

METODE SHRANJEVANJA KRIPTOGRAFSKIH KLJUČEV

Zadnja posodobitev dne 12. 12. 2023

Možnost A - Shranjevanje kriptografskih ključev pri izvajalcu

1. IDENTIFIKACIJA SREDSTEV

1.1 Izvajalec na izrecno zahtevo naročnika hrani kriptografske ključe, ki so potrebni za dešifriranje informacij na platformi ("kriptografski ključi"). Ta varnostni ukrep se izvaja zaradi izpolnjevanja zakonskih zahtev in za ustrezno zaščito podatkov v prijavih.

2. NAČIN IZDAJE IN PREDAJE KLJUČEV

2.1 Izvajalec izda kriptografske ključe na izrecno pisno zahtevo naročnika.

2.2 Da bi zagotovili največjo varnost postopkov izdaje in predaje kriptografskih ključev, je naročnik dolžan izvajalcu navesti seznam oseb, ki so pooblaščen za vložitev ustrezne zahteve.

2.3 Izvajalec dostavi kriptografske ključe navedenim osebam.

3. ODGOVORNOSTI STRANK

3.1 Izvajalec je dolžan dati kriptografske ključe na voljo naročniku, pod pogojem, da zahtevo vložijo pooblaščen osebe.

3.2 Izvajalec ne prevzema nikakršne odgovornosti za preverjanje predpogojev, ki upravičujejo izdajo kriptografskih ključev, pri čemer se kot zadosten pogoj šteje zahteva pooblaščenih oseb.

3.3 Zahtevnik se obravnava v običajnem delovnem času. Če je zahteva za izdajo kriptografskih ključev vložena zunaj delovnega časa ali ob praznikih, lahko nastanejo dodatni stroški.

3.4 Če pride do izgube, uničenja ali nepooblaščen uporabe kriptografskih ključev iz razloga na strani naročnika, naročnik povrne škodo in zavaruje izvajalca pred vsako odgovornostjo za škodo, ne glede na njeno naravo, ki bi nastala naročniku, izvajalcu in/ali tretjim osebam.

4. OBDOBJE HRAMBE

4.1 Kriptografski ključi se hranijo ves čas trajanja pogodbe med naročnikom in izvajalcem. Po prenehanju pogodbe jih izvajalec varno izbriše in dostop do vsebine platforme ni več mogoč.

Linija Spregovori!

Projekt Transparency International Slovenia
www.spregovori.si | info@spregovori.si

Možnost B - Shranjevanje kriptografskih ključev pri naročniku

1. IDENTIFIKACIJA SREDSTEV

1.1 Naročnik je odgovoren za shranjevanje kriptografskih ključev, potrebnih za dešifriranje informacij na platformi ("kriptografski ključi"). Ta varnostni ukrep se izvaja zaradi izpolnjevanja zakonskih zahtev in kot zagotovilo, da do podatkov v prijavah dostopa izključno le naročnik.

2. NAČINI SKRBNIŠTVA

2.1 Naročnik je odgovoren za pravilno in varno shranjevanje kriptografskih ključev. Naročnik zlasti izvaja vse potrebne tehnične in organizacijske ukrepe za zagotovitev njihove zaupnosti, pristnosti in celovitosti.

3. ODGOVORNOST STRANK

3.1 Naročnik se zaveda, da lahko ogrožanje zaupnosti, pristnosti in celovitosti kriptografskih ključev lahko povzroči ogrožanje zaupnosti, pristnosti in celovitosti informacij na platformi ter nezmožnost dostopa do njih.

3.2. Naročnik je izključno odgovoren za hrambo kriptografskih ključev ter je dolžan izvajalcu povrniti škodo in ga zavarovati pred vsako odgovornostjo za škodo, ne glede na njeno naravo, ki bi nastala naročniku, izvajalcu in/ali tretjim osebam zaradi izgube, uničenja in/ali nepooblaščne uporabe kriptografskih ključev.