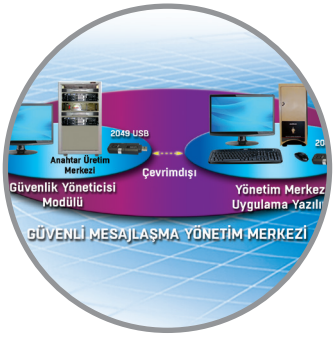
aselsan

# 2049 GÜMES

## GÜVENLİ MESAJLAŞMA SİSTEMİ


GÜVENLİ MESAJLAŞMA SİSTEMİ

www.aselsan.com.tr




# 2049 GÜMES

## Güvenli Mesajlaşma Sistemi

GÜMES, birimler arasında çevrimdışı açık anahtar altyapısı kullanılarak güvenli mesajlaşmayı sağlayan ASELSAN 2049 USB modülü, kullanıcı arayüz yazılımı ve kullanıcı/sertifika yönetiminin gerçekleştirildiği Anahtar Üretim Merkezi'nden (AÜM) oluşan sistem çözümüdür.

Sistemin temel işlevi "GİZLİ" gizlilik seviyesine sahip bilgisayar üzerinde bulunan verileri çevrimdışı (offline) şifrelemek ve GÜMES üzerinde tanımlı kullanıcılara dağıtmaktır. Şifreleme ve şifre çözme işlemi, herhangi bir ağa bağlı olmayan, bağımsız bilgisayarlarda yapılmaktadır. Sistemde kullanıcıların yaptığı tüm işlemler ve 2049 USB modülü üzerinde oluşan alarmlar veritabanında kriptolu saklanmaktadır.

- Dosya kriptolama için AES-256 simetrik algoritması,
- Hash fonksiyonları için SHA-256 algoritması,
- Asimetrik kriptolama ve elektronik imza işlemleri için NIST Eliptik Eğri kullanılmaktadır.

### 2049 USB Cihazı Teknik Özellikleri

| | |
|---|---|
| USB Uyumluluğu | USB 2.0 Full Speed |
| Boyut | ~95.5mm x 32.5mm x 13.5mm |
| İşletim Sistemi | Windows |
| Kullanıcı Arayüzü | Kolay kullanımlı PC arayüzü |

### Güvenlik Özellikleri

- Farklı algoritmalara destek
- Donanımsal algoritma(FPGA üzerinde)
- Anahtar ve sertifika üretimi için Açık Anahtar Altyapısı
- Acil silme işlevi
- Elektronik Kimlik Modülü(EKİM) ile kullanıcı erişim denetimi
- ECDSA sayısal imza algoritması
- TEMPEST standartlarına uygunluk
- Güvenli silme(Secure Delete) yazılımı


2049 USB CİHAZI



**T**: 0 (312) 592 10 00 | **F**: 0 (312) 354 13 02 | hbtmarketing@aselsan.com.tr