TELSEC

KRIPTOGRAFSKI UREĐAJ

Općenito

Kriptografski uređaj TELSEC strogo je namjenski sklopovski uređaj koji služi za kriptografsku zaštitu govornog, podatkovnog i video prometa.

Izvedba uređaja projektirana je tako da se integrira u postojeću komunikacijsku infrastrukturu instalacijom između krajnjeg uređaja i centrale.

Značajke

- Zaštita govora, podataka i video signala
- Diffie-Hellman 2048 razmjena ključeva
- Elliptic-curve 384 razmjena ključeva
- AES-256 simetrična enkripcija
- SHA-3 „hash" algoritam
- Autentifikacija korisnika pametnom karticom
- PSK modem
- Ethernet 10/100 Mbps
- Rad s analognim i VoIP telefonima
- Ethernet konekcija prema računalu (DHCP)
- T.30 signalizacija
- TEMPEST i TAMPER zaštita uređaja
- Hardverski generator slučajnih brojeva

Modovi rada

VoIP	IP - Telefonija	PSTN
• Zaštita govora i datoteka u internet i privatnim intranet mrežama • Kompatibilan sa SIP i H.323 standardima • Zaštita video linka • Automatski prijelaz u ovaj mod rada, kad uređaji detektiraju mogućnost izravne komunikacije	• G.711 govorni kodek • SIP i H.323 pozivanje • T.30/V.8 signali (fax pass-through mod) • PSK modem • Automatski prijelaz u VoIP mod kad uređaji detektiraju mogućnost izravne komunikacije	• PSK modem • Koristi standardni 3.1 kHz kanal (300 – 3400 Hz) • T.30/V.8 signali (fax pass-through mod)

Pomorski centar za elektroniku d.o.o. Split

Split – Croatia
Zrinsko-Frankopanska 209

Tel: +385 21 495-622
Fax: +385 21 495-679

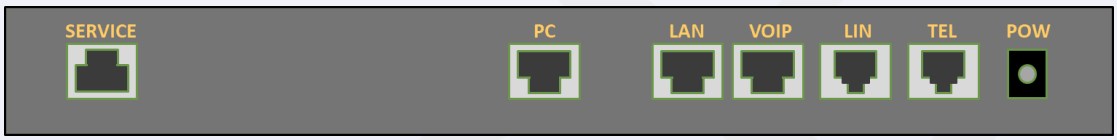
www.pce.hr
E-mail: pce@pce.hr

Opis uređaja

Glavni motiv za razvoj ovog uređaja je sve veća zastupljenost VoIP telekomunikacijskih mreža koje su poveznicima (gateway) uključeni u klasičnu (SDH/SONET) telefonsku infrastrukturu. Na tržištu postoje uređaji koji zasebno štite analogne i VoIP (internet/intranet) kanale, međutim zaštita korisnika javne telefonske mreže koji mogu biti na IP ili analognom priključku, predstavljao je poseban izazov. Naime, moderne telefonske centrale, zbog uštede u kapacitetu ukupnog podatkovnog prometa, koriste metode kompresije koje ne zadovoljavaju uvjete u kojima se mogu koristiti modulacijske metode zadovoljavajuće brzine. U tom slučaju, uređaj automatski aktivira T.30/V.8 signale kojima zahtjeva prijelaz na G.711 način kompresije. Nakon toga aktivira se modemski prijenos, posebno dizajniran za ovu namjenu, i uspostavlja se zaštićen govorni kanal. Ukoliko je detektirana izravna IP komunikacija, uređaj ne koristi modem, već se zaštita obavlja na RTP paketima. Štiti se jedan audio i jedan video kanal (ukoliko postoji).

Autentifikacija korisnika ili administratora, temelji se na pametnoj kartici. Koristeći naše uređaje za upravljanje sustavom, kupac potpuno samostalno konfigurira korisničke, administratorske i aktivacijske kartice.

Opis sučelja



Sučelje	Tip	Opis
SERVICE	RJ-45	Samo za potrebe testiranja uređaja u tvorničkim uvjetima
PC	RJ-45	Standardan Ethernet 10/100 Mbps priključak za PC. Putem posebne aplikacije omogućava korisniku prijenos datoteka i administriranje uređaja.
LAN	RJ-45	Standardan Ethernet 10/100 Mbps priključak. Spaja se prema VoIP centrali.
VOIP	RJ-45	Standardan Ethernet 10/100 Mbps priključak. Spaja se na VoIP telefon s ili bez video podrške. Omogućava i napajanje aparata putem PoE metode do 20W.
LIN	RJ-11	Standardan dvožični telefonski priključak prema telefonskoj centrali putem analognog signala.
TEL	RJ-11	Standardan dvožični telefonski priključak prema analognom telefonskom aparatu.
POW		Dvopolni konektor napajanja. Nominalno 12 V DC.

PREDNJA STRANA UREĐAJA

Sučelje	Tip	Opis
POW	LED	Status napajanja
FILE	LED	U tijeku je prijenos datoteke
VIDEO	LED	Pored govornog, štiti se i jedan komprimirani video kanal
SEC	LED	Komunikacija je uspostavljena i zaštićena
AUTH	LED	Korisnik je uspješno autentificiran putem pametne kartice
RUN	LED	Softver normalno funkcionira
LOAD	LED	U tijeku je učitavanje softvera
SmartCard	Otvor za pametnu karticu	Mjesto za umetanje pametne kartice