СПОДЕЛИ ДОЖИВУВАЊА

УСЛОВИ ЗА КРЕИРАЊЕ И КОРИСТЕЊЕ НА УСЛУГАТА

ДОВЕРЛИВОСТ KS CLOUD

2018

Овие Услови за креирање и користење на услугата Доверливост KS Cloud ги уредува односите помеѓу Корисникот и Македонски Телеком, како Издавач на дигитален сертификат, во процесот на дигитално потпишување документи, како и начинот на работа на веб базираната апликација за потпишување, обезбедена од Издавачот https://cloudsigning.telekom.mk.
Условите за креирање и користење на услугата Доверливост KS Cloud е составен дел на Договорот за користење на услугата – Дигитален сертификат, склучен помеѓу Корисникот и Македонски Телеком.

Креирање на Доверливост KS Cloud дигиталните сертификати

Процесот на креирање на дигиталните сертификати се одвива во високо безбедна околина заштитена по сите стандарди за работа со дигитални сертификати. Креирањето на клучевите се изведува на HSM уреди кои гарантираат највисоко ниво на безбедност.

Hardware Security Module (HSM)

Hardware Security Module (HSM) е физички процесирачки уред кој управува и ги заштитува дигиталните клучеви за обезбедување високо ниво на безбедност при автентификација и обезбедува широк спектар на крипто операции.

Чување на дигиталните сертификати

Приватните клучеви се чуваат во криптирана форма. Криптирањето на приватните клучеви се изведува во HSM уредот со помош на два параметра: корисничкиот ПИН кој го знае исклучиво крајниот корисник и „master" клучот кој е зачуван на HSM уредот и никогаш не го напушта. На тој начин се избегнува можноста за каква било злоупотреба на приватните клучеви на крајните корисници.

Користење на дигиталните сертификати

Корисниците можат да го употребуваат Доверливост KS Cloud сертификатот за сите крипто операции за кои е наменет од кој било уред и од која било локација. При употребата на дигиталните сертификати, корисникот мора секогаш да го приложи ПИН бројот што само тој го знае и поседува, со цел да се овозможи процесот на декрипција на приватниот клуч, тој за да може да се употреби за дигитално потпишување. Никој освен крајниот корисник кој го знае ПИН-от асоциран со даденият клуч нема можност да изврши каква било крипто операција со него.
Одговорноста за чување на ПИН бројот асоциран со приватниот клуч е одговорност на самиот корисник. Во случај на губење на ПИН бројот, корисничкиот сертификат и асоцираниот приватен клуч, сертификатот не може повеќе да се користи и ќе треба да се издаде нов.

Промена на ПИН

Корисникот може во кој било момент да изврши промена на ПИН бројот преку својот профил на веб порталот согласно корисничкото упатство. Промената на ПИН-от е препорачлива операција секогаш кога корисникот се сомнева во неговата тајност.

Загубен ПИН

Чувањето на ПИН-от е во целосна одговорност на крајниот корисник. Тој не се чува никаде во каков било облик и нема можност за негово враќање во случај да биде заборавен или загубен. Во случај на загубен ПИН, корисничкиот сертификат и асоцираниот приватен клуч не можат повеќе да се декриптираат и да се користат и со тоа стануваат неупотребливи.

Механизми за заштита од злоупотреба на дигиталниот сертификат

Македонски Телеком обезбедува високодостапна и безбедна инфраструктура која го гарантира чувањето на приватните клучеви во криптирана форма во случај на несакани хардверски проблеми или елементарни непогоди. Дополнително, обезбедува механизми за непрекинато работење, како и за брзо враќање на системите во функција во случај на какви било непогоди.

Ограничување на одговорноста

Македонски Телеком нема да има никаква одговорност за евентуално погрешно користење или користење од неовластено лице на дигиталниот сертификат, ниту пак, каква било одговорност во однос на каква било материјална (обична штета или испуштена корист) или нематеријална штета, настаната на Корисникот или трети лица, а како резултат на употребата на веб апликацијата за дигитално потпишување https://cloudsigning.telekom.mk.