IndependenceKey

Kako šifriramo občutljive podatke?

..Uporabniki interneta se lahko upravičeno sprašujejo, ali so njihovi osebni ali poslovni podatki sploh lahko še varni. Recept za učinkovito varovanje podatkov je preprost: ne zaupajte nikomur in sami prevzemite odgovornost za ustrezno varovanje!..

Šifrirni ključ USB IndependenceKey podjetja Quantec iz Švice (www.independencekey.com) predstavlja vsestransko varnostno napravo za izvajanje močnega strojnega šifriranja podatkov in komunikacij po standardu AES. S to edinstveno napravo je mogoče zares učinkovito in varno posredovati, deliti in hraniti občutljive podatke na različnih pomnilniških medijih in v oblaku ter varno komunicirati na storitvi VoIP.

Kako deluje naprava IndependenceKey?

Naprava se preprosto vstavi v priključek USB na računalniku. Ob prvi uporabi je treba izvesti inicializacijo ključa, kjer določimo tudi glavno geslo. Po petih zaporednih poskusih vnosa napačnega gesla se naprava zaklene in postane neuporabna. S tem se ustvari zaščita pred nepooblaščeno uporabo in krajo podatkov. Za razliko od programskih rešitev za šifriranje podatkov pri strojnih varnostnih modulih oziroma pametnih karticah šifrirni ključi nikoli ne zapuščajo naprave. Rdeč logotip »K« na napravi začne enakomerno utripati, ko je naprava pripravljena za delovanje.

Kaj je na zaslonu?

Z dvojnim klikom na ikono »K« ali izbiro IndependenceKey v meniju Start se zažene preprost, prijazen uporabniški vmesnik. Sestavljen je iz šestih modulov: seznama stikov, varnega telefoniranja na storitvi VOIP, diska USB, šifriranega diska, upravljanja z gesli in varnostnega pokrovčka (security cap).

Seznam stikov je sestavljen iz vseh prej uparjenih uporabnikov naprave IndependenceKey, s katerimi je mogoče deliti šifrirane informacije. Uparjanje (»spoznavanje« naprav med seboj) je zelo preprosto in se lahko opravi fizično z neposrednim vstavljanjem naprave B v priključek USB naprave A. Vsak lastnik naprave vnese svoje geslo in napravi se »spoznata« oziroma samodejno izvedeta izmenjavo šifrirnih ključev. Po tem postopku lastniki naprav na svojem seznamu stikov lahko vidijo »spoznano« napravo.

Uparjanje naprav IndependenceKey je mogoče tudi na daljavo prek interneta. V tem primeru se kot posrednik uporablja strežnik proizvajalca

Quantec v Švici, ki ne shranjuje nobenih javnih ključev. Quantecovi strežniki samo omogočijo varno »spoznavanje« naprav. Skozi celoten postopek so podatki iz naprave A do naprave B šifrirani in neberljivi. Postopek je popolnoma varen, ker se pri uparjanju posreduje le del serijske številke čipa TPM (Trusted Platform Module) v napravi, ki je za vsako napravo IndependenceKey edinstven.

Varna telefonija VoIP in priključitev drugih naprav USB

IndependenceKey je edinstvena rešitev za strojno šifriranje spletnih pogovorov VOIP. S priključitvijo standardnih slušalk USB v priključek USB naprave IndependenceKey omogoča šifriran pogovor. Oba udeleženca prej seveda opravita uparjanje naprav.

Šifrirani spominski mediji

V priključek USB naprave IndependenceKey je mogoče priključiti katerokoli napravo za shranjevanje podatkov (zunanji diski, pomnilniški ključi USB in drugo), kar omogoča šifriranje vseh podatkov na priključenem mediju. Vsi ti podatki postanejo nedostopni vsem, razen lastniku naprave IndependenceKey, ki je izvedel šifriranje.

Varnostni pokrovček (security cap)

Čeprav so šifrirni ključi varno shranjeni v napravi IndependenceKey, vedno obstaja možnost izgube ali tatvine same naprave. Brez varnostnega pokrovčka lahko izgubimo vse podatke, šifrirane z napravo IndependenceKey. Z varnostnim pokrovčkom, ki ga shranimo varno in ločeno od naprave IndependenceKey, omogočimo ponovno branje vseh šifriranih podatkov, tudi v primeru uporabe novega ključa IndpendenceKey. Vanj preprosto vstavimo stari varnostni pokrovček in začne se proces inicializacije, ki omogoča povrnitev vsebine v novo napravo IndependenceKey. Čez nekaj trenutkov se nova naprava obnaša popolnoma enako kot stara. Isti postopek velja v primeru, da bi pozabili glavno geslo, kar se običajno zgodi bolj pogosto.

V poslovnih okoljih

IndependenceKey Commander je posebej primeren za uporabo v podjetjih in organizacijah. Taka naprava ima možnost upravljanja vseh šifriranih naprav IndependenceKey v organizaciji, ki so povezane z napravo Commander. Z njim je mogoče onemogočiti oziroma zakleniti posamezni IndependenceKey in tudi odšifrirati vse dokumente, ki so bili zašifrirani s katerimkoli ključem IndependenceKey v organizaciji. Postopek uvedbe hierarhije ključev IndependenceKey je preprost. Vsak IndependenceKey, ki ga želite imeti pod nadzorom, vstavite v ključ USB, opredeljen kot Commander. S tem je ključ USB umeščen v hierarhijo naprav in pripravljen za uporabo pri zaposlenem, ki si potem sam določi svoje geslo.

Zaščita podatkov še nikoli ni bila tako preprosta!

(P. R.)