

# SETEL T2 SECURE DESKTOP PHONE

ELECTRONICS DIVISION



 **LEONARDO**

SETEL Secure Phone products protect voice and data communications in digital and analog networks of armed forces government authorities and civil organisations.

SETEL Secure Phones are available in three versions:

- › T2 desktop device for use at National/NATO restricted information level
- › R2 mobile device for use at National/NATO restricted information level
- › T6 desktop also enhancing at National/NATO Secret the level of confidentiality of the exchanged information

T2 Desktop phone and data terminal provides the latest technology for both non-secure and secure end-to-end Voice over IP and in analog networks, eliminating the needs for multiple desktop phones. SCIP and Crypto Modernisation compliant, the SETEL T2 is the only VoIP phone certified to protect informations at IT National level and also supports multiple key-sets as sponsored by governments and coalitions.

This product has been developed and provided by the Setel Consortium composed by Leonardo and Telsy.

## KEY BENEFITS

- › Cost-effective, modern secure phone
- › Easy to operate and manage
- › Cross-network operations
- › Comprehensive security measures
- › State-of-the-art keys management
- › Enhanced Interoperability
- › Cloud-based secure data communications
- › Ideal replacement of former secure desktop phones
- › Future-ready

T2 phone is a single-desktop with integrated security and access control based on PIN and Smart Card/CIK. SCIP is a multinational standard for secure voice and data communication also including national and multinational modes which employ different cryptography.

SCIP may operate over the wide variety of communications systems, including commercial land line telephone, military radios, communication satellites, Voice over IP and several different cellular telephone standards.

In the range of SETEL Secure Phone Products, the customers are given the flexibility to choose the device that most efficiently protects against the most important security threats allowing them to safely share sensitive information through encrypted voice and text conversations.

By using products that have been assessed and approved by industry-independent security authorities for compliance with the high security standards posed by such organisations, individuals and organisations can make phone calls while remaining confident that their communications are protected against eavesdropping and manipulation attacks along the entire transmission path and that only the intended recipients will gain access to the information.

### **Cost-effective, modern secure phone:**

ETE encrypted operation across networks, security mechanisms on EAL5+ security token/smartcard, SCIP runs on Secure Voice communications up to NATO/National Restricted.

### **Ease of operation and manage:**

Simple to install, large and intuitive backlight display, removable smart card, remote web-based administration tool, Non-CCI item in absence of security token.

### **Cross-network operation:**

Over Analog PSTN, and VoIP/SIP IP networks with or without SCIP Protocol.

### **Comprehensive security measures:**

Simultaneous voice/data encrypted operations in VPN modes, user access control, emergency zeroizing, tamper protection, protected access to all crypto functions, up to Restricted COMSEC National/NATO level security.

### **State-of-art of keys management:**

Keys and configuration file generation via KDC-SCIP Key Distribution Centre, off-line keys distribution via USB token.

### **Enhanced interoperability:**

With government secure phones and commercial IP Phones, in SCIP clear and secure mode with SCIP-enabled devices of other NATO nations.

### **Cloud-based secure data communications:**

Proprietary VPN to Telsy Secure Cloud System (TSCS) delivering advanced data services, i.e. email exchange, file transfer, SIP server interaction.

### **Ideal replacement of former secure desktop phones:**

Smooth transition to secure VoIP by means of the easy-to-use menu as user network evolves from former secure PSTN modes.

### **Future-ready:**

Not a retrofit of older technology, integrated security, use in multiple networks, software easy-to-upgrade modular architecture, National/NATO PKI.



SETEL T2 Desktop phone provides in a single device the latest technology for secure IP, end-to-end voice over IP and analogue PSTN networks. Through a removable security token, based on a smart card, the unit delivers the highest security standard relying on EAL5+ Common Criteria. SETEL T2 Desktop Phone is protected by authentication based on password and security token preventing any unauthorized usage. As a "security token" free standalone device, the phone is not subjected to the regulations and restrictions of circulation of military classified units and still may be used to place unsecure calls, just like an ordinary desktop phone. When connected to a Personal Computer or to a ICT network, SETEL T2 Phone supports simultaneous encrypted voice and data communications to and from integrated service servers.

SETEL T2 Phone supports the following enhanced security features available in all operational modes:

- › User authentication and identification
- › Emergency Key and sensible data erasing
- › Anti-tampering
- › Event security log
- › Non-CCI item in absence of security token
- › Theft recovery
- › Self-testing and safe alarm
- › Confidentiality and integrity of the information

In PSTN operations, SETEL T2-SCIP allows:

- › Standard analogue calls in native clear mode.
- › SCIP secure calls (as per standard SCIP 214.1)

In IP/VOIP operation modes, SETEL T2-SCIP device allows:

- › Communications over IP network in native clear Mode
- › Access to private LAN, through IP network
- › SCIP secure calls (as per standard SCIP 214.2)
- › SAMMS Management
- › Data transfer protection with Secure Cloud System

During SCIP operations, the unit supports the new market-emerging features as:

- › Simultaneous voice call and data transfer
- › Communications in SCIP clear and SCIP crypto mode over IP and PSTN networks, compliant to SCIP 210, SCIP 214.1 and SCIP 214.2
- › Compliance with SCIP 233 for end-to-end NATO/ National approved encrypted voice and data
- › Interoperability with other SCIP devices on mobile networks or military infrastructural networks
- › Interoperability, in clear and secure mode, with SCIP devices of other NATO Nations
- › Interoperability with all Leonardo SETEL Phones

The remote web-based administration tool is an easy-to-use secure data terminal enabling configuration and monitoring of SETEL networks. The administration tool is composed by the following subsystems:

- › Secure Cloud System (SCS)
- › SCIP Application Monitoring Management System (SAMMS)



In addition, the Key Distribution Centre (KDC) completes the SETEL SW Suite.

SCS represents the enhanced communication infrastructure able to provide security functionalities as VPN Concentrator and Firewalling and enhanced data services as e-mail server, file data transfer server and SIP server.

SAMMS Application provides dedicated SCIP devices management including monitoring and provisioning operations. SAMMS is designed for future interoperability with National and NATO PKI. KDC is the management system of the SCIP cryptographic credentials, keys and certificates, for National and NATO classified communications.

#### PHONE BASIC FEATURES:

- › Multi-language programmable messages
- › Rapid call menu
- › Programmable telephone directory
- › Last Number Redial
- › Loudspeaker listening
- › Audio Control: Selectable ringtone, Speakerphone, Volume controls, Mute
- › 480x272 pixels graphic colour 4.3" resistive touch-screen display
- › Visual Display: Call History log, Time and Date

## TECHNICAL DESCRIPTION

### FORM FACTOR

- › Dimensions: 230mm x 200mm x 80mm
- › Weight: 2.6kg

### POWER

- › PoE (Power over Ethernet) or external power source at 9-36 Vdc
- › AC Power option 110 to 220 VAC
- › Power consumption < 4W

### COMMUNICATION INTERFACES

- › 2 x 10/100BASE-T RJ-45 connector
- › 1 X FXO RJ-11 connector
- › 2 USB ports

### ENVIRONMENTAL

- › Operation 0°C to + 50°C
- › Storage - 20°C to + 70°C
- › Humidity 20% to 95% non-condensing
- › MIL-STD-810F for temperature, humidity, vibration, shock and altitude

### NETWORK OPERATIONAL MODES

- › Analogue PSTN Standard mode
- › VoIP over IP mode
- › Clear and Secure SCIP over IP and PSTN network modes

### VOICE COMMUNICATIONS

- › Speech Processing/Vocoders Non Secure G.711, G.729A  
Secure G.729 D @6.4kbps,  
MELPe @2.4kbps
- › IP/VoIP Secure Operations Full-duplex over IP networks  
Call in clear to standard  
VoIP telephones
- › SCIP Secure Operations SCIP 210 “Blank & Burst”  
and “Burst w\o Blank” modes  
Protocol SCIP214.2 “SCIP  
over RTP” (RFC3261, RFC  
1889, RFC 4566)

### DATA COMMUNICATIONS

- › Secure Data Rate Maximum 100 kb/s

### IP/VOIP COMMUNICATION PROTOCOLS

- › IETF SIP, RFC 3261
- › DHCP, Ipv4, ipv6 (upgradable), RTP

### SCIP COMMUNICATION PROTOCOLS

- › SCIP 210 ,SCIP 214.1, SCIP 214.2; SCIP 214.3
- › SCIP 233
- › SCIP 221 Rev3

### CRYPTO HARDWARE

- › Physical RNG According to FIPS PUB 140-2
- › Security Token ISO7816, EAL 5+

### CRYPTOGRAPHIC ALGORITHMS

- › Suite (Type) B

### KEY MANAGEMENT

- › Keys and configuration files generation via KDC
- › Off-line key distribution
- › Multi-Profiles Automatic SCIP Keyset selection

### ACCESS CONTROL/ SECURITY MECHANISMS

- › Two-factor authentication to the security token by means of password
- › Zeroize by a hardware dedicated function

### INTEROPERABILITY

- › SETEL Desktop and Mobile Phones
- › Interoperable with all standard products from competing companies compliant with standard specifications in all supported network operational modes

For more information:  
infomarketing@leonardocompany.com



leonardocompany.com

Electronics Division  
Via Tiburtina  
Km 12.400  
00131 Rome - Italy  
T +39 06 41501  
F +39 06 4131133

This publication is issued to provide outline information only and is supplied without liability for errors or omissions. No part of it may be reproduced or used unless authorised in writing. We reserve the right to modify or revise all or part of this document without notice.

2020 © Leonardo Sp.A.

MT00021 03-21

