# TACEK

## Portable Offline Crypto Equipment

TÜBİTAK
BİLGEM
CENTER OF RESEARCH FOR ADVANCED TECHNOLOGIES OF INFORMATICS AND INFORMATION SECURITY


## OFFLINE FILE ENCRYPTION SYSTEM

TACEK system secures files at any confidentiality level including COSMIC TOP SECRET by encrypting. Files encrypted by TACEK can be stored and sent through public communication channels safely. A message, document or data file that resides on a USB mass storage device or CD/DVD can be encrypted and decrypted at high speeds.

Organizational roles and their assignment to equipments are managed in the Key Management Center. On the equipment association of these entities to real users are managed by the local administrator. The user who encrypts the files determines the one or more organizational roles that are allowed to decrypt the file. For a user to be able to perform encryption or decryption tasks as one of the system wide entities: 1. this entity must have been assigned to the equipment in the Key Management Center, and 2. the user should have been assigned as a representative of the entity by the local administrator. User access control can optionally be done by fingerprints and smartcards besides the default complex password control. The events are logged (in encrypted form) on the equipment. When needed these logs can be examined and exported by the centrally defined auditor user.

Critical controls (such as user access control, entity-user assignment control, alarm situation control, data integrity checks) are performed by crypto module in hardware. Moreover all red cryptographic variables are handled and stored in such a way that software has no option to decrypt or see their contents. Red and black data is processed in electrically separate modules on the equipment. The crypto module lies in between the module that process the black data and the module that process red data, connecting them to each other. Therefore it is not possible for red data to go to black side without encryption. There are 2 USB ports on red side, 1 USB ports on black side. The devices used on these ports are labeled electronically by the equipment to prevent a possible later incorrect usage (black medium to red port and vice-a-versa).

The initialization key material is loaded to the equipment by secure key fill devices, which is compatible with national and NATO systems. Periodic keys are distributed in encrypted form and loading is carried out by local administrator, using a CD/DVD or USB-mass storage device.

The equipment is mechanically and electronically designed to fulfill the SDIP-27 Level-A standard.

# COMMUNICATION AND INFORMATION ASSURANCE

| TECHNICAL SPESIFICATIONS | |
|---|---|
| General Features | Portable Equipment with folding LCD Monitor and Internal Battery |
| Security Features | Red - Black Separation<br>All critical controls are performed by crypto hardware<br>Red keys can only be accessed by crypto hardware<br>Emergency erase of keys<br>Security logs |
| Processor | Red: ETX-CD 1.66 GHz Dual Core Low Power, 1 GB DDR-RAM<br>Black: BlackFin DSP Processor<br>Key Control: ARM-9 Processor |
| Ciphering | 2 GB data encryption/decryption |
| Ciphering Rate | 80 Mbit/sec |
| Keys | Initialization with NATO and National Systems compatible "Secure Key Fill Device"<br>Black key distribution<br>Key storage for at least 1 month, when not powered |
| Access Control | Password, Smart Card (Optional), Fingerprint (Optional) |
| I/O Interfaces | One USB 2.0 High-Speed I/O Interface at Black Side<br>Two USB 2.0 High-Speed I/O Interfaces at Red Side<br>DS101 Interface for key loading<br>100Mbps Ethernet Interface at Red Side |
| Updates | Ciphered Software Updates with signature verification |
| TEMPEST EMI/EMC | SDIP-27 Level-A |
| User Interface | 12" LCD Monitor<br>Turkish Keypad<br>Internal Touch-pad<br>Ability to connect external monitor, USB mouse/Keypad<br>Easy to use graphical interface |
| Power Supply | Compatible with 9-36V DC input<br>90-220VAC 47-63 Hz Adapter with 24V DC output<br>Internal Battery (minimum 30 minutes standalone operation time) |
| Environmental Conditions | Operating Temperature: 0 ~ 50°C<br>Storage Temperature: -20 ~ 65°C<br>Relative Humidity: %90 at +40°C |
| Physical Dimensions | 330mm x 285mm x 85mm (w x d x h)<br>< 9 Kg<br>Suitable for desktop usage |
| Due to continuous improvement studies, these spesifications are subject to change without notice. | |

TUBITAK BILGEM UEKAE
T: +90262 648 1000 • F: +90262 648 1100 • E: bilgem@bilgem.tubitak.gov.tr
W: http://www.bilgem.tubitak.gov.tr • A: P.BOX: 74, 41470, Gebze, Kocaeli, TURKEY