TELSEC

CRYPTOGRAPHIC DEVICE

General

Cryptographic device TELSEC is designed to protect voice, data and video, against interception on communication channel.

TELSEC can be integrated to an existing communication infrastructure on easy way, by installing it between endpoint and telephone exchange.

Features

- Secure voice, data and video
- Diffie-Hellman 2048 key exchange
- Elliptic-curve 384 key exchange
- AES-256 symmetric encription
- SHA-3 „hash" algorithm
- Smart card user authentication
- PSK modem
- Ethernet 10/100 Mbps
- VoIP and analog telephone support
- Ethernet PC connection (DHCP)
- T.30/V.8 signaling
- TEMPEST and TAMPER protection
- Hardware random number generator

Operaton modes

VoIP	IP - Telephony	PSTN
• Secure voice and data over internet/intranet • SIP and H.323 signaling compatible • Secure video channel • Device automatically switch to this mode if direct IP communication is detected •	• G.711 voice codec • SIP and H.323 signaling compatible • T.30/V.8 signaling (fax/ modem pass-through mode) • PSK modem • Device automatically switch to VoIP mode if direct IP communication is detected	• PSK modem • Use standard 3.1 kHz channel (300 – 3400 Hz) • T.30/V8 signaling (fax/modem pass-through mode)

Pomorski centar za elektroniku d.o.o. Split

Split – Croatia
Zrinsko-Frankopanska 209

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

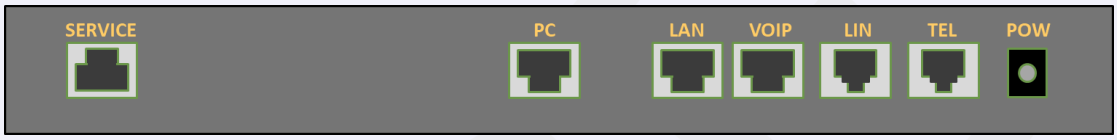
www.pce.hr
E-mail: pce@pce.hr

Functional description

Main motivation for development of **TelSec** are security concerns arising from increasing prevalence of VoIP and IP –Telephony telecommunication networks which use gateways to classical (SDH/ SONET) telephone infrastructure. Currently, there are devices that encrypt either analog or VoIP channels, thus, users that utilize both channels must implement complex communication schemes. Modern telephone exchanges usually initiate voice channel with compression. In this case, device automatically generate T.30/V.8 signaling which change audio codec to G.711 type. In this situation devices can communicate using modem signals, specially designed for this purpose.
In case of direct IP communication, device protect one voice and, if presented, one video RTP channel.

User authentication implementation is based on smart card. Complete system can be configured using our system management devices which enable client to customize user, administrator and activation smart cards.

Interfaces



Back side

Interface	Type	Description
SERVICE	RJ-45	Only for factory purpose
PC	RJ-45	Standard Ethernet 10/100 Mbps interface to PC. Using our Java application user can exchange files. Administrator is enabled to make changes in device settings.
LAN	RJ-45	Standard Ethernet 10/100 Mbps interface. Connection toward VoIP exchange/gateway.
VOIP	RJ-45	Standard Ethernet 10/100 Mbps interface. VoIP telephones (with or without video capability) can be connected to this interface. Interface support PoE type 1 and 2 as source to telephone.
LIN	RJ-11	Standard two-wire analog telephone interface to PSTN exchange.
TEL	RJ-11	Standard two-wire analog telephone interface to phone.
POW		Power supply connector (12V DC 2A).

Front side

Interface	Type	Description
POW	LED	Power LED indicator
FILE	LED	File transfer activity
VIDEO	LED	Video channel present
SEC	LED	Secure communication established
AUTH	LED	Smart card user authentication OK
RUN	LED	Software is correctly started
LOAD	LED	Software is in loading state (half light). Software loaded (full light).
SmartCard	Smart card slot	Place to insert smart card

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