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

линк към консултацията

Информация

Откриване / Приключване: 18.02.2022 г. - 04.03.2022 г. Неактивна

Номер на консултация: #6579-K

Област на политика: Архив - Държавна администрация

Тип консултация: ---

Тип вносител: Национално

Трансформацията на държавната администрация в дигитална изисква наличие на възможности за сигурно и надеждно установяване и проверка на самоличността на потребителите на електронни административни услуги. С оглед изграждането на технологична възможност за електронна идентификация чрез мобилно устройство, Министерството на електронното управление разработи техническа спецификация за изграждане на мобилно приложение за електронна идентификация и електронно подписване – BGID. Предвид огромната важност на процеса по електронна идентификация за цялостното развитие на електронното управление в Република България, техническата спецификация се публикува за обществена консултация с цел отчитане на приноса и мнението на всички заинтересовани страни преди обявяването на обществената поръчка.

Създадената технологична възможност за електронна идентификация чрез мобилно устройство ще разреши дългогодишния проблем с липсата на широко разпространено, достъпно, сигурно, надеждно, лесно за използване и безплатно средство за електронна идентификация, удобно разположено в мобилно устройство.

Начини на предоставяне на предложения и становища

- Портала за обществени консултации (изисква се регистрация чрез имейл);
- Електронна поща на посочените адреси;
- Системата за сигурно електронно връчване https://edelivery.egov.bg/ (изисква се квалифициран електронен подпис или ПИК на НОИ);
- Официалния адрес за кореспонденция.

Документи

Пакет основни документи:

Техническа спецификация за изграждане на мобилно приложение за електронна идентификация и електронно подписване – BGID - вер. 1.0 | 18.02.2022

Техническа спецификация за изграждане на мобилно приложение за електронна идентификация и електронно подписване – BGID - вер. 1.0 | 18.02.2022

Позиция на браншовия синдикат Информационни технологии - вер. 1.0 | 28.02.2022

Становище на „Българска телекомуникационна компания” ЕАД - вер. 1.0 | 04.03.2022

Консултационен документ:

Справка становища:

Коментари

Коментари (pdf)

Коментари (csv)

Автор: Mihail-Ernesto Mihailov (04.03.2022 22:35)

Добавяне на функционалност за автоматична валидация чрез устройства без оператор

Предлагам поддръжка на функционалност за валидация чрез автоматични (и понякога подвижни, т.е. без фиксиран адрес) валидатори.

Автоматични валидатори са устройства (технически средства), които могат да извършват автоматична валидация на идентичност, по QR код, презентиран от мобилното приложение на лицето, което иска да се идентифицира, без наличие на оператор (човек) обслужващ процеса на валидация.

Бизнес приложение на подобна услуга на BGID – идентификация на физически лица на киоски (например за плащане на сметки), пътуване в обществен транспорт чрез устройства за автоматична валидация на превозни документи и други.

Възможен начин на работа и модел за реализация:

-необходимо ниво на идентификация „ниско“ до "значително"

-мобилното приложение BGID генерира при поискване от потребител криптиран QR Код за автоматична валидация, който съдържа токен, издаден от сървърната част на системата за идентификация. По този токен, и други атрибути, които може да са носени в QR, или в сървъра на BGID, валидаторът може да извършва офлайн или онлайн проверка на лични данни чрез обръщение към API на BGID.

-примерно приложение - токенът може да идентифицира пътник в обществен транспорт, които (анонимно или не за превозвача), може да притежава “сметка” в системите на превозвача, асоциирана с токена, с която са свързани превозни документи - било то предварително закупени, или налични с отложено плащане. По този начин BGID приложението може да се ползва за пътуване в обществения транспорт, а и в редица други ситуации. Подобен механизъм е добър за по-добро опазване на лични данни, например за несподеляне с транспортния оператор на информация за правоимане (например преференция при пътуване за студент, ученик, пенсионер и др.) и лични данни на лице, имащо право на преференциално пътуване, а само, чрез достъп до съответен регистър, удостоверяване на наличието на право на преференция, оставайки потребителят анонимен за транспортния оператор.

-правата на валидаторите за наличния набор от лични данни могат да се определят на база на договорени отношения с доставчика на услугите, ползващи автоматична валидация.

Автор: Цветелина Севлиевска (04.03.2022 17:57)

Бележки и коментари по проекта

1. Публикуваният проект на „Техническа спецификация за изграждане на мобилно приложение за електронна идентификация и електронно подписване – BGID“ не е в съответствие с цитиратата нормативна уредба (Законът за електронната идентификация и правилника за прилагането му), която регламентира технологията и обществените отношения свързани с предоставяне и ползване на електронната идентификация. В тази връзка за да изпълни администрацията принципите на публичност и предвидимост, промяната на правната уредба е необходимо да предхожда действията по реализация на информационни системи и приложения.
2. Техническата спецификация изключва възможността потребителите, които вече притежават квалифициран електронен подпис да го използват за подписване на електронни документи през описаното приложение. Това ще създаде неудобство и объркване на потребителите, на които ще се наложи при заявяване и ползване на електронни административни услуги през приложението да използват усъвършенстван електронен подпис, а при ползване на електронни услуги, предоставяни от лицата, осъществяващи публични функции, и организации, предоставящи обществени услуги да използват притежавания квалифициран електронен подпис. В тази връзка предлагам спецификацията да се допълни с изисквания за разработване на протоколи за комуникация и интеграция със системи на трети страни, които предоставят услуги за отдалечено подписване.

3. В техническата спецификация не е предвидена възможност за лицата по чл. 1, ал. 2 от Закона за електронно управление (ЗЕУ) да използват извършената електронна идентификация през приложението за идентификация и потвърждаване на самоличността на физическите лица, които заявяват ползване на предоставяните от тези лица и организации електронни услуги. Това препятства изпълнението на чл. 5, ал. 2 от същия закон. В тази връзка предлагам спецификацията да се допълни с изисквания за разработване на протоколи за комуникация и интеграция със системите на лицата по чл. 1, ал. 2 от ЗЕУ.
4. Съгласно Регламент (ЕС) 910/2014 нивата на осигуреност на националните схеми за електронна идентификация следва да отговарят на изискванията на чл. 8. Съответствието с тези изисквания се удостоверява с одит от орган за оценка на съответствието. В техническата спецификация не е предвидено одитиране на процеса. В тази връзка, предлагам МЕУ да обмисли възможността в техническата спецификация да се предвидят и задължения на разработчика за участие в посочения процес.
5. Аналогично на чл. 8 на действащия Закон за електронната идентификация да се предвиди възможност за извършване на дейностите по потвърждаването на самоличността на лицата чрез физическо присъствие да се извършват и от трети страни, които отговарят на определени условия.

Автор: ИВАН ДОБРОВОЛОВ (04.03.2022 15:22)

Достъпност за хора с увреждания
Електронния подпис е особено важен за хората с увреждания, тъй като чрез него те могат да бъдат значително улеснени в комуникацията и упражняването на своите права.

Той е още по-важен за хората със зрителни увреждания, тъй като съществуват дори и законови изисквания, които усложняват упражняването на тези права (например чл. 189, ал. 2 от ГПК, който изисква сляп, но грамотен човек да се подписва саморъчно, но за да е признат от съда като частен, документът трябва да е приподписан допълнително от двама свидетели).

С оглед на това, за да няма риск от дискриминация, следва при определянето на фирмите, разработващи софтуер за електронни подписи, да спазват изискванията за достъпност както на настолните и мобилните приложения, така и на уеб услугите.

При задаване на техническите изисквания, например при тръжни процедури, следва изрично да се изисква електронните услуги, свързани с електронния подпис да са достъпни за хора с увреждания, и по-специално, за хора със зрителни увреждания.

Като универсален стандарт може да се посочи WCAG 2.1, който е възприет от ЕС като стандарт, с който трябва да са съобразени публичните уеб сайтове и предлаганите от тях мобилни услуги, включително и препоръките на w3c за Accessible Rich Internet Applications (WAI-ARIA).

В заключение, моля да имате в предвид, че при съставянето на Техническата спецификация за изграждане на мобилно приложение за електронна идентификация и електронно подписване – BGID, следва да включите и изисквания за достъпност за хора с увреждания (вкл. зрителни) на крайния продукт.

Автор: Христо Филипов (04.03.2022 14:45)

Коментари и предложения, част 2

8. Авторски права срещу софтуер с отворен код – в някои случаи може да е по-полезно да се активират вече съществуващи продукти, включително защитени с авторски права и/или патентовани продукти. Използването на доказани и сертифицирани критично важни компоненти е жизненоважно за осигуряване на постоянна сигурност и създаване на доверие и увереност в системата. Това може да бъде по-рентабилен и по-малко отнемащ време подход в случаи на компоненти, които са жизненоважни за получаване на услуга с eIDAS съвместимост. Това се отнася особено за компоненти като QSCD и някои от решенията за приобщаване, които са от решаващо значение за определяне на нивото на сигурност на цялата услуга. Това конкретно се отнася до:

- Софтуер за заснемане на документи
- Софтуер за биометрично данни
- “Liveness” Софтуер (за засичане на жив човек).
- Създаване на QES

9. Решението трябва също така да гарантира съответствие със следните международни стандарти:

- ICAO 9303: Машинно четими пътни документи
- NIST FRVT: Биометрично лицево разпознаване
- ISO/IEC 30107 - 3: Биометрично разпознаване на атака
- ISO/IEC 19795 - 1:2006: Ефективност на биометрична проверка
- eIDAS EN 319 - 401: Квалифицирани подписи

10. Позоваване на регламента за създаване на единна цифрова платформа – това трябва да бъде изключено от търга, тъй като е извън обхвата на цифровата идентичност. Добре е да се работи по този въпрос отделно и да не се комбинира с проекта за цифрова идентичност.
11. Не е ясно дали и как ще бъде закупен необходимия хардуер. Или дали участникът трябва да предостави също така и хардуера. Това се отнася за хардуер като HSM-s(Hardware Security Modules) например. При някои от компонентите на цялата система за цифрова идентичност и при конкретни софтуерни продукти може да има нужда и от специфичен хардуер.
12. Изискването на специфични видове поддръжка за удостоверяване и цифрово подписване (като SAML) или всякакви други специфични технически решения, които имат няколко възможни опции, може да изключи някои от другите технологии за цифрова идентичност от търга. Препоръчително е такъв вид изисквания да бъдат по-общи и да не се отнасят за специфични неща като SAML,

или подобни.

С риск да се повторя добавям и следните предложения:

- Системата трябва да включва технологии, обезпечаващи надеждна регистрация и последваща проверка, посредством реален ("жив") човек в реално време, посредством надеждни устройства и среди.
- Системата трябва да осигурява текущо и специално управление на заплахите, когато поддържа националните програми за идентичност и високорискови транзакции, което предпазва от непрекъснато развиващия се пейзаж на заплахите (включително дълбоки фалшификати, атаки с инжекции и т.н.)
- Системата трябва да използва сертифицирани по eIDAS компоненти (сертифицирани за високо ниво на LoA), които са били използвани в сертифицирани от ЕС eIDAS внедрявания на живо.
- Системата трябва да се придържа към процеси за управление на сигурността и производителността, включително биометрична производителност, независимо тестване на платформата и сертифициране

Автор: Христо Филипов (04.03.2022 14:44)

Коментари и предложения

1. Изискванията и проектът като цяло трябва да бъдат оперативно съвместими с предвидения портфейл за цифрова самоличност на ЕС за всички европейци (https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2663).

   Това е от голяма важност, за да се гарантира, че българските граждани могат да използват приложението за достъп до отговарящи на условията услуги на ЕС в други държави-членки. От решаващо значение е да се гарантира, че България може да работи на дигиталния пазар на ЕС, така че гарантирането на оперативна съвместимост и текущото съответствие с тези нововъзникващи стандарти от началото на този проект е от решаващо значение. Опитът за модернизиране на оперативната съвместимост след създаването на приложението няма да работи.

2. С оглед на раздел 1 от документацията, не се споменава одит и сертифициране. Тъй като целта е закупуване на съвместими с eIDAS решения, одитът на услугата трябва да бъде включен в търга и в планирането на сроковете. Не е реалистично разработките и одита да се извършат в рамките на 9 месеца, както се изисква в документите. Ако съответствието с eIDAS е важно, трябва да бъде включенн и одит. Реалистичен срок за извършване на одит за съответствие с eIDAS е 1 година. Ако повечето от компонентите на услугата ще се разработват специфично само за България, може да има нужда от удължаване на този период. Това е особено важно, ако в България в рамките на този проект ще се прави ново устройство за създаване на квалифициран подпис (QSCD).
3. Не се споменава CA(Certificate Authority) и CA услуги. Това е жизненоважен компонент на всяка система за цифрова идентичност и в тръжните документи трябва поне да се споменава за CA, в случай че CA е извън обхвата на тази

оферта.

4. Изискванията за разработка на софтуер са прекалено подробни. Такива изисквания биха били добре, ако целта е закупуване на ресурси за разработчици. Но ако целта е да се закупи крайният резултат, тогава трябва да има повече гъвкавост в процеса на разработка.
5. Изискванията в раздел 7 са твърде подробни и в същото време някои от важните изисквания липсват в този раздел. Препоръчително е вместо такива подробни изисквания да има препратка към някои стандарти, най-добри практики или подобни.
6. По-подробни SLA изисквания трябва да бъдат включени в тръжната документация. Ако участникът знае броя на потребителите, той може да прецени по-точно цената и възможностите на цялата система. Следователно изискванията на SLA, включително броя на потребителите, необходимото време за реакция и т.н., трябва да бъдат включени в офертата.
7. Поддръжката и техническото обслужване трябва да бъдат включени като изискване в документацията на възложителя. Понастоящем гаранционните изисквания са повече за необходимостта от поддръжка и обслужване, отколкото за действителните гаранционни случаи. Следователно може да има отделни точки за поддръжка и техническо обслужване.

Автор: Михаил Михайлов (04.03.2022 12:59)

към документацията

Във връзка с обявено преразглеждането на Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета чрез съобщението на Комисията от 19 февруари 2020 г., озаглавено „Изграждане на цифровото бъдеще на Европа“, с цел да се подобри неговата ефективност, да се даде възможност и на частния сектор да се възползва от него и да се насърчи използването на надеждна цифрова самоличност от всички европейци, както и с че в проекта за Изграждане на мобилно приложение за електронна идентификация и електронно подписване – BGID, е заложено съответствие с известните изисквания към европейски дигитален портфейл , с настоящето предлагаме промени, които в по-голяма степен да гарантират, че Българските граждани ще получат, решение отговарящо на най-съвременните изисквания за цифрова самоличност, като потребителят ще може да контролира количеството данни, предоставяни на доверяващите се страни, и ще бъде информиран за атрибутите, необходими за предоставянето на конкретна услуга.

1. В точка:

1.2.Технологични дефиниции

Да се добави

Термин	Описание	
Европейски портфейл за цифрова самоличност	Лични цифрови портфейли, които позволяват на гражданите да се идентифицират по цифров път и да съхраняват и управляват данни за самоличност и официални документи в електронен формат. Тези документи може да включват свидетелство за управление на МПС, медицински рецепти или дипломи. С помощта на портфейла гражданите ще могат да доказват самоличността си, когато това е необходимо, за да получат достъп до услуги онлайн, да споделят цифрови документи или просто да докажат конкретна лична характеристика, например възраст, без да разкриват своята самоличност или други лични данни. Във всеки един момент гражданите ще имат пълен контрол върху данните, които споделят.	

2. В точка:

2.3.За проекта

Настоящият проект обхваща дейности по изграждане на приложение за мобилна електронна идентификация и подписване BGID, като целите на проекта са

реализират въвеждане на използването на идентификация на потребителите посредством национален електронен идентификатор.

Да се промени, както следва:

2.3.За проекта

Настоящият проект обхваща дейности по изграждане на приложение за портфейл за цифрова самоличност за мобилна електронна идентификация и подписване BGID, като целите на проекта са реализират въвеждане на използването на идентификация на потребителите посредством национален електронен идентификатор.

3. В точка:

2.4.Нормативна рамка

Проектът се осъществява в съответствие с изискванията, регламентирани със следните нормативни актове и стратегически документи:

.....

Да се добави в:

Международни стандарти:

- ISO/IEC 18013-5:2021 - Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application

4. В точка:

3.4.Очаквани резултати

Очакваните резултати от изпълнението са:

- Изградени мобилни приложения за електронна идентификация и подписване
- Надградени пилотни системи с високо ниво на използване от граждани и бизнес за използване на мобилна идентификация и подписване
- Повишаване на използването на вече съществуващи електронни административни услуги

- Високо ниво за готовност за покриване на изискванията на предложението за изменение на Регламент (ЕС) 910/2014 за т.нар. европейски дигитален портфейл, след влизането му в сила

Последния параграф да се промени, както следва:

- Високо ниво за готовност за покриване на изискванията на предложението за изменение на Регламент (ЕС) 910/2014 за т.нар. европейски дигитален портфейл, след влизането му в сила. В този случай мобилното приложение за електронна идентификация и електронно подписване – BGID трябва да се развие в приложение BGID за портфейл за цифрова самоличност.

Автор: Михаил Михайлов (04.03.2022 12:59)

към документацията

Във връзка с обявено преразглеждането на Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета чрез съобщението на Комисията от 19 февруари 2020 г., озаглавено „Изграждане на цифровото бъдеще на Европа“, с цел да се подобри неговата ефективност, да се даде възможност и на частния сектор да се възползва от него и да се насърчи използването на надеждна цифрова самоличност от всички европейци, както и с че в проекта за Изграждане на мобилно приложение за електронна идентификация и електронно подписване – BGID, е заложено съответствие с известните изисквания към европейски дигитален портфейл , с настоящето предлагаме промени, които в по-голяма степен да гарантират, че Българските граждани ще получат, решение отговарящо на най-съвременните изисквания за цифрова самоличност, като потребителят ще може да контролира количеството данни, предоставяни на доверяващите се страни, и ще бъде информиран за атрибутите, необходими за предоставянето на конкретна услуга.

1. В точка:

1.2.Технологични дефиниции

Да се добави

Термин	Описание	
Европейски портфейл за цифрова самоличност	Лични цифрови портфейли, които позволяват на гражданите да се идентифицират по цифров път и да съхраняват и управляват данни за самоличност и официални документи в електронен формат. Тези документи може да включват свидетелство за управление на МПС, медицински рецепти или дипломи. С помощта на портфейла гражданите ще могат да доказват самоличността си, когато това е необходимо, за да получат достъп до услуги онлайн, да споделят цифрови документи или просто да докажат конкретна лична характеристика, например възраст, без да разкриват своята самоличност или други лични данни. Във всеки един момент гражданите ще имат пълен контрол върху данните, които споделят.	

2. В точка:

2.3.За проекта

Настоящият проект обхваща дейности по изграждане на приложение за мобилна електронна идентификация и подписване BGID, като целите на проекта са реализират въвеждане на използването на идентификация на потребителите посредством национален електронен идентификатор.

Да се промени, както следва:

2.3.За проекта

Настоящият проект обхваща дейности по изграждане на приложение за портфейл за цифрова самоличност за мобилна електронна идентификация и подписване BGID, като целите на проекта са реализират въвеждане на използването на идентификация на потребителите посредством национален електронен идентификатор.

3. В точка:

2.4.Нормативна рамка

Проектът се осъществява в съответствие с изискванията, регламентирани със следните нормативни актове и стратегически документи:

.....

Да се добави в:

Международни стандарти:

- ISO/IEC 18013-5:2021 - Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application

4. В точка:

3.4.Очаквани резултати

Очакваните резултати от изпълнението са:

- Изградени мобилни приложения за електронна идентификация и подписване
- Надградени пилотни системи с високо ниво на използване от граждани и бизнес за използване на мобилна идентификация и подписване
- Повишаване на използването на вече съществуващи електронни административни услуги
- Високо ниво за готовност за покриване на изискванията на предложението за изменение на Регламент (ЕС) 910/2014 за т.нар. европейски дигитален портфейл, след влизането му в сила

Последния параграф да се промени, както следва:

- Високо ниво за готовност за покриване на изискванията на предложението за изменение на Регламент (ЕС) 910/2014 за т.нар. европейски дигитален портфейл, след влизането му в сила. В този случай мобилното приложение за електронна идентификация и електронно подписване – BGID трябва да се развие в приложение BGID за портфейл за цифрова самоличност.

Автор: Boian Baev (04.03.2022 00:37)

Обща препоръка - само малко допълниение

Частни схеми за е-ИД поддържат двата ДКЕУУ - БОРИКА АД и Евротръст.

Автор: Boian Baev (04.03.2022 00:37)

Обща препоръка - само малко допълниение

Частни схеми за е-ИД поддържат двата ДКЕУУ - БОРИКА АД и Евротръст.

Автор: Boian Baev (04.03.2022 00:37)

Обща препоръка - само малко допълниение

Частни схеми за е-ИД поддържат двата ДКЕУУ - БОРИКА АД и Евротръст.

Автор: Boian Baev (03.03.2022 17:33)

Обща препоръка

Днес е Националия ни празник ... На всички „ЧЕСТИТО“ ...

А сега кратък коментар по т.н. Техническа спецификация за BGID !

Забележете, Спецификацията е за мобилно приложение за е-идентификация и е-подпис, т.е. за нещо, което „виси ей-така свободно“, а не в обхвата на изпълнение на национална ТЕХНИЧЕСКА СХЕМА ЗА е-ИД и е-подпис (било то усъвършенстван или квалифициран). Та нали имаме Закон за електронната иденти.фикация (ЗЕИ), който е приет и „втасва“ от няколко години... . Само е споменато, че това приложение следва да се осъществи в съответствие със съответстващите и известни нормативни актове за е-управление (включително и ЗЕИ). И понеже е за е-ИД, най-вече трябва да

съответства на ЗЕИ. А това е възможно само ако приложението се „потопи“ (т.е.работи) в установена и изградена национална ТЕХНИЧЕСКА СХЕМА за е-идентификация с нейните субекти-участници в схемата (Орган на е-ИД – МВР, съответни Администратор(и) (напр. ДКЕУУ), Център/по-скоро Центрове за валидация и техните ИТ-системи и Регистри, и най накрая лицата, които ще ползват приложението). Така, че мобилното приложение е последната „брънка“ на СХЕМАТА !!!

В този смисъл, добре е в Техническата спецификация да има отделен раздел, определящ една ВАЛИДНА национална схема за еИД (ако има/е взето конкретно решение), така че бъдещата ОП за мобилното BGID да адресира тази схема. Още повече, че към настоящия момент вече има имплементирани и успешно се ползват технически решения базирани на мобилни приложения за издаване, регистрация, валидация и поддръжка на е-ИД и на мобилен/облачен КЕП на физически лица и такива, представляващи юридически лица. Това са частни схеми за еИД, които сравнително бързо и лесно могат да се изградат до национален обхват (в предвид много краткия период за реализация на BGID) и впоследствие да се нотифицират като национални-частни такива. Примери за такъв спешен подход в Европейския съюз има много ...

Ако има такъв раздел в предлаганата Техническа спецификация, бъдещата ОП ще адресира много точно поченциални и успешни участници в реализацията на BGID.

А и още нещо, което не следва да се забравя – промените в Регламент 910/2014 на ЕС за удостоверителните услуги (и специално за е-идентификацията). Като следствие – това е European digital identity Wallet (както мобилен, така и web-базиран), който ще адресира както националната така и през-граничната е-идентификация заедно с доставка на валидирани е-атестати/атрибути за лицата.

Б. Баев

Автор: Румен Николов (02.03.2022 17:52)

Коментари по спецификацията (продължение)

А как биха реагирали от ЕК/ЕС, ако бъдат реализирани и двете системи и се окажем с два различни root CA, които претендират да издават валидна електронна идентичност?!

И не на последно място, използването на УЕИ като подпис не е уредено нито в закона за електронна идентификация, нито в правилника за прилагането му. В тази връзка според мен е редно първо да се направят промените в закона, а не първо да се напише софтуера и след това фирмата, която го прави, да предложи и съответните законови промени, както е и написано в текущата спецификация. Това не би било проблем за електронната идентификация като част от проекта „поколение 2019“, тъй като е предвидено системите трябва да се адаптират при промени в законодателството.

Румен Николов

Автор: Румен Николов (02.03.2022 17:50)

Коментари по спецификацията

Идеята за електронна идентификация чрез телефон не е лоша като цяло. Описаната в този проект, според мен обаче, има доста проблеми и дава повече въпроси, отколкото отговори.

КЕП е с валидност до 3 години и не би следвало да се използва до края на изтичането на валидността му, а не както е описано в т. 4 от текущата спецификация – „до 1 година след влизане в продукционен режим на националната схема по ЗЕИ“.

Доколкото става ясно т. 4 от текущата документация, КЕП, ПИК на НАП/НОИ, и УКД на НЗОК могат и в момента се използват за достъп до електронни административни услуги само в България. **Целта на този проект е САМО да осигури възможност за ползване на трансгранични електронни услуги в рамките на ЕС**: „Чрез посочените средства обаче българските граждани не могат да се идентифицират, когато заявяват електронни административни услуги в други държави-членки на Европейския съюз, което препятства възможността за ползване на трансгранични електронни услуги в рамките на ЕС.“

Кое налага необходимостта да осигурим ползване на трансгранични електронни услуги в рамките на ЕС в момента? В техническата спецификация по този проект се споменават САМО електронни административни услуги в България! А за тези услуги и в момента има работеща електронна идентификация!

В тази връзка – ако ще бъде правена реализация на проекта в този му вид, е необходимо да бъде добавен и регистър/списък на наличните трансгранични електронни услуги в рамките на ЕС, от които ще могат да се възползват българските граждани.

Не мисля, че желаещите да използват трансгранични електронни услуги в рамките на ЕС, каквато е и целта на този проект, са толкова много, че да се реализира допълнителен проект за електронна идентификация.

Използването на смартфон/таблет или друго устройство е възможно съгласно техническата спецификация в Приложение 8 от обществената поръчка с наименование „Проектиране, изграждане и управление на Система за издаване на български лични документи поколение 2019“. УЕИ може да бъде записан на устройствата след като се регистрират от съответен Администратор в Подсистемата за управление на носители (ПУН). Но генерирането на електронния идентификатор, както и всички други регистри и процеси свързани с издаване на УЕИ, ще са изградени и няма нужда да бъдат дублирани. Т.е. така предложената схема за електронна идентификация ще дублира над 90% функционалностите и изискванията, описани в Техническата спецификация Приложение 8: „Изграждане на централизирана система за електронна идентификация“, която е част от обществената поръчка за документи „поколение 2019“, а за тази поръчка има и

определен изпълнител.

Текущата система за персонализация на български лични документи стартира в началото на 2010 г. Техниката е на над 12 години, като на станциите за снемане на биометрични данни все още се използва Windows XP, която отдавна не се поддържа от Майкрософт. Стартирането на производство на документи „поколение 2019“ е предвидено за около 2 години след подписване на договора. Това значи, че трябва да бъде осигурена поддръжка на техниката към текущата система, която започва 13та година от амортизационния период за още минимум 2 години. Спирането или промяната на поръчката за документи „поколение 2019“ ще отнеме поне 2 години, които ще трябва да бъдат добавени към поддръжка на текущата система за издаване на лични документи. Колко човека имат работещ принтер на над 15 години?

Заслужава ли си да се стартира нова обществена поръчка за дейност, която всъщност до голямата си степен е част от вече стартирана обществена поръчка, на която има и определен изпълнител?

В момента идентификацията на граждани за достъп до електронните услуги на администрацията работи. Аз лично имам и ПИК на НАП, на НОИ и КЕП и използвам активно съществуващите електронни услуги. Не мисля обаче, че е необходимо дублирането на реализирането на националната схема за електронна идентификация и това дублиране да се оправдава само с цел ползване на трансгранични електронни услуги в рамките на ЕС. Условията за сигурна и надеждна електронна идентификация на гражданите при предоставяне на електронни административни услуги са заложени като част от обществената поръчка за лични документи „поколение 2019“.

Не е редно за едно и също нещо да се разходва два пъти обществен ресурс. Освен системите за издаване и регистрация на УЕИ ще бъде дублирана и PKI инфраструктурата (HSM устройства, сървъри …), които са и в другия проект.

Автор: Моско Аладжем (02.03.2022 17:03)

Някои препоръки по спецификацията

Поздравявам колегите за публичното представяне на спецификацията.

Ето няколко мисли по представения текст:

1. Документът би спечели, ако се знае, кой е авторът или авторите. От една страна ще сме сигурни, че авторът няма да е свързан с бъдещия изпълнител. От друга страна всичко, което ще бъде написано в крайния вариант, ще има по-голяма тежест и отговорност.

2. Спецификацията планира с обществена поръчка да се избере изпълнител, на който да се възложи отговорната задача за изгради национален **модел за създаване, разпределение и използване на криптографски ключове за целите на реализирането на електронната идентификация и подписване**. Това трябва

да се извърши в Дейност 1.

Ако Възложителят одобри резултата на Дейност 1, наречен “Системен проект”, Изпълнителят ще продължи с разработването на необходимия софтуер.

Проблемите, които виждаме в това направение, са следните:

1. Разчита се Изпълнителят да изгради национален модел, който Възложителят да одобри. Но какво ще се случи, ако моделът не се окаже „читав“ и не трябва да бъде одобряван, но има договор, в който софтуерът трябва да бъде готов до края на лятото или есента. Не е ли по-добре администрацията, в лицето на специалистите, създали Архитектурата на електронното управление, да поемат отговорността и да публикуват за обсъждане този модел.
2. Електронната идентификация не е „от вчера“. Мобилната също: https://www2.e-gov.bg/bg/events/54
3. Едва ли някой мисли, че този проект ще започне от кота“0“ („to start from SCRATCH“). Не е ли по-добре да се посочат, кои вече съществуващи модули, от вече публикувани проекти, намиращи се в наличните хранилища за проекти от този тип, трябва да бъдат използвани.
4. Внушението ми е, че е време специалистите, създаващи спецификации за софтуер в отворен код, да спрат да планират финансирането на едни и същи дейности (едни и същи по функционалност модули). Очевидната ни цел е да има многократно използване на вече разработения с държавни средства софтуер и така да се спести време и да се намали реалната цена на създавания продукт, в интерес на обществото.
5. Вярно е, че на стр. 22 на спецификацията е казано: „Да се изследва възможността резултатният продукт (Системата) да се изгради частично (библиотеки, пакети, модули) или изцяло на базата на съществуващи софтуерни решения, които са софтуер с отворен код“, но се планира това да стане, след като е спечелена ОП и е сключен договор за разработване на всички модули. Някак си не ми се вярва, че някой Изпълнител ще върне 60 или 80 % от финансирането на Възложителя, защото в хода на изпълнение на проекта е решил да използва готови библиотеки.
6. В заключение бих препоръчал:
   a. Авторите на спецификацията да публикуват модела, по който трябва да се изгради системния проект за обсъждане.
   b. Авторите на спецификацията да посочат библиотеките, които трябва да бъдат използвани от бъдещия изпълнител.
   c. Бих препоръчал самият проект да бъде разделен на няколко независими SOA `модули, които да бъдат реализирани паралелно от различни изпълнители под компетентния и зорък поглед на българското ИТ общество.
   d. Тъй като Възложителят, в лицето на МЕУ, не планира с този проект да се усвояват големи средства(искрено се надяваме, че е така), възлагайки задачата по създаване на основните модули на отделни лица или малки колективи ще се избегнат проблемите, свързани с големите обществени поръчки. Нещо повече ще се избегне налагането на монопол на едни или други фирми, което е една от целите на новия подход.

Автор: Станимир Минков (24.02.2022 16:21)

тестов коментар 2 администратор
до: Божидар Божанов, министър МИНИСТЕРСТВО НА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ гр. София   П О З И Ц И Я   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“).

Автор: Станимир Минков (24.02.2022 16:19)

тестов коментар 1 администратор
тестов коментар 1 администратор

Автор: Апостол Николов (23.02.2022 12:30)

Одит на приложението от международна компания по сигурността

Въпросната система ще представлява единна точка на достъп до държавната администрация.

Това я превръща в "single point of failure".

От тази гледна точка е необходимо при избора на проект да се направи анализ на неговата сигурност.

Това, според мен се вижда в почти всички коментари.

Затова смятам за уместно, да се привлече трета страна от сферата на киберсигурността, като допълнителен одит при избора на изпълнител и оценка на неговата работа.

Автор: Любомир Иванов (22.02.2022 10:09)

8.2.8 Процес на подписване

Предаването само на хеш и описание при подписване, може да доведе до това потребителя, без да подозоира, да подпише различен документ. Няма възможност такова подписване да може да бъде оспорено, тъй като потребителя никога не е имал достъп до документа - обект на подписване, за да може да провери неговата хеш стойност.

Странта, която изчизлява хеша трябва да има доверието на потребителя. Тъй като това условие е трудно да бъде постигнато, трябва да има възможност документа да бъде прегледан и неговия хеш да бъде изчислен на самото мобилно устройство. След сравнение на предоставения и изчисления хеш да се продължи с процеса на подписване.

Може да се специфицира списък от поддържани формати за документи за подписване, които да могат да бъдат преглеждани на мобилни устройства.

Алтернативно, описанието от т. 8.2.8 трябва да бъде част от процедурата по подписване, с локално изчисляване на хеш и включването на този хеш в електронния подпис.

Тази мярка би увеличила увереността у потребителя, че подписва това, което вижда.

Автор: Boris Todorov (21.02.2022 23:50)

Информационно обслужване АД - изпълнителя на тази спецификация

Предлагам да се проведе прозрачна процедура по ЗОП и да има реално състезание за избор на изпълнител. Злите езици говорят, че изпълнителя е вече известен и работи по реализацията и това е Информационно обслужване АД. Ако е така защо ни губите времето и говорите за прозрачност и равен старт на бизнеса в България. То и преди ИО АД вземаше, но нали щеше да има промяна. То в случай не промя, то и замяна или подмяна НЯМА.

Предлагам да се гарантира, че Информационно обслужване АД няма да е предизвестения изпълнител на тази поръчка.

Автор: Boris Todorov (21.02.2022 23:38)

Малко за начина на разработка

1. Agile нали това е техническа грешка. Моля се да е така. Нека не смесваме правенето на сайт със сериозен проект, който ще гарантира идентификацията на лицата пред държавата. Още повече, че този подход противоречи на етапите в т.6 и дейностите в т. 8. Кое ще правите с Agile - модела по т. 8.1 или разработката по следващата дейност. предлагам да се преразгледа изискваната методология за разработка и да се заложи класическа.

2. Документация - нищо по темата или то щото ИО АД ще го прави, няма нужда от документация. И недейте се кри зад т.9.2 Системен проект. Толкова жалко са описани изискванията към него, че повече не може и да бъде. МТИТС и ДАЕУ залагаха на точен опис на изискваните документи като част от разработката и не

знам кой го разпозна като лоша практика. Предлагам да се опишат в детайли цялата очаквана документация по проекта, включително конвенция за писане на код, за да няма после - Ние го публикувахме, ама само ИО АД може да си го чете.

3. Българите в чужбина пак сте ни забравили - или пак извади си ПИК, КИН, КЕП (ама български, защото сме родолюбци). Стига! Само не отхвърляйте бележката с .... то паспорта е за тях. А за чужденците - на първо място гражданите на държавите-членки на ЕС - няма ги и това е дискреминация или BGiD е само за българи и електронните услуги са само за тях. Придлагам да се включат ясни изисквания в спецификацията за възможност за идентификация за всички групи граждани. Да не забравяме и лицата с двойно гражданство.

4. По изискванията за гаранционна поддръжка и наличност на системата - Нали не си мечтаете да минете с тези изисквания - размити и на практика винаги оправдаващи изпълнителя ИО АД. Предлагам да се въведат изисквания за 365/24/7 подръжка, ясен SLA - например присумарно един час неработоспособност на годишна база - глоба от 20 % от стойността на проекта, време за реакция половин час, време за отстраняване на инцидент или решение възстановяващо работоспособността 1 час, изисквания за архитектура, която да гарантира пълна функционална резервираност на решението.

Много слаба първа спецификация, г-н Божанов - личи си че сте я бързали и правили на коляно. Дано актуализирания вариант също мине обществено обсъждане. Проектът е много важен и си заслужава внимание.

Автор: Драган Иванов (21.02.2022 10:12)

Използването на телефононер номер

Привет,

Предложението ми е да отпаднат изцяло изискванията за събиране/съхраняване/използване на телефонен номер: **"При регистрация, гражданите трябва да посочат и мобилен телефон и имейл адрес."**

и тук:

"В сървърната част на системата трябва да се съхранява:

...

контактна информация (имейл и телефон)"

и тук:

"Управление на устройствата

...

Всяко устройство (след първото) трябва да бъде валидирано с еднократен линк, изпратен на имейл и/или телефон (като SMS).

Към момента всяка аветентикация чрез мобилната мрежа (СМС или обаждане) обикновено е най-слабото звено в сигурността, като примери за това са всевъзможните SIM swapping атаки, включително и чрез съдействието на недобросъвестни служители в мобилните оператори. Отделно от това, в глобален свят и с милиони българи зад граница (и извън ЕС), много от които не поддържат български номер, използването на телефонен номер е непрактично и ненужно. Известията към потребителите могат да са изцяло чрез приложението и/или чрез имейл.

Относно добавяне (оторизация) на допълнително устройство: вместо СМС, валидирането може да се осъществи чрез известия до всички вече регистрирани устройства за одобрение или отказ на новото устройство, и/или с линк изпратен по имейл.

С две думи, не виждам нито една добра причина да се съхранява и използва телефонен номер като средство и няколко причини да не се използва.

Поздрави за добре свършената работа до тук!

Автор: Георги Кременлиев (21.02.2022 09:50)

липса на физическа възможност за пропътуване на разстояние спрямо геокоординатите на IP адреса на по

Това е добър feature, но пък от гледна точка на "surveilance" е малко ограничаващо. и не, аргумента "ама вие какво ще кирете?" не е валиден.

Нека има информация за потербителя, и възможност той да поиска блокиране на ID-то си, но не и системата да го блокира автоматично.

Автор: Георги Кременлиев (21.02.2022 09:48)

физическа идентификация

осъзнавам че това не е целта за момента, но би било много удобно да се добави функционалност за идентификация и пред физически лица в самото приложение. Т.е. да мога да покажа на екрана информацията нужна за удостоверение + QR код за проверка на тази информация.

осъзнавам нуждата от промяна на законовата рамка, но мисля че тук му е мястото на един такъв feature.

Автор: Alex Stoykov (21.02.2022 01:57)

Коментар

Спецификацията е твърде техническа, не е продуктова.

-Приложението трябва да бъде тествано на ниво концепция с реални хора. Дали пенсионери или ниско образовани граждани биха могли да се регистрират и ползват приложението сами или ще бъдат дискриминирани?

-Изплозването на геолокация и камера изисква изричното разрешение от потребителя, което отново може да доведе до фал старт.

-Чужденците у нас могат ли да се възползват от това приложение ако нямат български документи на самоличност?

- Apple често де-регистрират приложения които използват геолокация или лични данни. Има ли план при такава ситуация? Покрива ли се от гаранционните условия?

Автор: Минотавър Херкулески (20.02.2022 23:12)

Дискриминационно предложение

Предложението е дискриминационно и дефакто изисква гражданите да използват не просто точно определени операционни системи, но и то с минимално изисквана версия.

Няма никаква причина държавата да спомага допълнително за монопола на Apple/Google в тази посока. Или го правите като хората - достъпно за всеки един гражданин, или изобщо не го правите.

Автор: Добромир Панчев (20.02.2022 21:02)

Локация и биометрични данни

Здравейте, поздравления за ясно и точно написаното задание! Както знаем, лихвари и тартори на определени групи имат незаконната практика да събират лични карти и банкови карти на групи хора и ги ползват от тяхно име. Това задължително трябва да избегнем при електронната идентификация. Не трябва да се разрешава повече от едно активно устройство. Идентификация само с биометрични данни - лицево разпознаване или пръстов отпечатък без възможност за замяната им с PIN на телефона. На устройствата на Apple това е възможно с конфигурация. Това гарантира физическото присъствие на човека поне доколкото масовите технологии го позволят. Проблем е, че пръстовите отпечатъци могат да се конфигурират в настойките на телефона и е възможно да се въведат и на друг човек, т.е. може да се злоупотреби. Лицевото разпознаване също може да се конфигурира за друг човек и това са проблеми, за които предполагам бихме могли да потърсим решение. Но поне могат да се случат само със съдействието на собственика. Приложението трябва са работи само когато GPS приемникът има fix с добра точност, за да може да се проследи локацията при злоупотреби.

Автор: Крис Хамид (20.02.2022 08:39)

Предложения за сигурност и поддръжка

Здравейте,

Призовавам за поддръжка на комплексни пароли до 99 символа и поддръжка на MFA приложения и ключове като : Yubikey / Yubico

Имаики предвид че потребителите ще имат разнородни устройства и версии на OS в разработката и тестването на мобилните приложение трябва да се заложи поддръжка на повече версии и OEM специфично за Android. Android 7 - 12 включително, Поради разликата между stock Android & OEM версиите и т.н.

Също така призовавам за разработване на Native приложения тъй като сигурността може да се обезпечи по-лесно спрямо Cordova, Xamarin и други multi-platform технологии и плюс това в бъдеще ще бъде по-лесно надграждането на приложенията, обновления и адаптация към нови версии на OS.

https://developer.android.com/topic/security/best-practices#java

Автор: Елиан Куртев (19.02.2022 10:11)

Тестване и ОС

Здравейте,

Освен направените вече коментари, според мен трябва да бъдат уточнени и ясно записани няколко малки детайла:

1. т.8.3.1 и т.8.4.1 - Мобилно приложение разработено за операционните системи Android и iOS, работещо на **смартфони, с минимална версия на оперционната система, както следва:**

1. **За смартфони поддържащи Android OS - v.9.0;**
2. **За смартфони поддържащи iOS - v.12.0;**

Според закона "Мобилно приложение" е приложение работещо на мобилни у-ва - "като смартфон или таблет". Следователно се получава двузначност, тъй като Android OS се поддържа, както на таблет, така и на смартфон, докато от Apple решиха наскоро да сменят името на операционната с-ма на техните таблети на iPadOS. Ясно е, че iPadOS, стъпва изцяло на iOS, но това уточнение ще внесе яснота дали приложението ще бъде разработено само за смартфони или както за смартфони, така и за таблети. В случай, че е за двата типа устройства , то тогава със сигурност scope-ът ще се увеличи, макар и с малко.

2. т. 6.4 - частта "..., за да се демонстрира", според мен, трябва да бъде заменена с "..., за да бъде валидирано". "Валидацията" означава много повече в софтуерната разработка, а именно, че ще бъде изпълнено тестване, чрез различни техники, което всъщност ще демонстрира правилното изпълнение на изискванията.

ISTQB definition - "validation:

Confirmation by examination and through provision of objective evidence that the requirements for a specific intended use or application have been fulfilled."

Автор: Пламен Колев (19.02.2022 09:51)

Коментар

По отношение на 7.2.3:

Бих добавил и "Pilot" логическа среда. Нейното място е между Staging (Test) и Production. Pilot е среда, максимално близка до реалната, където се извършва тестване на Release Candidate версия на софтуера с натоварване максимално близко до реалността.

По отношение на 7.2.5:

Системата за ежедневен бекъп на данните следва да бъде организирана по два параметър: географски и локален. Географски е за сигурност на съхранението на данните и застраховка (защита) от непредвидени ситуации - пожар, земетресение,... Локален е за скорост на възстановяване.

Автор: Георги Кременлиев (19.02.2022 09:21)

Коментари

HSM са споментаи май само на едно място. Мисля че трябва да бъде казано изрично като изискване за съхраняване на ключовете на сървера.

има на много места в текста "или" (напр. или PIN или биометрика). знам че се опитвате да направите заданието възможно най-отворено за различни технологии, но на мен ми изглежда че печелившия участник ще избере пътя на на най-малкото съпротивление и ще направи само по-лесния вариант, което ще е пак стъпка в правилната посока, но ми се иска да се поддържат повече възможности от начало.

говорейки за възможности, мисля че е добра идея в такъв проект да бъде заложена и извън-гаранционна поддръжка по зададени параметри за да може системата да бъде доразвивана бързо при възникване на нови изисквания на базата да този спечелен договор. Нека тази поддръжка да бъде период от поне 5 години и да има

някакви рамки, но да я има и да не се чуди министерството как да си поиска някоя бърза доработка само защото трябва да пуска нова обществена поръчка.

Иначе посоката на документа е правилната и дори и в този вид да остане е огромна крачка напред!

Автор: Иван Атанасов (18.02.2022 23:32)

Първоначална регистрация.

Здравейте,

Поздравления за проекта, само лек коментар относно текст в т. 8.2.2 "При регистрация, гражданите трябва да посочат и мобилен телефон и имейл адрес."

Не смятам за удачно системата да изисква телефонен номер за завършване на регистрация. Често има граждани които имат устройства, но не и активен номер, било то по тяхно желание или не. Ако все пак се иска телефонен номер нека то е по желание за получаване на определени уведомления. Тъй като приложението може да доставя нотификации/известия и без него. И да може да се избира предпочитан метод за връзка. Ако има няколко, email, телефонен номер, нотфикации.

Другото на което смятам, че може да се обърне внимание е прехвърлянето на друго у-во. Добре е да се заложи метод с паспорт и с новите лични карти, с чип тъй като те ще съществуват, а ПИК на НОИ/НАП най-вероятно ще бъде закрит като система. За да може да има алтернатива на СМС и да не зависи достъпа към е-услуги от достъп до телефонен номер.

Благодаря Ви!

Автор: Виктор Никифоров (18.02.2022 20:53)

Предложение за функционалност

Електронната идентификация, чрез мобилно устройство би трябвало да може да работи и без наличие на интернет, както и да се използа за идентификация на гражданин използващ друго устройство за достъп до интернет, а не мобилното устройство с инсталираното и активирано приложение за eID.

Хипотетичен сценарий: Имаме активиран мобилен телефон с електронна идентификация, без мобилен интернет и WIFI. Имаме и наличен десктоп компютър с LAN достъп до интернет и липса на безжична комуникация. Потребителя би трябвало, използвайки мобилното си устройство да може да се идентифицира пред органите на държава, използвайки стационарния компютър и неговия браузър.

Възможност решение на горния проблем е мобилното устройство (приложението за eID) да генерира еднократен токън или нещо друго, което да може да се използва за идентификация на потребителя.

Автор: Vasko Tomanov (18.02.2022 18:26)

Бележки по документа
Разгледах документа подробно:

- Първото ми впечатление е че е доста подробен и не съм напълно сигурен дали всички детайли за технологии и изисквания имат приложение тъй като може голяма част от тях да нямат общо с реалното изпълнение а от друга стара следенето за спазването им ще оскъпи нещата сериозно - и трябва да се очаква сериозна цена за вътрешен контрол от самия разработчик по проекта - като минимум моята оценка е за 2-ма постоянно заети които да проверяват всеки детайл дали отговаря на заданието.

Нещо което липсва:

- Хората си губят и сменят телефоните - и това се случва на най-неподходящите места - например на почивка в чужбина, командировка и т.н. - и не видях (може да съм пропуснал) да има изискване за лесно преместване на приложението от един телефон на друг или на нов телефон и оторизирането му за работа на този нов телефон/устройство.

За технологиите :

Те са от две части :

1. Идентификация (Identity)

2. Подпис (Sign)

1. Идентификация

- Машинно(вътрешно - уникално) ID - има си добре известен сигурен начин и той се нарича UUID (GUID a windows потребителите) - всякакви други съчинения по темата могат да доведат до неприятни резултати (например ако се налага издаването му на разпределени места а не от централно - другите технологии имат проблем с това)

- Човешко ID (Human Readable) - стандартната практика е национален идентификационен номер + фамилия (в нашия случай ЕГН и Фамилия)

- Начини за първоначална идентификация : Съвременните са или с SMS/Vibre код или с токен (token/code) който се генерира на мобилно устройство на което се подава ПИН(pass-code) 5 цифри набрани от потребителя и то използвайки този ПИН + времето (предполага се че мобилното устройство е със синхронизиран таймер) - и резултата обикновено 8 цифри се подава към сървъра като втората част от two-factor идентификация - алгоритъма е добре познат - HMACSHA на RSA като вече патента е паднал и свободен за използване

2. Подписване

- Използват се генерално три начина :

I. chalenge-response подава се код от сървъра (може да се сканира QR код или просто да се набере в телефона от екрана) + ПИН(pass-code) 5 цифри и използвайки HMACSHA се получава отговор който се навира на страницата и се проверява от сървъра и записва - това е прост ясен и добър начин

II. SMS/Vibre код който се праща и се записва в страницата - не е много добър вариант но е достатъчно сигурен също

III. Публичен/Частен ключ (в момента обикновено се използва Elliptic-curve cryptography) като публичния стой в сървъра а частния в приложението - пак се отключва с ПИН и има проблем с предаването до сървъра тъй като не малък по обем и не може да се напише просто на уеб страницата (ако услугата се достъпва от компютър а се оторизира от телефон) - има решение с fingerprint на подписа - но накрая пак стигаме до необходимост от Интернет на мобилното устройство в момента на подпис - което е сериозен проблем в много ситуации.

История

Начало на обществената консултация - 18.02.2022

Приключване на консултацията - 04.03.2022

Справка за получените предложения

Справка или съобщение.