Datu šifrēšanas instrukcija

Instrukcija satur norādes droša pārskata faila sagatavošanai saskaņā ar noteikumiem "Informācijas par kredītiestādes klientiem un to veiktajiem darījumiem apkopošanas un sniegšanas Finanšu un kapitāla tirgus komisijai normatīvie noteikumi" (<https://www.vestnesis.lv/op/2016/236.18>). Darbību piemēros ir izmantota bezmaksas programmatūra, bet tā nav uzskatāma par vienīgo iespējamo. Atļauts pielietot alternatīvas programmatūras, taču rezultātam (nosūtāmam failam) jābūt atbilstošam instrukcijā norādītam.

Paraugā izmantota šāda programmatūra:

* 7-ZIP (http://www.7-zip.org/download.html);
* GnuPG "GPG" (https://gnupg.org/download/index.html).

Par korektu ZIP arhīvu tiek uzskatīts arhīvs, kas atbilst ISO/IEC 21320-1:2015 standartam par ZIP formāta konteineriem (arhīvs kompresēts ar DEFLATE kompresijas algoritmu, netiek lietota iebūvētā ZIP šifrēšana, failu nosaukumi satur tikai ASCII, nevis UTF-8 paplašinātos simbolus).

Par korektu PGP šifrētu failu tiek uzskatīts tāds, kas atbilst OpenPGP standartam (IETF RFC 4880).

Veicamie soļi:

1. ZIP arhīva izveidošana.

ZIP arhīva izveidošanai, pielietojot 7-Zip arhivēšanas programmu komandrindā, izmantojama šāda komanda, lai iegūtu ZIP arhīvu, kas satur data.csv un info.xml failus:

>[Ceļš uz 7-zip direktoriju]>7z.exe a [Ceļš kur novietot izvedojamo arhīvu]\AML.zip [Ceļš uz info.xml failu]\info.xml [Ceļš uz info.csv]\info.csv



1. GPG atslēgu pārvaldība.
GPG atslēga atrodama FKTK Datu ziņošanas sistēmā (<https://dati.fktk.lv>) dokumentā "Par Informācijas par kredītiestādes klientiem un to veiktajiem darījumiem apkopošanas un sniegšanas Finanšu un kapitāla tirgus komisijai normatīvie noteikumi" pielikumā - FKTK\_NN\_197\_2016\_public.gpg (Key ID A46BE11E, Fingerprint: 19B9 8E5D BE99 B80E E582 C5F1 C698 342A A46B E11E).

Pēc atslēgas lejupielādes tā jāimportē Jūsu sistēmas *atslēgu saišķī (keyring)* izmantojot šādu komandu:

> gpg –homedir [Ceļš uz atslēgusaišķa (keyring) direktoriju] –import [Ceļš uz FKTK publiskās atslēgas failu]\ FKTK\_NN\_197\_2016\_public.gpg

Pēc atslēgas importa, lai pārliecinātos par tās esamību Jūsu atslēgas saišķī (keyring), izmantojama šāda komanda:

> gpg –homedir [Ceļš uz atslēgusaišķa (keyring) direktoriju] --list-keys



1. Droša PGP arhīva izveidošana.

FKTK nosūtāmais arhīva fails veidojams ar komandu:

>gpg --output [Ceļš uz izejas failu]\AML.pgp --recipient FKTK\_NN\_197\_2016 --encrypt [Ceļš uz ieejas failu]\AML.zip

 Situācijā, ja pēc šīs komandas izpildes Jūs saņemat šādu paziņojumu par to, ka atslēga nav marķēta kā uzticama, komandas izpildi apstipriniet ar taustiņu y:

>y



Gadījumā, ja neizmantojat piemērā minēto programmatūru un atbilstošas komandas, noteikti ievērot šādas prasības:

* Šifrējot ZIP failu, pie šifrēšanas jānorāda tikai un vienīgi ar FKTK\_NN\_197\_2016 publiskā atslēga (viens saņēmējs);
* Šifrētajam failam nav jāsatur digitālais paraksts no iesūtītāja puses;
* ZIP arhīvs nedrīkst saturēt citus failus, kā tikai "data.csv" un "info.xml".