **Васил Палавров** – началник на отдел „Административнонаказателна дейност", Главна дирекция „Автомобилна инспекция", ИААА;
3. **Нели Мицева** – главен специалист в отдел „Правен", дирекция „Административно-правно обслужване", ИААА;
4. **Христинка Иванова** – главен експерт в отдел „Технически прегледи и одобряване на ППС", дирекция „ППС и водачи", ИААА;
5. **Станко Иванов** – началник на отдел „Правоспособност и професионална компетентност", дирекция „ППС и водачи", ИААА;
6. **Бисер Петров** – държавен експерт в отдел „Международни правни норми", в дирекция „Правна", МТИТС;
7. **Йоанна Иванова** – главен експерт в отдел „Обществени поръчки", в дирекция „Стопански дейности и управление на собствеността", МТИТС;
8. **Даниела Пешева** – държавен експерт в отдел „Политика в информационното общество", в дирекция „Информационни технологии", МТИТС;
9. **Васил Невенов** – главен експерт в отдел „Бюджет", дирекция „Финанси", МТИТС.

В периода 14 – 17 януари 2019 г. комисията продължи работата си, като разгледа допълнително представеното разяснение и доказателства от участника, изискани с писмо рег. № РД-14-82 от 08.01.2019 г.

С писмо рег. № РД-14-82/11.01.2019 г. участника „Демакс Ди Пи Ай" АД е представил следните документи:

1. Писмо (разяснение), подписано от инж. Марин Несторов, изпълнителен директор на „Демакс Ди Пи Ай" АД;
2. Референция, издадена от Изпълнителна агенция „Автомобилна администрация" относно Договор № РД-32-5/10.06.2016 г. и Договор № РД-30-47/13.06.2011 г.;

3. Референция, издадена от „Печатница на Българска народна банка“ АД относно Договор № 01-000794/19.02.2016 г., Договор № 01-03615/14.10.2016 г. и Договор № 01-000760/06.03.2017 г.;

4. Референция, издадена от ДЗЗД „Консорциум трафик за София„ с предишно наименование - ДЗЗД „Консорциум Ю ТИ АЙ Груп - иновативни трафик системи“ относно Договор от 21.10.2016 г.;

5. Копие от Договор от 21.10.2016 г. с приложения № 1 и № 2;

6. Приемо-предавателен протокол от 30.11.2016 г. за предаване на 85 бр. устройства и захранващи интерфейсни кабели към тях, инсталира, провежда първоначално изпитване, въвежда в експлоатация и прехвърля правото на собственост върху система за приоритетно преминаване на автомобили със специален режим на движение през кръстовища.

От представените документи комисията установи следното:

1. В последния абзац от разяснението на участника се твърди, „че „Демакс Ди Пи Ай“ АД покрива изискването на Възложителя участникът да е изпълнил услуга за система, поддържаща работа с квалифицирани електронни подписи за минимум 5 000 (пет хиляди) регистрирани потребители“. Като доказателство за твърдението са посочени референциите, издадени от Изпълнителна агенция „Автомобилна администрация“ относно Договор № РД-32-5/10.06.2016 г. и Договор № РД-30-47/13.06.2011 г. и референцията, издадена от „Печатница на Българска народна банка“ АД относно Договор № 01-000794/19.02.2016 г., Договор № 01-03615/14.10.2016 г. и Договор № 01-000760/06.03.2017 г.

В документацията за обществената поръчка, в Раздел III „Критерии за подбор. Изисквания и указания“ т. 3.1 е регламентирано, че през последните три години, считано от датата на подаване на офертата участникът трябва да е изпълнил успешно дейности с предмет и обем, както следва:

- най-малко една услуга, включваща разработка и внедряване на уеб базирана информационна система, с използване на система за управление на бази данни и поддържаща работа с квалифицирани електронни подписи за минимум 5 000 (пет хиляди) регистрирани потребители и
- най-малко една услуга за изграждане на виртуализирана сървърна инфраструктура.

От информацията за посочените по-горе договори, сключени с Изпълнителна агенция „Автомобилна администрация“ и ДЗЗД „Консорциум Ю ТИ АЙ Груп - иновативни трафик системи“ е видно, че участникът не покрива изискването на Възложителя да е изпълнил услуга за система, **поддържаща работа с квалифицирани електронни подписи за минимум 5 000 (пет хиляди) регистрирани потребители**, тъй като изискването на Възложителя е за „една система“, поддържаща работа с квалифицирани електронни подписи за минимум 5 000 (пет хиляди) регистрирани потребители, докато участникът е изпълнил няколко „системи“, поддържащи работа с квалифицирани електронни подписи, които сумарно надвишават бройката от 5 000 потребители, но нито една от тях самостоятелно не осигурява работа с 5000 потребители.

2. С писмо рег. № 32-01-819/21.12.2018 г. „Демакс Ди Пи Ай“ АД е представил нов еЕЕДОП, в който, в Част IV „Критерии за подбор“, Раздел В „Технически и професионални способности“, „За поръчки за услуги: извършени услуги от конкретен вид“ е декларирал изпълнението на договор за „Изработка, инсталация, първоначално изпитване и въвеждане в експлоатация на система за приоритетно преминаване на автомобили със специален режим на движение през кръстовища, което представлява услуга включваща изграждане на виртуализирана сървърна инфраструктура 6000 (шест хиляди) регистрирани потребители за конкретния договор. Договор от 21.10.2016 г.“.

От представените допълнително документи – разяснение, подписано от инж. Марин Несторов, изпълнителен директор на „Демакс Ди Пи Ай“ АД, копие на Договор от 21.10.2016 г. и приложение № 2 към него може да се направят следните изводи:

Съгласно чл. 1, ал. 1.1 на Договор от 21.10.2016 г. изпълнителят „Демакс Ди Пи Ай“ АД следва да „достави, инсталира, проведе първоначално изпитване, въведе в експлоатация и прехвърли на Възложителя правото на собственост върху система за приоритетно преминаване на автомобили със специален режим на движение през кръстовища, включваща:....

в/ Софтуер за работа и конфигуриране на устройствата по букви „а“ и „б“ по-горе за срок от 1 (една) година (Приложение № 2)“.

При така дефинирания предмет на посочения договор не може да се направи еднозначен извод, че кандидатът отговаря на изискването в документация (Раздел III, т.3.1) да е изпълнил „най-малко една услуга, включваща разработка и внедряване на уеб базирана информационна система, с използване на система за управление на бази данни и поддържаща работа с квалифицирани електронни подписи за минимум 5 000 (пет хиляди) регистрирани потребители“, тъй като предвидената в Договора от 21.10.2016 г. доставка на софтуер не би могла да се приеме за равнозначна на **разработване на информационна система**.

В допълнение, в представеното от участника приложение № 2 е посочено, че „При въвеждане на информация от страна на потребителя, системата ще предоставя методи за валидиране и контрол на нейната вярност и цялостност. При наличие на грешно въведена или непълна информация системата трябва ще извежда подходящи подканващи и/или предупредителни съобщения.“ Ако се приеме, че пораждащата неяснота комбинация от думите „трябва ще“ е техническа грешка, то в приложението липсва описание на методите за валидиране и контрол, което прави преценката за съответствие с изискванията на Техническото задание невъзможна.

В т. 2 от приложение № 2 е посочено, че едно от основните предимства на техническото решение е „високо ниво на сигурност посредством архитектура за аутентификация на крайните потребители чрез PKI (Public Key Infrastructure; квалифициран електронен подпис)“. Това е единственото място в представените документи, в които се споменава квалифициран електронен подпис (КЕП), изискуем съгласно документация Раздел III, т.3.1 от документацията. Използването на PKI е пояснено малко по-подробно в т. 3 от приложение № 2 към Договор от 21.10.2016 г. От поясненията става ясно, че в превозните средства ще се монтират комуникационни устройства и радио антени, като е предвидено свързване на външните интерфейси на превозните средства със специален режим, но не е уточнено с какво ще се осъществява това свързване (т. 4 Хардуер). В т. 3 е пояснено „че сигналът от комуникационните устройства ще се подава към контролери на светофарите, които на база на този сигнал ще променят режима си на работа. Командата е радио телеграма, а „комуникационните канали са криптирани посредством PKI“. Уточнено е, че командите може да съдържат множество данни, но **никъде не е посочено, че е предвидена проверка на подаваната информация, как ще става тя и къде ще се използва КЕП.**

Следва да се отбележи, че PKI, което на български се превежда по няколко начина - „инфраструктура на публичния ключ“, „инфраструктура с публичен ключ“, „публична ключова идентификация“ – е технология за проверка на автентичността на електронен документ с помощта на публичен ключ. **Това е съвкупността от хардуер, софтуер, хора, политики и процедури, необходими за издаването, управлението, разпределението, използването, съхранението и отнемането на цифрови сертификати.** PKI се реализира по модела клиент-сървър, т.е. проверката за дадена информация, предоставена в инфраструктурата, може да се извърши само по инициатива на клиента.

В криптографията PKI е споразумението, което свързва определен публичен ключ с идентичността на неговия собственик. Това свързване се осъществява чрез:

• Сертифициращ орган (Certificate Authority или CA), който гарантира еднозначността на свързването чрез строго установен процес на регистрация и издаване на цифровия сертификат, което може да става както от софтуер, така и от човек. CA носи отговорност за легитимността на издадените сертификати, т.е. той удостоверява, че публичния ключ, който се съдържа в сертификата, наистина принадлежи на човека или организацията, записана в сертификата.

• Регистриращ орган (Registration Authority или RA) – незадължителен елемент на системата, предназначен за регистрация на ползвателите. CA поверява на RA проверката на информацията за субекта. Регистриращият орган разглежда подадените молби за издаване на сертификати. След проверката на правилността на информацията, RA я подписва със своя ключ и изпраща на CA заявка за издаване или отхвърляне на сертификат. Сертифициращият орган след проверка на ключа на RA издава сертификат.

• Хранилище - съдържа сертификати и списъци със сертификати (COC) и служи за разпространението им сред ползвателите.

• Архив на сертификатите — хранилище на всички издадени сертификати (вкл. сертификати с изтекъл срок на действие). Архивът се използва за проверка на автентичността на електронните подписи, с които са подписвани документите.

• Център на заявките — незадължителен компонент на системата, в който крайните ползватели могат да заявят или оттеглят сертификат.

• Крайни ползватели — ползватели, приложения или системи, които са собственици на сертификата и използващи инфраструктура за управление с публични ключове.

• Проверяващ орган (Vertification Authority или VA) - издадения от сертифициращия орган сертификат с публичен ключ са кодирани редица атрибути като идентичност на титуляря, самият публичен ключ, тяхната връзка, условията за валидност и др. по начин, който гарантира че не могат да бъдат фалшифицирани.

PKI може да се разглежда като комбинация от операционна система и приложни услуги, които правят възможен и лесен процеса на прилагане на криптографията. Това се изразява в:

• Управление на ключовете – PKI улеснява издаването на нови публични ключове, изважда от употреба ключове, компрометирали своята надеждност, и управлява нивото на доверие към ключовете на различните потребители.

• Публикуване на ключовете – PKI предлага добре дефиниран способ за всеки желаещ да намери и използва даден публичен ключ, както и информация за валидността на даден ключ.

• Използване на ключовете – PKI включва и набор от приложения, използващи ключове за криптиране и подписване на данните за обмен.

Съгласно чл. 3 на Регламент (ЕС) № 910/2014 и чл. 13, ал. 3 от Закона за електронния документ и електронните удостоверителни услуги, „Квалифициран електронен подпис“ означава усъвършенстван електронен подпис, който е създаден от устройство за създаване на квалифициран електронен подпис и се основава на квалифицирано удостоверение за електронни подписи.“

Квалифицираният електронен подпис има значението на саморъчен подпис.

Електронният подпис е реквизит на електронен документ, предназначен за защитата му от фалшификация. Това е криптографски подпис или по-точно, математическа функция, получена в резултат на криптографска обработка на информацията, извършена с цел да се удостовери самоличността на изпращача и да се гарантира, че информацията не е била променяна по пътя между изпращането и получаването. Електронният подпис използва за криптирането алгоритъм, с една степен по-сигурен от алгоритмите, използващи хеш-функция за удостоверяване на самоличността на изпращача. Използва се асиметрична криптография с двойка ключове – частен и публичен, като с единия се криптира, а с другия се декриптира. Частният ключ е таен. Той се генерира и съхранява върху смарт-карта, притежавана от

собственика на подписа. Достъп до картата и ключа в нея има само той, чрез ПИК. Подписването се осъществява именно с частния ключ

Публичният ключ е нужен, за да се разчете подписът, положен с частния ключ. Публичният ключ е достъпен за всеки издаден подпис, стига това да е разрешено от неговия притежател и може да бъде разгледан и свален от всеки. Това дава възможност за разчитане на документите, подписани от съответния притежател на частния ключ. Ако се използва публичен ключ, различен от ключа от двойката, подписът не може да бъде разчетен.

От казаното по-горе следва, че Public key infrastructure се различава от квалифициран електронен подпис. Първото е технология за проверка на автентичността на електронен документ с помощта на публичен ключ, а второто е реквизит на електронен документ, предназначен за защитата му от фалшификация.

На тази база и отчитайки предоставеното разяснение и допълнителна информация, съдържаща се в Договора от 21.10.2016 г. и приложение № 2 към него, комисията не приема, че кандидатът отговаря на изискването в документацията за обществената поръчка, Раздел III „Критерии за подбор. Изисквания и указания" т. 3.1, където е регламентирано, че участникът трябва да е изпълнил успешно дейности с предмет и обем, както следва: най-малко една услуга, включваща разработка и внедряване на уеб базирана информационна система, с използване на система за управление на бази данни и поддържаща **работа с квалифицирани електронни подписи за минимум 5 000 (пет хиляди) регистрирани потребители**.

Въз основа на гореизложеното и на основание чл. 56, ал. 1от Правилника за прилагане на Закона за обществените поръчки комисията не допуска до разглеждане техническото предложение на участника „Демакс Ди Пи Ай" АД, тъй като установи, че същият не отговаря на критериите за подбор - Раздел III „Критерии за подбор. Изисквания и указания" т. 3.1, първо тире.

Комисията състави и подписа този протокол на 17.01.2019 г.

Председател:

На осн.Чл.2.ал.1 от ЗЗЛД Дамян Войновски

членове:

На осн.Чл.2.ал.1 от ЗЗЛД Васил Палавров

На осн.Чл.2.ал.1 от ЗЗЛД Нели Мицева

На осн.Чл.2.ал.1 от ЗЗЛД Христинка Иванова

На осн.Чл.2.ал.1 от ЗЗЛД Станко Иванов

На осн.Чл.2.ал.1 от ЗЗЛД Бисер Петров

На осн.Чл.2.ал.1 от ЗЗЛД Йоанна Иванова

На осн.Чл.2.ал.1 от ЗЗЛД Даниела Пешева

На осн.Чл.2.ал.1 от ЗЗЛД Васил Невенов