КОМЕНТАРИ КЪМ ОБЩЕСТВЕНА КОНСУЛТАЦИЯ ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ ЗА ЕЛЕКТРОННА ИДЕНТИФИКАЦИЯ И ЕЛЕКТРОННО ПО
Коментар
Добавяне на функционалност за автоматична валидация чрез устройства без операторПред функционалност за валидация чрез автоматични (и понякога подвижни, т.е. без фиксиран а валидатори.Автоматични валидатори са устройства (технически средства), които могат да валидация на идентичност, по QR код, презентиран от мобилното приложение на лицето, к идентифицира, без наличие на оператор (човек) обслужващ процеса на валидация.Бизнес п услуга на BGID – идентификация на физически лица на киоски (например за плащане на см обществен транспорт чрез устройства за автоматична валидация на превозни документи и на работа и модел за реализация:-необходимо ниво на идентификация „ниско“ до "значите приложение BGID генерира при поискване от потребител криптиран QR Код за автоматична съдържа токен, издаден от сървърната част на системата за идентификация. По този токе които може да са носени в QR, или в сървъра на BGID, валидаторът може да извършва офла проверка на лични данни чрез обръщение към API на BGID. -примерно приложение - токенъ идентифицира пътник в обществен транспорт, които (анонимно или не за превозвача), мож “сметка” в системите на превозвача, асоциирана с токена, с която са свързани превозни до предварително закупени, или налични с отложено плащане. По този начин BGID приложени за пътуване в обществения транспорт, а и в редица други ситуации. Подобен механизъм е опазване на лични данни, например за несподеляне с транспортния оператор на информац (например преференция при пътуване за студент, ученик, пенсионер и др.) и лични данни преференциално пътуване, а само, чрез достъп до съответен регистър, удостоверяване на преференция, оставайки потребителят анонимен за транспортния оператор.-правата на ва набор от лични данни могат да се определят на база на договорени отношения с доставчик ползващи автоматична валидация.

Бележки и коментари по проектаПубликуваният проект на „Техническа спецификация за и
приложение за електронна идентификация и електронно подписване – BGID“ не е в съотве
нормативна уредба (Законът за електронната идентификация и правилника за прилагане
регламентира технологията и обществените отношения свързани с предоставяне и ползва
идентификация. В тази връзка за да изпълни администрацията принципите на публичност
промяната на правната уредба е необходимо да предхожда действията по реализация на и
и приложения.Техническата спецификация изключва възможността потребителите, които
квалифициран електронен подпис да го използват за подписване на електронни документи
приложение. Това ще създаде неудобство и объркване на потребителите, на които ще се н
ползване на електронни административни услуги през приложението да използват усъвър
подпис, а при ползване на електронни услуги, предоставяни от лицата, осъществяващи пуб
организации, предоставящи обществени услуги да използват притежавания квалифициран
тази връзка предлагам спецификацията да се допълни с изисквания за разработване на пр
и интеграция със системи на трети страни, които предоставят услуги за отдалечено подпи
спецификация не е предвидена възможност за лицата по чл. 1, ал. 2 от Закона за електрон
използват извършената електронна идентификация през приложението за идентификация
самоличността на физическите лица, които заявяват ползване на предоставяните от тези л
електронни услуги. Това препятства изпълнението на чл. 5, ал. 2 от същия закон. В тази вр
спецификацията да се допълни с изисквания за разработване на протоколи за комуникаци
системите на лицата по чл. 1, ал. 2 от ЗЕУ.Съгласно Регламент (ЕС) 910/2014 нивата на оси
националните схеми за електронна идентификация следва да отговарят на изискванията н
с тези изисквания се удостоверява с одит от орган за оценка на съответствието. В техниче
е предвидено одитиране на процеса. В тази връзка, предлагам МЕУ да обмисли възможност
спецификация да се предвидят и задължения на разработчика за участие в посочения про
на действащия Закон за електронната идентификация да се предвиди възможност за извъ
по потвърждаването на самоличността на лицата чрез физическо присъствие да се извърш
които отговарят на определени условия.

Достъпност за хора с увреждванияЕлектронния подпис е особено важен за хората с увреждa
те могат да бъдат значително улеснени в комуникацията и упражняването на своите права
хората със зрителни увреждания, тъй като съществуват дори и законови изисквания, които
упражняването на тези права (например чл. 189, ал. 2 от ГПК, който изисква сляп, но грамо
подписва саморъчно, но за да е признат от съда като частен, документът трябва да е приг
от двама свидетели). С оглед на това, за да няма риск от дискриминация, следва при опред
разработващи софтуер за електронни подписи, да спазват изискванията за достъпност как
мобилните приложения, така и на уеб услугите. При задаване на техническите изисквания,
процедури, следва изрично да се изисква електронните услуги, свързани с електронния по
хора с увреждания, и по-специално, за хора със зрителни увреждания. Като универсален ст
посочи WCAG 2.1, който е възприет от ЕС като стандарт, с който трябва да са съобразени п
предлаганите от тях мобилни услуги, включително и препоръките на w3c за Accessible Rich
(WAI-ARIA). В заключение, моля да имате в предвид, че при съставянето на Техническата сп
изграждане на мобилно приложение за електронна идентификация и електронно подписва
включите и изисквания за достъпност за хора с увреждания (вкл. зрителни) на крайния про

Коментари и предложения, част 2Авторски права срещу софтуер с отворен код – в някои сл
полезно да се активират вече съществуващи продукти, включително защитени с авторски
патентовани продукти. Използването на доказани и сертифицирани критично важни компо
за осигуряване на постоянна сигурност и създаване на доверие и увереност в системата. Т
рентабилен и по-малко отнемащ време подход в случаи на компоненти, които са жизненова
услуга с eIDAS съвместимост. Това се отнася особено за компоненти като QSCD и някои от р
приобщаване, които са от решаващо значение за определяне на нивото на сигурност на ця
конкретно се отнася до: Софтуер за заснемане на документи Софтуер за биометрично данн
засичане на жив човек). Създаване на QESРешението трябва също така да гарантира съотв
международни стандарти: ICAO 9303: Машинно четими пътни документи NIST FRVT: Биомет
разпознаване ISO/IEC 30107 - 3: Биометрично разпознаване на атака ISO/IEC 19795 - 1:2006:
биометрична проверка eIDAS EN 319 - 401: Квалифицирани подписиПозоваване на регламен
единна цифрова платформа – това трябва да бъде изключено от търга, тъй като е извън об
идентичност. Добре е да се работи по този въпрос отделно и да не се комбинира с проекта
идентичност.Не е ясно дали и как ще бъде закупен необходимия хардуер. Или дали участн
предостави също така и хардуера. Това се отнася за хардуер като HSM-s(Hardware Security
някои от компонентите на цялата система за цифрова идентичност и при конкретни софту
има нужда и от специфичен хардуер.Изискването на специфични видове поддръжка за удо
подписване (като SAML) или всякакви други специфични технически решения, които имат н
опции, може да изключи някои от другите технологии за цифрова идентичност от търга. Пр
вид изисквания да бъдат по-общи и да не се отнасят за специфични неща като SAML, или п
повторя добавям и следните предложения:Системата трябва да включва технологии, обезп
регистрация и последваща проверка, посредством реален ("жив") човек в реално време, по
устройства и среди.Системата трябва да осигурява текущо и специално управление на зап
поддържа националните програми за идентичност и високорискови транзакции, което пред
развиващия се пейзаж на заплахите (включително дълбоки фалшификати, атаки с инжекц
трябва да използва сертифицирани по eIDAS компоненти (сертифицирани за високо ниво на
използвани в сертифицирани от ЕС eIDAS внедрявания на живо.Системата трябва да се при
управление на сигурността и производителността, включително биометрична производите
тестване на платформата и сертифициране

Коментари и предложенияИзискванията и проектът като цяло трябва да бъдат оперативно 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, з българските граждани могат да използват приложението за достъп до отговарящи на усло други държави-членки. От решаващо значение е да се гарантира, че България може да раб пазар на ЕС, така че гарантирането на оперативна съвместимост и текущото съответствие стандарти от началото на този проект е от решаващо значение. Опитът за модернизиране съвместимост след създаването на приложението няма да работи.С оглед на раздел 1 от д споменава одит и сертифициране. Тъй като целта е закупуване на съвместими с eIDAS реш услугата трябва да бъде включен в търга и в планирането на сроковете. Не е реалистично да се извършат в рамките на 9 месеца, както се изисква в документите. Ако съответствиет трябва да бъде включенн и одит. Реалистичен срок за извършване на одит за съответствие повечето от компонентите на услугата ще се разработват специфично само за България, м удължаване на този период. Това е особено важно, ако в България в рамките на този проек устройство за създаване на квалифициран подпис (QSCD).Не се споменава CA(Certificate Au Това е жизненоважен компонент на всяка система за цифрова идентичност и в тръжните д да се споменава за CA, в случай че CA е извън обхвата на тази оферта.Изискванията за разр прекалено подробни. Такива изисквания биха били добре, ако целта е закупуване на ресур ако целта е да се закупи крайният резултат, тогава трябва да има повече гъвкавост в проц разработка.Изискванията в раздел 7 са твърде подробни и в същото време някои от важни този раздел. Препоръчително е вместо такива подробни изисквания да има препратка към добри практики или подобни.По-подробни SLA изисквания трябва да бъдат включени в тръ Ако участникът знае броя на потребителите, той може да прецени по-точно цената и възмо система. Следователно изискванията на SLA, включително броя на потребителите, необход и т.н., трябва да бъдат включени в офертата.Поддръжката и техническото обслужване тря като изискване в документацията на възложителя. Понастоящем гаранционните изисквани необходимостта от поддръжка и обслужване, отколкото за действителните гаранционни сл може да има отделни точки за поддръжка и техническо обслужване.

към документациятаВъв връзка с обявено преразглеждането на Регламент (ЕС) № 910/201
парламент и на Съвета чрез съобщението на Комисията от 19 февруари 2020 г., озаглавено
цифровото бъдеще на Европа“, с цел да се подобри неговата ефективност, да се даде възм
сектор да се възползва от него и да се насърчи използването на надеждна цифрова самоли
европейци, както и с че в проекта за Изграждане на мобилно приложение за електронна ид
електронно подписване – BGID, е заложено съответствие с известните изисквания към евр
портфейл , с настоящето предлагаме промени, които в по-голяма степен да гарантират, че
ще получат, решение отговарящо на най-съвременните изисквания за цифрова самоличнос
ще може да контролира количеството данни, предоставяни на доверяващите се страни, и ц
атрибутите, необходими за предоставянето на конкретна услуга. 1. В точка:1.2.Технологич
добавиТерминОписаниеЕвропейски портфейл за цифрова самоличностЛични цифрови порт
позволяват на гражданите да се идентифицират по цифров път и да съхраняват и управля
самоличност и официални документи в електронен формат. Тези документи може да включ
управление на МПС, медицински рецепти или дипломи. С помощта на портфейла граждани
доказват самоличността си, когато това е необходимо, за да получат достъп до услуги онла
цифрови документи или просто да докажат конкретна лична характеристика, например въ
своята самоличност или други лични данни. Във всеки един момент гражданите ще имат п
данните, които споделят. 2. В точка:2.3.За проектаНастоящият проект обхваща дейности п
приложение за мобилна електронна идентификация и подписване BGID, като целите на пр
въвеждане на използването на идентификация на потребителите посредством национален
идентификатор. Да се промени, както следва:2.3.За проекта Настоящият проект обхваща д
на приложение за портфейл за цифрова самоличност за мобилна електронна идентификац
като целите на проекта са реализират въвеждане на използването на идентификация на п
посредством национален електронен идентификатор. 3. В точка:2.4.Нормативна рамкаПро
съответствие с изискванията, регламентирани със следните нормативни актове и стратеги
се добави в:Международни стандарти:ISO/IEC 18013-5:2021 - Personal identification — ISO-com
Part 5: Mobile driving licence (mDL) application 4. В точка:3.4.Очаквани резултатиОчакваните р
изпълнението са:Изградени мобилни приложения за електронна идентификация и подписв
системи с високо ниво на използване от граждани и бизнес за използване на мобилна иден
подписванеПовишаване на използването на вече съществуващи електронни администрати
за готовност за покриване на изискванията на предложението за изменение на Регламент (
европейски дигитален портфейл, след влизането му в сила Последния параграф да се пром
следва:Високо ниво за готовност за покриване на изискванията на предложението за измен
910/2014 за т.нар. европейски дигитален портфейл, след влизането му в сила. В този случа
приложение за електронна идентификация и електронно подписване – BGID трябва да се р
BGID за портфейл за цифрова самоличност.

към документациятаВъв връзка с обявено преразглеждането на Регламент (ЕС) № 910/201 парламент и на Съвета чрез съобщението на Комисията от 19 февруари 2020 г., озаглавено цифровото бъдеще на Европа“, с цел да се подобри неговата ефективност, да се даде възм сектор да се възползва от него и да се насърчи използването на надеждна цифрова самоли европейци, както и с че в проекта за Изграждане на мобилно приложение за електронна ид електронно подписване – BGID, е заложено съответствие с известните изисквания към евр портфейл , с настоящето предлагаме промени, които в по-голяма степен да гарантират, че ще получат, решение отговарящо на най-съвременните изисквания за цифрова самоличнос ще може да контролира количеството данни, предоставяни на доверяващите се страни, и ц атрибутите, необходими за предоставянето на конкретна услуга. 1. В точка:1.2.Технологич добавиТерминОписаниеЕвропейски портфейл за цифрова самоличностЛични цифрови порт позволяват на гражданите да се идентифицират по цифров път и да съхраняват и управля самоличност и официални документи в електронен формат. Тези документи може да включ управление на МПС, медицински рецепти или дипломи. С помощта на портфейла граждани доказват самоличността си, когато това е необходимо, за да получат достъп до услуги онла цифрови документи или просто да докажат конкретна лична характеристика, например въ своята самоличност или други лични данни. Във всеки един момент гражданите ще имат п данните, които споделят. 2. В точка:2.3.За проектаНастоящият проект обхваща дейности п приложение за мобилна електронна идентификация и подписване BGID, като целите на про въвеждане на използването на идентификация на потребителите посредством национален идентификатор. Да се промени, както следва:2.3.За проекта Настоящият проект обхваща д на приложение за портфейл за цифрова самоличност за мобилна електронна идентификац като целите на проекта са реализират въвеждане на използването на идентификация на п посредством национален електронен идентификатор. 3. В точка:2.4.Нормативна рамкаПро съответствие с изискванията, регламентирани със следните нормативни актове и стратеги се добави в:Международни стандарти:ISO/IEC 18013-5:2021 - Personal identification — ISO-com Part 5: Mobile driving licence (mDL) application 4. В точка:3.4.Очаквани резултатиОчакваните р изпълнението са:Изградени мобилни приложения за електронна идентификация и подписв системи с високо ниво на използване от граждани и бизнес за използване на мобилна иден подписванеПовишаване на използването на вече съществуващи електронни администрати за готовност за покриване на изискванията на предложението за изменение на Регламент (европейски дигитален портфейл, след влизането му в сила Последния параграф да се пром следва:Високо ниво за готовност за покриване на изискванията на предложението за измен 910/2014 за т.нар. европейски дигитален портфейл, след влизането му в сила. В този случа приложение за електронна идентификация и електронно подписване – BGID трябва да се р BGID за портфейл за цифрова самоличност.
Обща препоръка - само малко допълнениеЧастни схеми за е-ИД поддържат двата ДКЕУУ - Евротръст.
Обща препоръка - само малко допълнениеЧастни схеми за е-ИД поддържат двата ДКЕУУ - Евротръст.
Обща препоръка - само малко допълнениеЧастни схеми за е-ИД поддържат двата ДКЕУУ - Евротръст.

Обща препоръкаДнес е Националия ни празник ... На всички „ЧЕСТИТО“ ... А сега кратък ко
Техническа спецификация за BGID !Забележете, Спецификацията е за мобилно приложение
е-подпис, т.е. за нещо, което „виси ей-така свободно“, а не в обхвата на изпълнение на наш
СХЕМА ЗА е-ИД и е-подпис (било то усъвършенстван или квалифициран). Та нали имаме Зако
иденти.фикация (ЗЕИ), който е приет и „втасва“ от няколко години... . Само е споменато, че
следва да се осъществи в съответствие със съответстващите и известни нормативни актов
(включително и ЗЕИ). И понеже е за е-ИД, най-вече трябва да съответства на ЗЕИ. А това е
приложението се „потопи“ (т.е.работи) в установена и изградена национална ТЕХНИЧЕСКА
идентификация с нейните субекти-участници в схемата (Орган на е-ИД – МВР, съответни Ад
ДКЕУУ), Център/по-скоро Центрове за валидация и техните ИТ-системи и Регистри, и най на
ползват приложението). Така, че мобилното приложение е последната „брънка“ на СХЕМАТ
добре е в Техническата спецификация да има отделен раздел, определящ една ВАЛИДНА н
еИД (ако има/е взето конкретно решение), така че бъдещата ОП за мобилното BGID да адре
повече, че към настоящия момент вече има имплементирани и успешно се ползват техниче
на мобилни приложения за издаване, регистрация, валидация и поддръжка на е-ИД и на мо
физически лица и такива, представляващи юридически лица. Това са частни схеми за еИД,
бързо и лесно могат да се изградат до национален обхват (в предвид много краткия перио
BGID) и впоследствие да се нотифицират като национални-частни такива. Примери за такъ
Европейския съюз има много ...Ако има такъв раздел в предлаганата Техническа специфик
адресира много точно поченциални и успешни участници в реализацията на BGID.А и още н
да се забравя – промените в Регламент 910/2014 на ЕС за удостоверителните услуги (и спец
идентификацията). Като следствие – това е European digital identity Wallet (както мобилен, т
който ще адресира както националната така и през-граничната е-идентификация заедно с
валидирани е-атестати/атрибути за лицата. Б. Баев

Коментари по спецификацията (продължение)А как биха реагирали от ЕК/ЕС, ако бъдат ре
системи и се окажем с два различни root CA, които претендират да издават валидна електр
не на последно място, използването на УЕИ като подпис не е уредено нито в закона за елек
нито в правилника за прилагането му. В тази връзка според мен е редно първо да се напра
а не първо да се напише софтуера и след това фирмата, която го прави, да предложи и съо
промени, както е и написано в текущата спецификация. Това не би било проблем за електр
като част от проекта „поколение 2019“, тъй като е предвидено системите трябва да се ада
законодателството. Румен Николов

Коментари по спецификациятаИдеята за електронна идентификация чрез телефон не е ло
Описаната в този проект, според мен обаче, има доста проблеми и дава повече въпроси, от
с валидност до 3 години и не би следвало да се използва до края на изтичането на валидно
описано в т. 4 от текущата спецификация – „до 1 година след влизане в продукционен реж
схема по ЗЕИ“.Доколкото става ясно т. 4 от текущата документация, КЕП, ПИК на НАП/НОИ,
в момента се използват за достъп до електронни административни услуги само в България
САМО да осигури възможност за ползване на трансгранични електронни услуги в рамките н
средства обаче българските граждани не могат да се идентифицират, когато заявяват еле
административни услуги в други държави-членки на Европейския съюз, което препятства в
ползване на трансгранични електронни услуги в рамките на ЕС.“Кое налага необходимостт
на трансгранични електронни услуги в рамките на ЕС в момента? В техническата специфик
споменават САМО електронни административни услуги в България! А за тези услуги и в мо
електронна идентификация!В тази връзка – ако ще бъде правена реализация на проекта в
необходимо да бъде добавен и регистър/списък на наличните трансгранични електронни у
от които ще могат да се възползват българските граждани.Не мисля, че желаещите да изп
електронни услуги в рамките на ЕС, каквато е и целта на този проект, са толкова много, че
допълнителен проект за електронна идентификация.Използването на смартфон/таблет или
възможно съгласно техническата спецификация в Приложение 8 от обществената поръчка
„Проектиране, изграждане и управление на Система за издаване на български лични докум
УЕИ може да бъде записан на устройствата след като се регистрират от съответен Админи
за управление на носители (ПУН). Но генерирането на електронния идентификатор, както и
и процеси свързани с издаване на УЕИ, ще са изградени и няма нужда да бъдат дублирани.
предложената схема за електронна идентификация ще дублира над 90% функционалности
описани в Техническата спецификация Приложение 8: „Изграждане на централизирана сис
идентификация“, която е част от обществената поръчка за документи „поколение 2019“, а
определен изпълнител.Текущата система за персонализация на български лични документ
на 2010 г. Техниката е на над 12 години, като на станциите за снемане на биометрични дан
Windows XP, която отдавна не се поддържа от Майкрософт. Стартирането на производство
„поколение 2019“ е предвидено за около 2 години след подписване на договора. Това значи
осигурена поддръжка на техниката към текущата система, която започва 13та година от а
за още минимум 2 години. Спирането или промяната на поръчката за документи „поколени
2 години, които ще трябва да бъдат добавени към поддръжка на текущата система за изда
документи. Колко човека имат работещ принтер на над 15 години?Заслужава ли си да се с
обществена поръчка за дейност, която всъщност до голямата си степен е част от вече стар
поръчка, на която има и определен изпълнител?В момента идентификацията на граждани
електронните услуги на администрацията работи. Аз лично имам и ПИК на НАП, на НОИ и К
съществуващите електронни услуги. Не мисля обаче, че е необходимо дублирането на реал
националната схема за електронна идентификация и това дублиране да се оправдава само
трансгранични електронни услуги в рамките на ЕС. Условията за сигурна и надеждна елект
на гражданите при предоставяне на електронни административни услуги са заложени като
поръчка за лични документи „поколение 2019“.Не е редно за едно и също нещо да се разхо
обществен ресурс. Освен системите за издаване и регистрация на УЕИ ще бъде дублирана
(HSM устройства, сървъри …), които са и в другия проект.

Някои препоръки по спецификациятаПоздравявам колегите за публичното представяне на
няколко мисли по представения текст:1. Документът би спечели, ако се знае, кой е авторъ
страна ще сме сигурни, че авторът няма да е свързан с бъдещия изпълнител. От друга стра
бъде написано в крайния вариант, ще има по-голяма тежест и отговорност.2. Спецификаци
обществена поръчка да се избере изпълнител, на който да се възложи отговорната задача
модел за създаване, разпределение и използване на криптографски ключове за целите на
електронната идентификация и подписване. Това трябва да се извърши в Дейност 1.Ако Въ
резултата на Дейност 1, наречен “Системен проект”, Изпълнителят ще продължи с разрабо
необходимия софтуер.Проблемите, които виждаме в това направение, са следните:Разчита
изгради национален модел, който Възложителят да одобри. Но какво ще се случи, ако моде
„читав“ и не трябва да бъде одобряван, но има договор, в който софтуерът трябва да бъде
или есента. Не е ли по-добре администрацията, в лицето на специалистите, създали Архите
електронното управление, да поемат отговорността и да публикуват за обсъждане този мо
идентификация не е „от вчера“. Мобилната също: https://www2.e-gov.bg/bg/events/54Едва ли
проект ще започне от кота“0“ („to start from SCRATCH“). Не е ли по-добре да се посочат, кои
модули, от вече публикувани проекти, намиращи се в наличните хранилища за проекти от
бъдат използвани.Внушението ми е, че е време специалистите, създаващи спецификации з
код, да спрат да планират финансирането на едни и същи дейности (едни и същи по функ
Очевидната ни цел е да има многократно използване на вече разработения с държавни сре
да се спести време и да се намали реалната цена на създавания продукт, в интерес на общ
стр. 22 на спецификацията е казано: „Да се изследва възможността резултатният продукт
изгради частично (библиотеки, пакети, модули) или изцяло на базата на съществуващи соф
са софтуер с отворен код“, но се планира това да стане, след като е спечелена ОП и е склю
разработване на всички модули. Някак си не ми се вярва, че някой Изпълнител ще върне 60
финансирането на Възложителя, защото в хода на изпълнение на проекта е решил да изпо
библиотеки.В заключение бих препоръчал:Авторите на спецификацията да публикуват мод
се изгради системния проект за обсъждане.Авторите на спецификацията да посочат библи
да бъдат използвани от бъдещия изпълнител.Бих препоръчал самият проект да бъде разде
независими SOA `модули, които да бъдат реализирани паралелно от различни изпълнители
зорък поглед на българското ИТ общество.Тъй като Възложителят, в лицето на МЕУ, не пла
се усвояват големи средства(искрено се надяваме, че е така), възлагайки задачата по създ
модули на отделни лица или малки колективи ще се избегнат проблемите, свързани с голе
поръчки. Нещо повече ще се избегне налагането на монопол на едни или други фирми, кое
новия подход.

тестов коментар 2 администратор<p>до:</p><p> </p><p&gt
министър</p><p>МИНИСТЕРСТВО НА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ</p><p&g
София</p><p> </p><p>П О З И Ц И
Я</p><p> </p><p>от:</p><p> </p>&lt
председател</p><p>БРАНШОВ СИНДИКАТ „ИНФОРМАЦИОННИ ТЕХНОЛ
НФТИНИ при КТ „Подкрепа“ гр. София, ул. Ангел Кънчев
№2</p><p> </p><p>относно:</p><p> </p
спецификация за изграждане на мобилно приложение за електронна идентификация и еле
– BGID</p><p> </p><p>Уважаеми Г-дин
МИНИСТЪР,</p><p> </p><p>Като национално представителна
на работещите в областта на информационните технологии, от наше име и от името на наш
членове приветстваме новосформираното Министерство на електронното управление (МЕУ
после да бъде започнат сериозен разговор относно българското Електронно управление &a
разговор не може да не засегне още в самото си начало въпроса за електронната идентиф
– за електронното подписване). Без предварително разрешаване на този въпрос
електронна среда е обречен или на липсата на гаранции за автентичност (и от там &n
юридическа значимост); или на частични решения „на парче“, които
Електронното управление разпокъсано, скъпо и неефективно.</p><p>
3.1. „Общи и специфични цели“ от проекта на Спецификацията е пос
„проектът е насочен към изграждане на удобно и достъпно средство за електро
потребителите на електронни административни услуги, както и за електронно подписване
електронни административни услуги чрез мобилни устройства“. По-детайлно се
на проекта, където от Дейност 3. „Разработване на мобилно приложение за пот
iOS“; и от Дейност 4. „Разработване на служебно мобилно приложени
iOS“ научаваме, че се предвижда разработването на мобилни приложения (респ
мобилни приложения) „за най-популярните операционни системи, като миниму
12“.</p><p> </p><p>възражение: Защо само &amp
устройства“?</p><p> </p><p>Безспорно, включван
устройства (преди всичко „умни“ телефони и отчасти – ра
фаблети и т.н., осигуряващи GSM-свързаност), е стъпка в правилната посока – з
използват такива устройства и практическите последици от включването им като възможн
идентификация и електронно подписване са
обнадеждаващи.</p><p> </p><p>Същевременно обаче много
подобни устройства, но ползват напр. стационарни или преносими компютри, които не са м
поддържат GSM-свързаност). Предимство при тях е, че настройването на операционната ср
приспособяването на системата към личните (а понякога и специфично професионални) ну
в сравнение с типичните мобилни устройства; поради което често сред потенциално най-ма
електронни идентификационни и подписни услуги (счетоводители, одитори, адвокати, нота
стационарните и преносимите компютри са предпочитани. За разлика от тях, мобилните ус
случаи не се поддават на специфични настройки и не позволяват тяхното защитаване извъ
мерки за сигурност – което поставя под въпрос надеждността им. Поставянето
като единствена възможност за достъп до електронни административни услуги ограничава
работа в операционна среда, позволяваща приспособяване към личните (и професионалнит
ползвателите. Не на последно място – съществуват отдалечени и слабо развити
покритието е несигурно и това би направило услугите
недостъпни.</p><p> </p><p>> Считаме, че системите
идентификация и електронно подписване на българското Електронно управление трябва о
могат да работят на всякакви други устройства (освен мобилните), които осигуряват interne
свързаност. В случай, че се настоява за включването на мобилния телефон като условие за

тестов коментар 1 администратор тестов коментар 1 администратор
Одит на приложението от международна компания по сигурносттаВъпросната система ще точка на достъп до държавната администрация.Това я превръща в "single point of failure".От необходимо при избора на проект да се направи анализ на неговата сигурност.Това, според всички коментари.Затова смятам за уместно, да се привлече трета страна от сферата на ки допълнителен одит при избора на изпълнител и оценка на неговата работа.
8.2.8 Процес на подписванеПредаването само на хеш и описание при подписване, може да потребителя, без да подозоира, да подпише различен документ. Няма възможност такова бъде оспорено, тъй като потребителя никога не е имал достъп до документа - обект на под провери неговата хеш стойност.Странта, която изчизлява хеша трябва да има доверието на това условие е трудно да бъде постигнато, трябва да има възможност документа да бъде п хеш да бъде изчислен на самото мобилно устройство. След сравнение на предоставения и продължи с процеса на подписване.Може да се специфицира списък от поддържани форма подписване, които да могат да бъдат преглеждани на мобилни устройства. Алтернативно, трябва да бъде част от процедурата по подписване, с локално изчисляване на хеш и включ електронния подпис. Тази мярка би увеличила увереността у потребителя, че подписва тов
Информационно обслужване АД - изпълнителя на тази спецификацияПредлагам да се пров процедура по ЗОП и да има реално състезание за избор на изпълнител. Злите езици говоря вече известен и работи по реализацията и това е Информационно обслужване АД. Ако е так времето и говорите за прозрачност и равен старт на бизнеса в България. То и преди ИО АД да има промяна. То в случай не промя, то и замяна или подмяна НЯМА.Предлагам да се гара Информационно обслужване АД няма да е предизвестения изпълнител на тази поръчка.

Малко за начина на разработка1. Agile нали това е техническа грешка. Моля се да е така. Н
правенето на сайт със сериозен проект, който ще гарантира идентификацията на лицата п
повече, че този подход противоречи на етапите в т.6 и дейностите в т. 8. Кое ще правите с
или разработката по следващата дейност. предлагам да се преразгледа изискваната метод
да се заложи класическа.2. Документация - нищо по темата или то щото ИО АД ще го прави
документация. И недейте се кри зад т.9.2 Системен проект. Толкова жалко са описани изис
повече не може и да бъде. МТИТС и ДАЕУ залагаха на точен опис на изискваните документи
разработката и не знам кой го разпозна като лоша практика. Предлагам да се опишат в дет
документация по проекта, включително конвенция за писане на код, за да няма после - Ние
само ИО АД може да си го чете.3. Българите в чужбина пак сте ни забравили - или пак изва
(ама български, защото сме родолюбци). Стига! Само не отхвърляйте бележката с .... то па
чужденците - на първо място гражданите на държавите-членки на ЕС - няма ги и това е ди
само за българи и електронните услуги са само за тях. Придлагам да се включат ясни изис
спецификацията за възможност за идентификация за всички групи граждани. Да не забрав
гражданство.4. По изискванията за гаранционна поддръжка и наличност на системата - На
минете с тези изисквания - размити и на практика винаги оправдаващи изпълнителя ИО АД
въведат изисквания за 365/24/7 подръжка, ясен SLA - например присумарно един час нера
годишна база - глоба от 20 % от стойността на проекта, време за реакция половин час, вре
инцидент или решение възстановяващо работоспособността 1 час, изисквания за архитект
пълна функционална резервираност на решението. Много слаба първа спецификация, г-н Е
я бързали и правили на коляно. Дано актуализирания вариант също мине обществено обсъ
много важен и си заслужава внимание.

Използването на телефононер номерПривет,Предложението ми е да отпаднат изцяло изис
събиране/съхраняване/използване на телефонен номер: "При регистрация, гражданите тря
мобилен телефон и имейл адрес."и тук:"В сървърната част на системата трябва да се съхра
информация (имейл и телефон)"и тук: "Управление на устройствата...Всяко устройство (сле
бъде валидирано с еднократенлинк, изпратен на имейл и/или телефон (като SMS). --- Към м
аветентикация чрез мобилната мрежа (СМС или обаждане) обикновено е най-слабото звено
примери за това са всевъзможните SIM swapping атаки, включително и чрез съдействието н
служители в мобилните оператори. Отделно от това, в глобален свят и с милиони българи з
ЕС), много от които не поддържат български номер, използването на телефонен номер е не
Известията към потребителите могат да са изцяло чрез приложението и/или чрез имейл. От
(оторизация) на допълнително устройство: вместо СМС, валидирането може да се осъщест
всички вече регистрирани устройства за одобрение или отказ на новото устройство, и/или с
имейл. С две думи, не виждам нито една добра причина да се съхранява и използва телефо
средство и няколко причини да не се използва. Поздрави за добре свършената работа до т

липса на физическа възможност за пропътуване на разстояние спрямо геокоординатите на
добър feature, но пък от гледна точка на "surveilance" е малко ограничаващо. и не, аргумен
кирете?" не е валиден. Нека има информация за потербителя, и възможност той да поиска
но не и системата да го блокира автоматично.

физическа идентификацияосъзнавам че това не е целта за момента, но би било много удоб
функционалност за идентификация и пред физически лица в самото приложение. Т.е. да м
информацията нужна за удостоверение + QR код за проверка на тази информация.осъзнав
на законовата рамка, но мисля че тук му е мястото на един такъв feature.

КоментарСпецификацията е твърде техническа, не е продуктова.-Приложението трябва да
концепция с реални хора. Дали пенсионери или ниско образовани граждани биха могли да
ползват приложението сами или ще бъдат дискриминирани?-Изплозването на геолокация и
изричното разрешение от потребителя, което отново може да доведе до фал старт.-Чужде
се възползват от това приложение ако нямат български документи на самоличност?- Apple
приложения които използват геолокация или лични данни. Има ли план при такава ситуаци
гаранционните условия?

ДискриминационноПредложениеПредложението е дискриминационно и дефакто изисква г
използват не просто точно определени операционни системи, но и то с минимално изискван
причина държавата да спомага допълнително за монопола на Apple/Google в тази посока. И
хората - достъпно за всеки един гражданин, или изобщо не го правите.

Локация и биометрични данниЗдравейте, поздравления за ясно и точно написаното задани
и тартори на определени групи имат незаконната практика да събират лични карти и банк
и ги ползват от тяхно име. Това задължително трябва да избегнем при електронната идент
се разрешава повече от едно активно устройство. Идентификация само с биометрични дан
разпознаване или пръстов отпечатък без възможност за замяната им с PIN на телефона. На
това е възможно с конфигурация. Това гарантира физическото присъствие на човека поне
технологии го позволят. Проблем е, че пръстовите отпечатъци могат да се конфигурират в
телефона и е възможно да се въведат и на друг човек, т.е. може да се злоупотреби. Лицево
може да се конфигурира за друг човек и това са проблеми, за които предполагам бихме мо
решение. Но поне могат да се случат само със съдействието на собственика. Приложението
когато GPS приемникът има fix с добра точност, за да може да се проследи локацията при з

Предложения за сигурност и поддръжкаЗдравейте,Призовавам за поддръжка на комплексн
и поддръжка на MFA приложения и ключове като : Yubikey / YubicoИмаики предвид че потре
разнородни устройства и версии на OS в разработката и тестването на мобилните приложе
заложи поддръжка на повече версии и OEM специфично за Android. Android 7 - 12 включите
между stock Android & OEM версиите и т.н.Също така призовавам за разработване на Native
сигурността може да се обезпечи по-лесно спрямо Cordova, Xamarin и други multi-platform т
бъдеще ще бъде по-лесно надграждането на приложенията, обновления и адаптация към н
OS. https://developer.android.com/topic/security/best-practices#java

Тестване и ОСЗдравейте, Освен направените вече коментари, според мен трябва да бъдат
записани няколко малки детайла: 1. т.8.3.1 и т.8.4.1 - Мобилно приложение разработено за
Android и iOS, работещо на смартфони, с минимална версия на оперционната система, както
поддържащи Android OS - v.9.0;За смартфони поддържащи iOS - v.12.0;Според закона "Моби
приложение работещо на мобилни у-ва - "като смартфон или таблет". Следователно се полу
като Android OS се поддържа, както на таблет, така и на смартфон, докато от Apple решиха
името на операционната с-ма на техните таблети на iPadOS. Ясно е, че iPadOS, стъпва изцял
уточнение ще внесе яснота дали приложението ще бъде разработено само за смартфони и
така и за таблети. В случай, че е за двата типа устройства , то тогава със сигурност scope-ъ
и с малко. 2. т. 6.4 - частта "..., за да се демонстрира", според мен, трябва да бъде заменен
валидирано". "Валидацията" означава много повече в софтуерната разработка, а именно, ч
тестване, чрез различни техники, което всъщност ще демонстрира правилното изпълнение
definition - "validation:Confirmation by examination and through provision of objective evidence th
specific intended use or application have been fulfilled."

КоментарПо отношение на 7.2.3: Бих добавил и "Pilot" логическа среда. Нейното място е ме
Production. Pilot е среда, максимално близка до реалната, където се извършва тестване на Р
на софтуера с натоварване максимално близко до реалността. По отношение на 7.2.5: Систе
бекъп на данните следва да бъде организирана по два параметър: географски и локален. П
сигурност на съхранението на данните и застраховка (защита) от непредвидени ситуации -
земетресение,... Локален е за скорост на възстановяване.

КоментарииHSM са споментаи май само на едно място. Мисля че трябва да бъде казано изри
съхраняване на ключовете на сървера. има на много места в текста "или" (напр. или PIN ил
се опитвате да направите заданието възможно най-отворено за различни технологии, но на
печелившия участник ще избере пътя на на най-малкото съпротивление и ще направи само
което ще е пак стъпка в правилната посока, но ми се иска да се поддържат повече възмож
начало.говорейки за възможности, мисля че е добра идея в такъв проект да бъде заложена
поддръжка по зададени параметри за да може системата да бъде доразвивана бързо при в
изисквания на базата да този спечелен договор. Нека тази поддръжка да бъде период от п
някакви рамки, но да я има и да не се чуди министерството как да си поиска някоя бърза д
трябва да пуска нова обществена поръчка.Иначе посоката на документа е правилната и до
остане е огромна крачка напред!

Първоначална регистрация.Здравейте, Поздравления за проекта, само лек коментар относ
регистрация, гражданите трябва да посочат и мобилен телефон и имейл адрес."Не смятам
изисква телефонен номер за завършване на регистрация. Често има граждани които имат у
активен номер, било то по тяхно желание или не. Ако все пак се иска телефонен номер нек
получаване на определени уведомления. Тъй като приложението може да доставя нотифик
него. И да може да се избира предпочитан метод за връзка. Ако има няколко, email, телефо
нотфикации.Другото на което смятам, че може да се обърне внимание е прехвърлянето на
се заложи метод с паспорт и с новите лични карти, с чип тъй като те ще съществуват, а ПИ
вероятно ще бъде закрит като система. За да може да има алтернатива на СМС и да не зав
услуги от достъп до телефонен номер.Благодаря Ви!

Предложение за функционалностЕлектронната идентификация, чрез мобилно устройство б
работи и без наличие на интернет, както и да се използа за идентификация на гражданин
устройство за достъп до интернет, а не мобилното устройство с инсталираното и активира
eID.Хипотетичен сценарий: Имаме активиран мобилен телефон с електронна идентификаци
интернет и WIFI. Имаме и наличен десктоп компютър с LAN достъп до интернет и липса на
Потребителя би трябвало, използвайки мобилното си устройство да може да се идентифиц
държава, използвайки стационарния компютър и неговия браузър.Възможност решение на
мобилното устройство (приложението за eID) да генерира еднократен токън или нещо дру
използва за идентификация на потребителя.

Бележки по документаРазгледах документа подробно: - Първото ми впечатление е че е дос
напълно сигурен дали всички детайли за технологии и изисквания имат приложение тъй ка
тях да нямат общо с реалното изпълнение а от друга стара следенето за спазването им ще
сериозно - и трябва да се очаква сериозна цена за вътрешен контрол от самия разработчик
минимум моята оценка е за 2-ма постоянно заети които да проверяват всеки детайл дали о
заданието. Нещо което липсва: - Хората си губят и сменят телефоните - и това се случва на
места - например на почивка в чужбина, командировка и т.н. - и не видях (може да съм про
изискване за лесно преместване на приложението от един телефон на друг или на нов тел
му за работа на този нов телефон/устройство. За технологиите : Те са от две части : 1. Иден
Подпис (Sign) 1. Идентификация - Машинно(вътрешно - уникално) ID - има си добре извест
се нарича UUID (GUID a windows потребителите) - всякакви други съчинения по темата мога
неприятни резултати (например ако се налага издаването му на разпределени места а не
технологии имат проблем с това) - Човешко ID (Human Readable) - стандартната практика е
идентификационен номер + фамилия (в нашия случай ЕГН и Фамилия) - Начини за първона
Съвременните са или с SMS/Vibre код или с токен (token/code) който се генерира на мобилн
подава ПИН(pass-code) 5 цифри набрани от потребителя и то използвайки този ПИН + врем
мобилното устройство е със синхронизиран таймер) - и резултата обикновено 8 цифри се п
втората част от two-factor идентификация - алгоритъма е добре познат - HMACSHA на RSA к
паднал и свободен за използване 2. Подписване - Използват се генерално три начина : I. ch
се код от сървъра (може да се сканира QR код или просто да се набере в телефона от екра
цифри и използвайки HMACSHA се получава отговор който се навира на страницата и се пр
записва - това е прост ясен и добър начин II. SMS/Vibre код който се праща и се записва в с
добър вариант но е достатъчно сигурен също III. Публичен/Частен ключ (в момента обикно
curve cryptography) като публичния стой в сървъра а частния в приложението - пак се откл
проблем с предаването до сървъра тъй като не малък по обем и не може да се напише про
ако услугата се достъпва от компютър а се оторизира от телефон) - има решение с fingerpri
накрая пак стигаме до необходимост от Интернет на мобилното устройство в момента на п
сериозен проблем в много ситуации.