ИНСТРУКЦИЯ ЗА КРИПТИРАНЕ НА ДОКУМЕНТИТЕ И СЪОБЩЕНИЯТА С ПУБЛИЧНИЯ КЛЮЧ НА КОМИСИЯТА ЗА ФИНАНСОВ НАДЗОР

КФН | КОМИСИЯ ЗА ФИНАНСОВ НАДЗОР

Финансовите субекти подават доклади за съществени инциденти, свързани с информационни и комуникационни технологии (ИКТ) до Комисията за финансов надзор или доброволно да уведомят Комисията за финансов надзор за значителни киберзаплахи, както и подават данни за информационния регистър на договорните си споразумения с трети страни доставчици на услуги в областта на ИКТ чрез защитен канал. За целите на предаване на посочената информация се ползва електронна поща с криптиране.

I. Технически предпоставки

1. Генериране на ключове от Комисията за финансов надзор и докладващия субект

Необходимо е Комисията за финансов надзор и докладващият субект да имат инсталиран софтуер GNU Privacy Guard (GPG) за генериране на двойка криптографски ключове с дължина 4096 бита (bits). Ключовете се използват за сигурна комуникация помежду си.

2. Публичен и частен ключ, генерирани от Комисията за финансов надзор

- Комисията за финансов надзор генерира публичен и частен ключ с дължина 4096 бита;
- публичният ключ на Комисията за финансов надзор се подписва с електронен подпис на председателя на Комисията за финансов надзор и се генерира .p7m файл - PKCS#7 Signed Message File;
- Комисията за финансов надзор публикува публичния ключ във формат .asc, заедно с .p7m файла на интернет страница си;

3. Публичен и частен ключ, генерирани от докладващия субект

- докладващият субект генерира публичен и частен ключ;
- публичният ключ се подписва с електронен подпис на законен представител/представители на докладващия субект или

упълномощено от тях лице и се генерира .p7m файл - PKCS#7 Signed Message File;

- публичният ключ на докладващия субект и генерирания .p7m файл се изпращат на Комисията за финансов надзор посредством съобщение, подписано с електронен подпис на законния представител/представители на докладващия субект или упълномощено от тях лице;

Съобщенията се изпращат чрез защитен канал на имейл ict_contact_point@fsc.bg, предназначен за докладване на съществени инциденти с ИКТ и уведомяване за значителни киберзаплахи.

4. Сигурен канал за обмен на информация

Разменените публични ключове между Комисията за финансов надзор и докладващия субект се използват за криптиране на кореспонденцията, водена между тях.

С цел криптиране на кореспонденцията пощенските кутии на изпращача и получателя е препоръчително да се настроят за автоматично криптиране и подписване на съобщения, като се гарантира съвместимост с OpenPGP стандарта. Криптирането и подписването могат да се извършват и ръчно.

II. Изпращане на информация към Комисията за финансов надзор

При изпращане на информация до Комисията за финансов надзор докладващия субект спазва следната последователност на действия:

- докладващият субект подписва всички документи с квалифициран електронен подпис (КЕП) на законния представител/и или упълномощено от тях лице, което гарантира автентичността и интегритета на информацията;
- ако файловете не могат да бъдат подписани с вграден електронен подпис или са повече от един, те се архивират в един общ .zip файл без парола, който се подписва във формат .p7m - PKCS#7 Signed Message File;

- докладващият субект криптира файла с публичния ключ на Комисията за финансов надзор преди да изпрати електронно съобщение;
- електронното съобщение се подписва с КЕП на законния представител/и на докладващия субект или упълномощено от тях лице, с което се гарантират автентичността и интегритета на съобщението, и се изпраща до Комисията за финансов надзор;
- Комисията за финансов надзор получава съобщението, извлича файловете и ги декриптира посредством съответния частен ключ.

Контролът за подписване, криптиране и архивиране на файловете е в задължение на докладващия субект.

III. Изпращане на информация от Комисията за финансов надзор

1. Критична информация

Аналогично на процеса по изпращане на информация от докладващия субект, Комисията за финансов надзор подписва изходящите файлове с КЕП на оправомощен служител, изпращащ съобщението, криптира ги с публичния ключ на докладващия субект и изпраща електронно съобщение, подписано с КЕП.

Докладващият субект получава съобщението, извлича файловете и ги декриптира посредством съответния частен ключ.

2. Некритична информация

Документи, съдържащи некритична информация, могат да не се криптират. Електронното съобщение, с което се изпраща некритичната информация се подписва с КЕП на оправомощения служител, изпращащ съобщението.

IV. Допълнителни изисквания

Докладващият субект е необходимо да има предвид следните

допълнителни изисквания:

- генерираните криптографски ключове е необходимо да са с минимална дължина RSA-4096;
- ключовете е необходимо да бъдат подновявани на всеки 2 години, а при съмнения за компрометиране – незабавно;
- при компрометиране на ключ Комисията за финансов надзор се уведомява с електронно съобщение, подписано с КЕП на законния представител/и или упълномощено от тях лице, в което се посочва и генерирания нов публичен ключ;
- електронните подписи е необходимо да са в съответствие с Регламент (ЕС) 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 година относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО (eIDAS).

V. Потвърждение на получените съобщения

За гарантиране на успешен обмен на информация между докладващия субект и Комисията за финансов надзор при всяко изпратено електронно съобщение се прилага следната процедура за потвърждение:

- докладващия субект подава до Комисията за финансов надзор съответната информация чрез защитен канал на изрично посочените имейл адреси;
- след като информацията е подадена по надлежния ред, докладващият субект ще получи потвърждение и референтен код, който гарантира успешното докладване;
- подадена информация, за която не е получено потвърждение и референтен код, се счита за неуспешно докладвана.