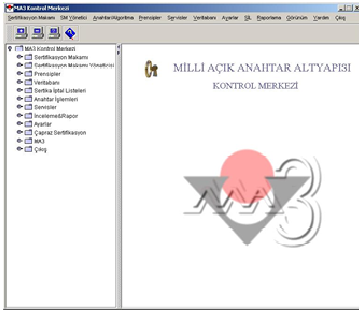


MA3

Milli Açık Anahtar Altyapısı

Veri güvenliği çözümleri...

“Açık Anahtar” tekniği kullanılarak, ağ uygulamalarına yüksek düzeyli güvenilir bir emniyet ortamının altyapısını sunar.



- *Veri Bütünlüğü*
 - *Kimlik Doğrulama*
 - *İnkâr Edememe*
 - *Gizlilik*
- temel güvenlik ilkelerini yerine getirir.*



Sertifikasyon Makamı (Güvenilir Üçüncü Taraf) yardımı ile gerekli olan anahtar ve sertifikaların oluşturulmasını, güvenli şekilde dağıtılmasını ve belirlenen prensiplerin sistemde uygulanmasını sağlar.

Prensipier çerçevesinde istemcilerden gelen sertifika isteği üzerine veya Web üzerinden sertifika dağıtımını gerçekleştirir.

MA3, sayısal imza ve ağ üzerinde veri güvenliğinin kullanıcıyı yormadan, uluslararası standartlar çerçevesinde, milli olarak gerçekleşmesidir. Ağ uygulamalarına kolayca entegre edilebilir.



Teknik Özellikler

MA3

Milli Açık Anahtar Altyapısı

Uygulama Alanları

- Sayısal imza
- E-mail güvenliği
- Web güvenliği
- VPN Anahtar dağıtımı

Modüller

- Sertifikasyon Makamı
- MA3 sisteminde kullanılan tüm sertifikaları üreten, imzalayan, prensip ve politikaların uygulanmasını sağlayan yazılımdır. Güvenilir Üçüncü Taraf (Trusted Third Party) görevini yerine getirir.
- Emniyetli Elektronik Posta Modülü (EPM)
- İstemci tarafında sayısal sertifikalar kullanımı ile güvenli haberleşmesini sağlar. MA3 Sertifikasyon Makamı ile on-line bağlantısı sayesinde kullanıcıların AAA'ya entegrasyonunu sağlar. İstemci Modülü
- İstemci tarafında AAA'ya entegrasyonunu sağlayarak, Sayısal Sertifika kotarma ve masaüstü dosya şifreleme işlevlerini yerine getirir.Emniyetli WEB Sistemi
- Temel Güvenlik İlkeleri'nin WEB ortamında uygulanmasını sağlar.

Desteklenen Standartlar

- X509 v3 Sertifika Standardı
- PKCS #1, #5, #7, #8, #10, #11
- RFC 822, 2510, 2511, 2459
- X500 Dizin Standardı
- LDAP v2, v3
- X509 CRL v2S/MIME v2, v3
- TLS,SSL v2,v3

Desteklenen Algoritmalar

- RSA, DSA, SHA-1, MD5, RC2, RC4, DES, TripleDES, Fortezza, Milli Algoritmalar

TÜBİTAK-UEKAE
ULUSAL ELEKTRONİK VE KRİPTOLOJİ ARAŞTIRMA ENSTİTÜSÜ



TÜBİTAK-UEKAE
ULUSAL ELEKTRONİK VE KRİPTOLOJİ ARAŞTIRMA ENSTİTÜSÜ

P.K. 74
41470 Gebze/Kocaeli
TÜRKİYE

Tel : (262) 648 1000

Faks : (262) 648 1100

e-posta : uekae@uekae.tubitak.gov.tr