AGENCIJA ZA KOMERCIJALNU DJELATNOST proizvodno, uslužno i trgovačko d.o.o. Savska cesta 31, 10000 Zagreb OIB: 58843087891	Evidencijski broj: 18/INV/OPN
II. Pojašnjenje Dokumentacije o nabavi	

ZAINTERESIRANIM GOSPODARSKIM SUBJEKTIMA

Na temelju točke 10. Dokumentacije o nabavi, u otvorenom postupku nabave „Zamjena sistema Tahoca i pripadnih HSM uređaja", Naručitelj objavljuje:

POJAŠNJENJE DOKUMENTACIJE O NABAVI

Na temelju zaprimljenog upita gospodarskog subjekta, Naručitelj daje pojašnjenje Dokumentacije o nabavi kako slijedi:

1. Pitanje

Uvidom u Tehničku dokumentaciju primjećen je mogući problem s potvrđivanjem iste; naime u retku Podrška za asimetrične ključeve navedeno je: *Must support work in a way that we can use RSA 1024 key for generating and sign.*

Ovaj dio je u sukobu s FIPS 140-2 Level 3 certifikacijom koja je također dio specifikacije. Problem je što ključevi duljine 1024 bita nisu dovoljno sigurni za FIPS te ukoliko želite koristiti ključeve te duljine morate isključiti FIPS mode što bi značilo da je rad s RSA 1024 ključevima podržan, ali gubite FIPS certifikaciju.

Najljepše bismo molili uputu kako postupiti.

1. Odgovor

Svjesni smo da rad s asimetričnim ključevima duljine 1024 bita nije FIPS certificiran i da HSM uređaj prilikom postavljanja neće biti u FIPS modu. Bitna nam je samo potvrda da izvan FIPS certificiranog načina rada HSM uređaj može raditi operacije generiranja asimetričnih ključeva duljine 1024 bita i potpisivanja istima.

FIPS 140-2 Layer 3 certifikacija uređaja je tražena zbog kasnije mogućnosti postavljanja uređaja u FIPS certificirani način rada.

POVJERENSTVO ZA NABAVU