Приложение към решение № 293 от 21 март 2011 г. на КРС

Проект!

НАРЕДБА ЗА ИЗИСКВАНИЯТА КЪМ АЛГОРИТМИТЕ ЗА СЪЗДАВАНЕ И ПРОВЕРКА НА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС

Глава първа
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. С наредбата се определят изискванията към алгоритмите за създаване на частен и публичен ключ за квалифициран електронен подпис и към алгоритмите за създаване и проверка на квалифициран електронен подпис.

Чл. 2. (1) Лицата, които създават частен и публичен ключ за квалифициран електронен подпис, и лицата, които създават и извършват проверка на квалифициран електронен подпис, са длъжни в процеса на създаването и проверката да спазват изискванията на наредбата.

(2) Когато лицето по ал. 1 е доставчик на удостоверителни услуги, то е длъжно да не съхранява или копира частни ключове и данни за създаването им.

Чл. 3. Доставчик на удостоверителни услуги, предлагащ и услугата по създаване на частен и публичен ключ за квалифициран електронен подпис, трябва да поддържа списък на прилаганите от него за тази цел алгоритми в "Практика при предоставяне на удостоверителни услуги", разработена съгласно изискванията на наредбата по чл. 21, ал. 2 от Закона за електронния документ и електронния подпис.

Глава втора
ИЗИСКВАНИЯ КЪМ АЛГОРИТМИТЕ ЗА КВАЛИФИЦИРАН ЕЛЕКТРОНЕН ПОДПИС

Чл. 4. **(1)** Създаването на частен и публичен ключ за квалифициран електронен подпис се осъществява чрез използване на алгоритъм, съответстващ на алгоритъма за създаване на квалифициран електронен подпис и при използване на сигурен източник на случайни числа.

(2) Хеш-алгоритмите и асиметричните алгоритми за квалифициран електронен подпис трябва да отговарят на изискванията на наредбата.

(3) Създаването на квалифициран електронен подпис включва:

1. прилагане на хеш-алгоритъм за изчисляване на хеш-идентификатор на електронното изявление;

2. прилагане на асиметричен алгоритъм за подписване;

3. прилагане на метод за допълване.

(4) Използваните алгоритми за квалифициран електронен подпис и изискванията към тях са посочени в приложение към наредбата.

Чл. 5. Алгоритмите за проверка на квалифициран електронен подпис съставляват логическо цяло с алгоритмите за създаването му.

Чл. 6. Съответствието на устройството за сигурно създаване на подписа с изискванията на чл. 17, ал. 1 от Закона за електронния документ и електронния подпис се удостоверява с документ, издаден от акредитирана лаборатория за осъществяване на такава проверка.

Допълнителни разпоредби

§ 1. По смисъла на тази наредба:

1. „хеш-алгоритъм” е математически алгоритъм, чрез който от електронно изявление с произволна дължина необратимо се създава хеш-идентификатор на изявлението.

2. „хеш-идентификатор” е число с фиксирана дължина, получено вследствие на прилагане на хеш-алгоритъм спрямо определено електронното изявление.

3. „сигурен източник на случайни числа” е метод за генериране на последователност от числа, в която всяко следващо число не може да бъде изчислено от предишните.

4. „метод за допълване (padding)” е процес, при който се преобразува хеш-идентификатора на електронното изявление преди прилагане на съответния алгоритъм за създаване на квалифициран електронен подпис.

§ 2. С наредбата се въвеждат относимите изисквания на Решение 2011/130 на Европейската комисия от 25 февруари 2011 г. за установяване на минимални изисквания за трансгранична обработка на документи, подписани от компетентните органи съгласно Директива 2006/123/ЕО на Европейския парламент и съвета относно услугите на вътрешния пазар (ОВ L 53/66, 26.02.2011)

Заключителни разпоредби

§ 3. Наредбата се приема на основание чл. 16, ал. 2 от Закона за електронния документ и електронния подпис и влиза в сила от 1 юли 2011 г.

§ 4. Наредбата отменя Наредба за изискванията към алгоритмите за усъвършенстван електронен подпис (Приета с ПМС № 17 от 31.01.2002 г., обн. ДВ. бр. 15 от 08.02.2002 г.)

Приложение към чл. 4, ал. 4

Изисквания за използваните алгоритми за квалифициран електронни подписи

1. Хеш-алгоритми:

1.1. SHA-1 (Secure Hash Algorithm);

1.2. SHA-2 (224, 256, 384, 512 бита);

1.3. RIPEMD-160 (Race Integrity Primitives Evaluation Message Digest) (256, 320 бита).

2. Не се допуска използването на следните хеш-алгоритми MD 4 и MD 5.

3. Допуска се използване и на други, различни от посочените в т. 1, хеш-алгоритми, които са с най-малко същото ниво на сигурност.

4. Дължината на идентификатора на електронното изявление следва да е не по-малка от 160 бита.

5. Асиметрични алгоритми за квалифициран електронен подпис:

5.1. RSA (Rivest-Shamir-Adleman) с минимална дължина 1024;

5.2. DSA (Digital Signature Algorithm);

5.3. ECDSA (Elliptic Curve Digital Signature Algorithm).

6. Допуска се използване и други алгоритми, различни от посочените в т. 5, за създаване на двойки ключове и създаване на електронни подписи, които са с най-малко същото ниво на сигурност.

7. Приложимите комбинации на асиметрични и хеш-алгоритми спрямо сигурността на квалифицирания електронен подпис по времетраене са следните:

Приложима комбинация	1 година	3 години	6 години
sha1-with-rsa	1 024		
sha256-with-rsa	1 024	1 536	2 048
RSASSA-PSS with mgf1SHA-1Identifier	1 024	1 536	2 048

Приложима комбинация	1 година	3 години	6 години
RSASSA-PSS with mgf1SHA-224Identifier	1 024	1 536	2 048
RSASSA-PSS with mgf1SHA-256Identifier	1 024	1 536	2 048
sha1-with-dsa	1 024		
sha1-with-ecdsa	163		
sha224-with-ecdsa	224	224	224
sha256-with-ecdsa	256	256	256

8. След изтичане на срока, посочен за съответната комбинация, трябва да се генерира нова двойка ключове и да се издава ново удостоверение за квалифициран електронен подпис.

9. Устойчивостта във времето на комбинацията от асиметричен и хеш-алгоритъм на доставчика на удостоверителни услуги трябва да е по-голяма или равна на устойчивостта във времето на комбинацията от асиметричен и хеш-алгоритъм, използвана за квалифициран подпис на краен потребител.

10. За нуждите на мобилни приложения се допуска използването на комбинацията sha1-with-rsa (1024) за издаване на удостоверение за квалифициран електронен подпис със срок на валидност не повече от 3 години.

11. При създаването на квалифициран електронен подпис трябва да се използват следните алгоритми: Canonical XML 1.0, Canonical XML 1.1 и Exclusive XML Canonicalization 1.0. Допуска се поддържането на други алгоритми с оглед проверка на подписа.