Приложение № 1 към Решение № 515 от 19.05.2011 г. на КРС

ТАБЛИЦА С ПОСТЪПИЛИТЕ В КРС СТАНОВИЩА ПО ПРОЕКТ НА НАРЕДБА ЗА ИЗИСКВАНИЯТА КЪМ АЛГОРИТМИТЕ ЗА СЪЗДАВАНЕ И ПРОВЕРКА НА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС
(процедура открита с решение на КРС № 293 от 21.03.2011)

№	ДОСТАВЧИК	ЗАБЕЛЕЖКА	СТАТУС	МОТИВИ
1.	**СПЕКТЪР АД**	**По приложение към чл. 4, ал. 4 – Изисквания за използваните алгоритми за квалифицирани електронни подписи, т. 7 да придобие следната редакция:** „7. Приложимите комбинации на асиметрични и хеш-алгоритми спрямо сигурността на квалифицирания електронен подпис по времетраене са следните: **1.** Приложима комбинация „***sha1-with-rsa***" за 3 и 6 години да стане **2048**; **2.** Да се създаде нова колона със заглавие „10 години (и повече)", която да съдържа следната информация в клетките: • За *sha1-with-rsa*: **4096**; • За *sha256-with-rsa*, *RSASSA-PSS with mgf1SHA-1Identifier, RSASSA-PSS with mgf1SHA-224Identifier, RSASSA-PSS with mgf1SHA-256Identifier* : **2048**; • За *sha224-with-ecdsa*: **224**; • За *sha256-with-ecdsa*: **256**." **Мотиви:** Съгласно ETSI TS 102 176-1 V2.0.0(2007-11) е допустима употребата на комбинации от асиметрични и хеш-алгоритми спрямо сигурността на квалифицирания електронен подпис по времетраене на *sha1-with-rsa* както следва: • Устойчивост във времето от комбинацията за удостоверение за квалифициран електронен подпис на крайни клиенти до 3 години с 2048; • Устойчивост във времето от комбинацията за удостоверение за квалифициран електронен подпис на ДУУ за 10 години и нагоре с 4096; • Root CA Certificates, издавани съгласно предвиденият норматив с кратък период на валидност, са неприложими за целите на дейността на регистрираните ДУУ; Все още липсват работещи информационни приложения, които да сработват с *sha256*, както у нас, така и в европейски мащаб.	**Приема се частично**	КРС приема да бъдат отразени частично предложените промени. **1.** Комисията изразява съгласие с предложението да бъде въведена нова колона в таблицата, която да предвижда издаване на удостоверения със срок по-дълъг от 6 г. Същевременно КРС намира за неудачно предложението да бъде създадена колона със заглавие „10 години (и повече)", тъй като подобно правило на практика позволява издаване на удостоверения без ограничение във времето. В тази връзка, КРС счита, че следва да бъде създадено правило, съобразно което максимално допустимия срок за удостоверение следва да бъде 20 г. С посочената редакция се създава яснота в нормативната уредба и се взима предвид както практиката в РБ относно средна продължителност на срока на валидност на базовите удостоверения на ДУУ, така и практиката в останалите държави-членки. **2.** На следващо място, комисията счита, че следва в проекта да се укаже еднозначно, че приложимите комбинации със срок на валидност на удостоверенията от 6 до 20 г. са допустими само за базови и оперативни удостоверения. **3.** По отношение на употребата на sha1-with-rsa, комисията счита, че тя следва да се допуска само за удостоверения със срок на валидност не по-дълъг от 3 г., предвид необходимостта за

№	ДОСТАВЧИК	ЗАБЕЛЕЖКА	СТАТУС	МОТИВИ
				съобразяване с изискванията на ETSI TS 102 176-1 V2.0.0(2007-11) Комисията отчита необходимостта от достатъчно време за преминаване към някоя от другите комбинации и в тази връзка предлага разумен срок от 5 г. за миграция.
2.	**ИНФОРМАЦИОННО ОБСЛУЖВАНЕ АД**	**По приложение към чл. 4, ал. 4 – Изисквания за използваните алгоритми за квалифицирани електронни подписи, т. 7 да придобие следната редакция:** „7. Приложимите комбинации на асиметрични и хеш-алгоритми спрямо сигурността на квалифицирания електронен подпис по времетраене са следните: **1.** Приложима комбинация „***sha1-with-rsa***" за 3 и 6 години да стане **2048**; **2.** Да се създаде нова колона със заглавие „10 години (и повече)", която да съдържа следната информация в клетките: • За *sha1-with-rsa*: **4096**; • За *sha256-with-rsa*, *RSASSA-PSS with mgf1SHA-1Identifier, RSASSA-PSS with mgf1SHA-224Identifier, RSASSA-PSS with mgf1SHA-256Identifier* : **2048**; • За *sha224-with-ecdsa*: **224**; • За *sha256-with-ecdsa*: **256**." **Мотиви:** Съгласно ETSI TS 102 176-1 V2.0.0(2007-11) е допустима употребата на комбинации от асиметрични и хеш-алгоритми спрямо сигурността на квалифицирания електронен подпис по времетраене на *sha1-with-rsa* както следва: • Устойчивост във времето от комбинацията за удостоверение за квалифициран електронен подпис на крайни клиенти до 3 години с 2048; • Устойчивост във времето от комбинацията за удостоверение за квалифициран електронен подпис на ДУУ за 10 години и нагоре с 4096; • Базовите CA сертификати, издавани съгласно предвиденият норматив с кратък период на валидност, са без практическа приложимост за целите на дейността на регистрираните ДУУ; След направено проучване беше констатирано, че към днешна дата липсва еднозначна информация относно готовността на системите на доставчиците на електронни услуги да работят коректно с *sha25*6 и по-големи дължини на асиметричните алгоритми, както у нас, така и в европейски	**Приема се частично**	Съобразно посоченото по горе.

№	ДОСТАВЧИК	ЗАБЕЛЕЖКА	СТАТУС	МОТИВИ
		мащаб. Преиздаването на базовите сертификати на ДУУ ще доведе до необходимост от повторна регистрация за използване на електронните услуги за крайните клиенти, което ефективно ще затрудни достъпа да вече работещите и активно използвани електронни услуги на НАП, НОИ, АМ и др.		
3.	**БОРИКА – БАНКСЕРВИЗ АД**	**Да бъде допълнена таблицата към приложението към чл.4 ал.4:** „Изисквания за използваните алгоритми за квалифициран електронни подписи„ т.7 за приложимите комбинации на асиметрични и хеш-алгоритми спрямо сигурността на квалифицирания електронен подпис по времетраене, както следва: **1.** Приложима комбинация „***sha1-with-rsa”*** за 3 и 6 години да стане **2048**; **2**. Да се създаде нова колона със заглавие „10 години (и повече)”, която да съдържа следната информация в клетките: • За *sha1-with-rsa, sha256-with-rsa*, *RSASSA-PSS with mgf1SHA-1Identifier, RSASSA-PSS with mgf1SHA-224Identifier, RSASSA-PSS with mgf1SHA-256Identifier, sha1-with-dsa* : **4096**; • За *sha224-with-ecdsa*: **224**; • За *sha256-with-ecdsa*: **256**.” **3.** За *sha1-with-dsa* за 3 и 6 години стойността да бъде: **2048.** **Мотиви:** В настоящия момент българските доставчици на удостоверителни услуги (ДУУ), както и европейските такива, използват основно приложима комбинация на асиметрични и хеш-алгоритми: **sha1-with-rsa.** Издадените и използваните базови и оперативни удостоверения на доставчиците се базират в повечето случаи на дължина на ключовете „4096” бита, издадени с период на валидност 10 и повече години. Ако тези данни не се допълнят в описаната по-горе таблица ще се наложи преиздаване на всички удостоверения на сега регистрираните ДУУ, както и на всички техни клиенти. По аналог на включването на колоната „10 и повече години”, моля да се допълнят липсващите стойности преди колоната „10 години”, тъй като след като се предполага, че алгоритъма SHA1 ще се ползва за по-голям период, той трябва бъде регламентиран и за останалите такива. В допълнение трябва да се посочи, че за сега и в близко бъдеще SHA1 остава единственият практически използван хеш-алгоритъм в приложенията за електронно подписване на документи. В голямата си част използваните приложенията отказват да работят с SHA256 и самата миграция към него ще се наложи да се отложи във времето.	**Приема се частично**	На първо място, относими към бележката са мотивите на комисията, посочени по т. 1 от настоящата таблица. На второ място, КРС не приема предложението за допълване на таблицата в частта „*sha1-with-dsa* за 3 и 6 години”. Доставчикът не е посочил мотиви, които да обосноват исканата промяна, поради което за КРС не е налице възможност да обсъди направеното предложение.

№	ДОСТАВЧИК	ЗАБЕЛЕЖКА	СТАТУС	МОТИВИ
4.	**СПЕКТЪР АД**	В Допълнителни разпоредби, § 1 да се създаде нова т. 5, в която да бъде дефинирано понятието „**мобилни приложения**”. „5. „Мобилни приложения са софтуерни приложения, интегрирани в устройство за сигурно създаване на подписа в мобилните телефони”. **Мотиви:** Липсата на дефиниране на „мобилни приложения” за целите на тази Наредба, създава предпоставка за широко тълкуване (напр. GSM приложения, преносими медии, Flash памети и т.н.).	**Приема се частично**	КРС приема за обоснована бележката за необходимост от дефиниране на понятието, но комисията счита, че определението трябва да е с редакция, както следва: *„Мобилни приложения” са софтуерни приложения за устройства за сигурно създаване на подписа, използвани в мобилни телефонни апарати, работещи под контрола на мобилна наземна мрежа – GSM и UMTS.”* КРС счита, че така редактирана нормата е по-точна от терминологична гледна точка.
5.	**ИНФОРМАЦИОННО ОБСЛУЖВАНЕ АД**	Да се дефинира понятието **„мобилни приложения”**.	**Приема се**	Съобразно посоченото по-горе.
6.	**БОРИКА – БАНКСЕРВИЗ АД**	Да бъде точно определено въведеното в приложението към чл.4 ал.4 „Изисквания за използваните алгоритми за квалифициран електронни подписи” т.10 понятие „**мобилни приложения**”. **Мотиви:** В наредбата не се указва значението на понятието „мобилни приложения”. То може да се разбира като приложения, изпълнявани върху мобилни апарати/системи или приложения, използващи мобилна (GPRS, UTMS и т.н.) преносна среда. Самите понятия мобилни апарати/системи и мобилна преносна среда също се нуждаят от детайлизиране. Описаните неясноти внасят объркване, както в тълкуването на понятието, така и в прилагането на наредбата.	**Приема се**	Съобразно посоченото по-горе.
7.	**ИНФОРМАЦИОННО ОБСЛУЖВАНЕ АД**	**Да се създаде преходна разпоредба със следното съдържание:** „Изискванията към алгоритмите за квалифициран подпис, посочени в приложението към чл. 4, ал. 4, не се прилагат по отношение на удостоверенията за електронен подпис, издадени от регистрирани доставчици на удостоверителни услуги до влизането в сила на тази наредба.”	**Приема се по принцип**	КРС приема, че в проекта не налице разпоредба, която да уреди заварените случаи. Предвид посоченото по бележка първа от настоящата таблица и с оглед предвидените изисквания в проекта, комисията счита, че правилото относно заварените случаи следва да бъде така: *„§ 3. (1) Издадените преди влизане в сила на наредбата удостоверения за*

№	ДОСТАВЧИК	ЗАБЕЛЕЖКА	СТАТУС	МОТИВИ
				усъвършенстван и универсален електронен подпис, които не отговарят на изискванията на наредбата, могат да се използват в срок до 5 години от влизане в сила на наредбата. *(2) Базовите и оперативните удостоверения на доставчиците на удостоверителни услуги, издадени преди влизане в сила на наредбата, могат да се използват и след изтичане на срока по ал. 1, но само за управление на издадени потребителски удостоверения за квалифициран електронен подпис, до изтичане на срока на валидност на последните.”*