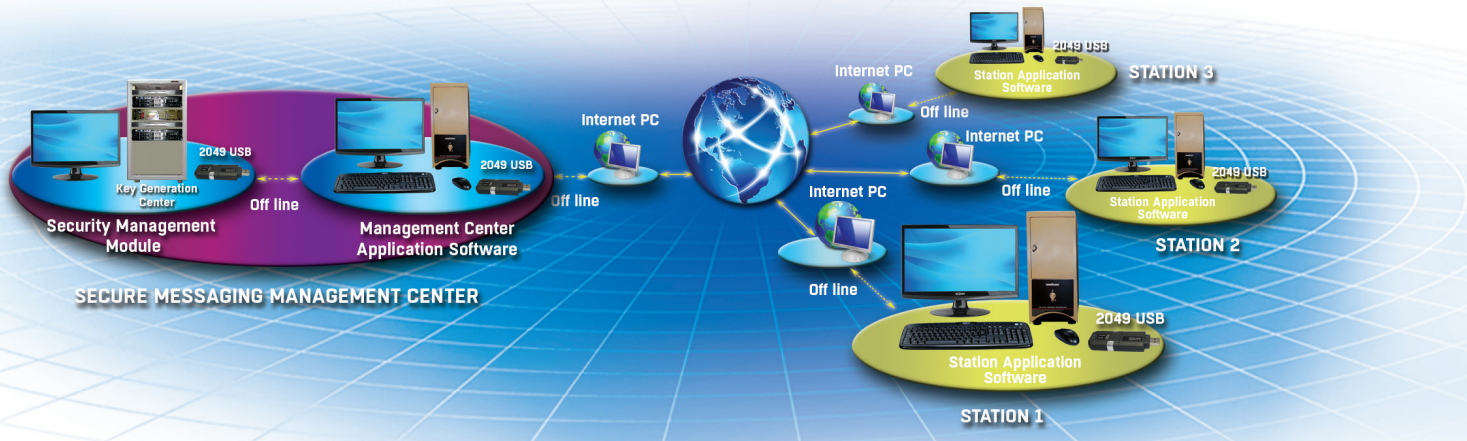
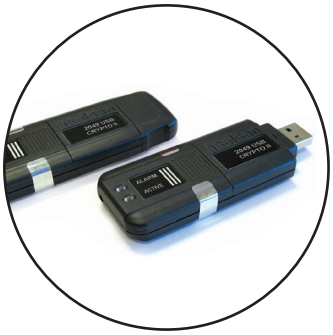
aselsan

SMS

SECURE MESSAGING SYSTEM





SMS

Secure Messaging System

Secure Messaging System is the system which consists of hardware and software providing the secure communication between terminals. SMS provides a secure messaging using Public Key Infrastructure (PKI) comprising ASELSAN 2049 USB Module, user application software and Key Management System (KMS) where user/certificate management is achieved.

In Secure Messaging System's Station, one computer, one 2049 USB Encryption crypto equipment, Crypto Ignition Keys(CIKs) and Station Application Software exist. In this system, public certificates of the users and stations are send via e-mail to active stations. After encrypted and signatured file transferred via internet medium by e-mail, only the users in the list can decrypt the file by using their own 2049 USB crypto equipment and CIKs.

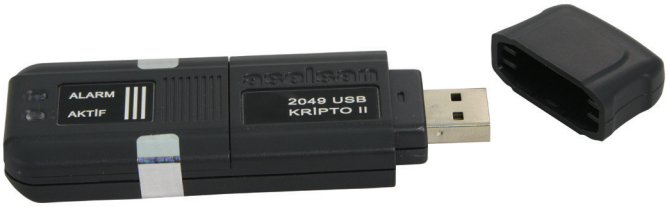
- All managing activities are achieved in Security Management Module
- Offline encryption over the "Secret" data in the PC
- All processes done by the users and the alarms occurred on the 2049 USB Module are stored on the database as encrypted
- For file encryption, symmetric algorithm AES 256 is used
- For Hash Functions SHA-256 Algorithm is implemented
- For asymmetric encryption and electronic signature NIST Elliptic Curve is applied

2049 USB Device Technical Features

USB Compatibility	USB 2.0 Full Speed
Dimensions	~95.5mm x 32.5mm x 13.5mm
Operating System	Windows, Linux, Android
User Interface	User Friendly Application Software

Security Features

- Supporting different algorithms
- Hardware implemented algorithm (on FPGA)
- Public Key Infrastructure (PKI) for the generation of key and certificate
- Emergency zeroization function
- User access control with Crypto Igniton Key (CIK)
- ECDSA digital signature algorithm
- Secure delete feature



2049 USB DEVICE

P: +90 (312) 592 10 00 | **F**: +90 (312) 354 13 02 | hbtmarketing@aselsan.com.tr