



Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

Çağrı KOÇ

Haziran 2008, Ankara

Çalışma Alanları:

Bilgi güvenliği, haberleşme ve ileri elektronik

Amaç:

Türkiye'nin teknolojik bağımsızlığını sağlamak, sürdürmek ve rekabet gücünü arttırmak

Sonuç:

Tamamen milli ve özgün olarak geliştirilen ulusal yazılım, cihaz ve sistemler



Bilgi Güvenliği

Kriptoanaliz Merkezi (KAM)

Elektromanyetik ve TEMPEST Test Merkezi (ETTM)

Yazılım Donanım Ortak Kriter Test Merkezi (OKTEM)

Akustik Test Merkezi

Ürün Geliştirme Proje Grupları

Elektronik Harp (İLTAREN)

Mikroelektronik (YİTAL)

Optoelektronik

Kamu Sertifikasyon Merkezi



**Kriptoanaliz
Merkezi
(KAM)**



**EMI/EMC Tempest
Test Merkezi
(ETTM)**



**Yazılım/Donanım
Ortak Kriter Test Merkezi
(OKTEM)**



**Akustik
Test Merkezi**



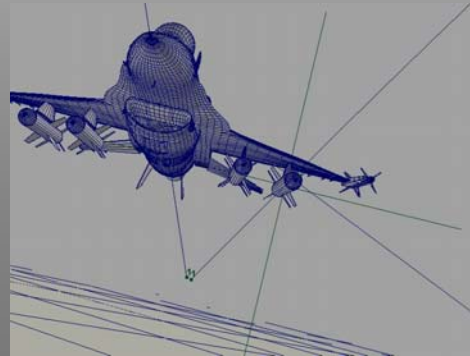
- TSK tarafından desteklenen kurulum projeleri
- İşletim esaslarını düzenleyen özel protokollar
- Kamu / özel sektör ihtiyaçlarını karşılamak üzere sunulan hizmetler
- ETTM ve OKTEM'in ISO 170025 TÜRKAK akreditasyon belgesi

Yazılım Geliştirme Altyapıları

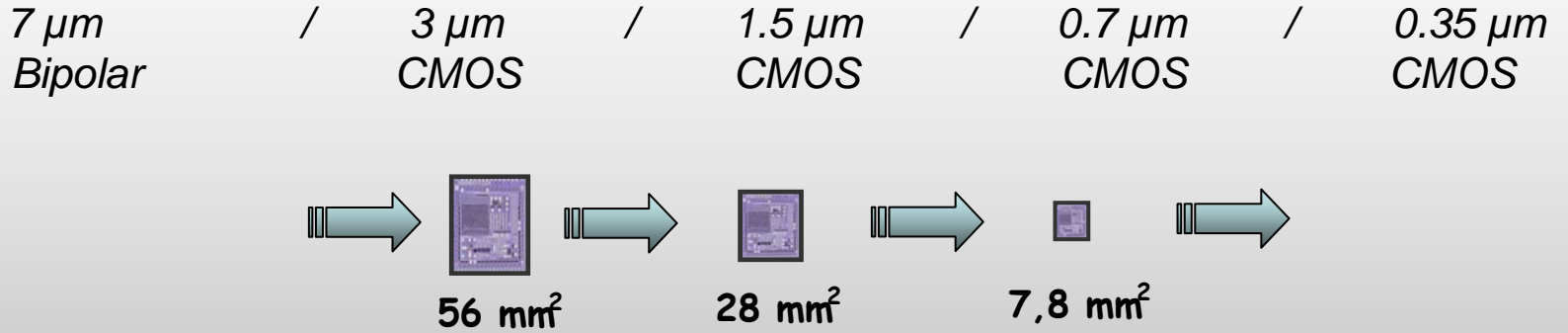
- Stratejik / Operatif Seviyeli Uygulamalar
- Taktik Seviyeli Uygulamalar
- Diğer Karar Destek Maksatlı Uygulamalar

Sistem Geliştirme Altyapıları

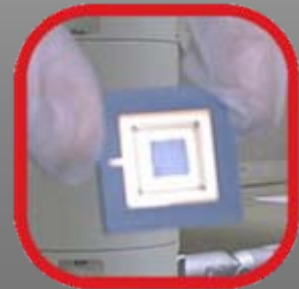
- Açık Çevrim Ölçüm Sistemleri
- Kapalı Çevrim Laboratuvar Test Düzenekleri
- RF / KÖ Test ve Değerlendirme Laboratuvarları
- EH Sistem Prototiplerinin Geliştirilmesi



Tümdevre üretim teknolojisi :



Halen TSK envanterinde olan ve gelecekte kullanılacak bütün kripto tümdevreleri Yarıiletken Teknolojileri Araştırma Laboratuvarı'nda (YİTAL) ÖZGÜN olarak tasarlanmakta ve üretilmektedir.



3 Eylül 2004 tarihli ve 21 numaralı Başbakanlık Genelgesi ile, **Kamu Sertifikasyon Yapısı'nın kurulması ve işletilmesi görev ve sorumluluğu** UEKAE'ye verilmiştir.

1 Temmuz 2005 tarihi itibarıyla KSM aktif duruma gelmiş ve sertifika dağıtımına başlamıştır.





Ürün Yelpazesi

Veri Kripto Cihazları

MİLON-I, MİLON-II, MİLON-III, MİLON-IV

MİLON-5, MİLON-6, MİLON-7

IP Kripto Cihazları : IPKC-E, AGC-100T

ISDN Kripto Cihazları : ISDN-BRI, ISDN-PRI, ISDN Telefon

Ses Emniyet Cihazları

MİLSEC-1, MİLSEC-2, MİLSEC-1S

MİLSEC-3 : NATO KY-58 eşdeğeri

Kriptolu Cep Telefonu

Off-line Kripto Cihazı

MİLOF-1

Dost-Düşman Tanıma Cihazları

IFF Mod4 Kripto Modülü

IFF Mod5 Kripto Modülü – sürüyor

Kripto Anahtarı Üretim, Dağıtım ve Yönetim Sistemleri

TELAYS – TAFICS Elektronik Anahtar Yönetim Sistemi

EKADAS – Elektronik Kripto Anahtar Dağıtım Sistemi

Anahtar Yükleme Cihazları

KAOC-8, KAYC-10, KAYC-32, KAYC-S

HF İletişim Ürünleri (FORMUS-Farklı Ortamlarda Muhabere Sistemi)

FORESC : FORMUS Erişim ve Sunucu Cihazı

FORBİS : FORMUS Bilgi İletim Sistemi

FORGEC : FORMUS Ağ Geçit Cihazı

HELİS : Helikopter İşletim Sistemi

Radar Ürünleri

SAGRAD : Sahil Gözetleme Radarı (Sahil Güvenlik Komutanlığı ihtiyacı için)

GEMRAD : Gemi Radarı (Deniz Kuvvetleri Komutanlığı ihtiyacı için)

GETRAD : Gemi Takip Radarı (Denizcilik Müsteşarlığı ihtiyacı için)

Sayısal Radyolink Cihazları

PDH Radyolink Cihazları – SRL5800A, SRL5800Q, SRC8000A, SRC8000Q

SDH Radyolink Cihazı – sürüyor

Optik İletişim Cihazları

Açık Anahtar Altyapısı (MA3)

Güvenlik Duvarı Yazılımı

Akıllı Kart İşletim Sistemi – AKİS

AKİS – Nitelikli Elektronik İmza ve Güvenlik

AKİS Para – Bankacılık sektörü, EMV onayı almış, kontaklı-kontaksız

AKİS GSM – GSM SIM kartı

Ulusal İşletim Sistemi – PARDUS

Milli Frekans Yönetim Sistemi – MARSSys

TEMPEST İşaret ve Güç Hattı Filtreleri

GSM Karıştırıcılar

Simülasyon Yazılımları

Ulusal Marker Kontrol Cihazı

Optoelektronik Ürünler

Doküman İnceleme Cihazları

Cam Gerilim Ölçme Cihazları

Lazerli Otomatik Cam Kontrol Sistemi

Lazerli Otomatik Kumaş Kontrol Cihazı

Genişlik Algılama Sistemleri

Renk Algılama Sistemleri

Spektrofotometrik Renk Uygunluk Makinesi

Mikro Spektral Tarayıcı

Olay Yeri Aydınlatma Cihaz Seti



Örnek Projeler

- Tamamen ulusal tasarım
- Ön planda tutulan bilgi güvenliği ilkeleri
- ISO 7816 uyumlu güvenli veri alışverişi
- Güvenli bilgi saklama özelliği
- Şifreleme yöntemi ve anahtar uzunluğu seçebilme özelliği
- Elektronik imza uyumluluğu
- CC EAL 4+ düzeyinde güvenlik onayı



-Kullanımda-

Melez/Çift Arayüzlü kartlar için AKİS

- ISO 7816 ve ISO 14443A-B standardına uygun tasarım
- e-Pasaport (ISO 7816) ve Başkacılık işlemleri (EMV) dahil bütün uygulamaları güvenli şekilde çalıştıracak donanım
- Özgün tekniklerle gerçekleştirilen iletişim güvenliği

- 2008 sonu -

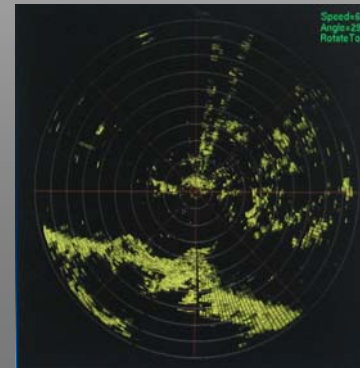
Aralık 2005	: PARDUS 1.0
Aralık 2006	: PARDUS 2007
Mart 2007	: PARDUS 2007.1 FelisChaus
Temmuz 2007	: PARDUS 2007.2 Caracal Caracal
Kasım 2007	: PARDUS 2007.2 Lynx Lynx
Haziran 2008	: PARDUS 2008



Açık kaynaklı yayımlanmakta, Genel Kamu Lisansı (GPL) ile dağıtılmaktadır.

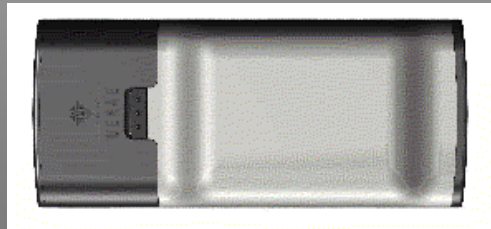
PARDUS, ofis araçları, internet araçları, çokluortam ve grafik araçları, oyunlar ve çok sayıda uygulama içermektedir.

- **SAGRAD** Sahil Gözetleme Radarı
 - Üretim prototipi tamamlandı.
- **GEMRAD** Gemi Radarı (MİLGEM LPI radar)
 - Üretim prototipi tamamlandı.
- **GETRAD** Gemi Takip Radarı (GTHS radarı)
 - Çalışmalar devam ediyor.

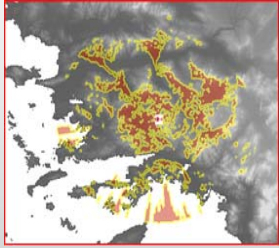


Mobil iletiřimi kriptolayarak gvenliđini sađlamak zere geliřtirildi.

Tamamen zgn tasarım donanım ve yazılım iđermetedir.

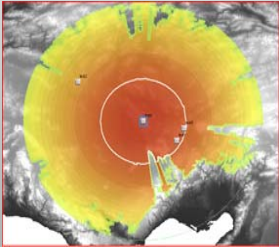


Management and Analysis Of Radio Spectrum System



Geniş frekans bantlı ve kapsamlı

TSK teçhizat envanter veritabanını içeren



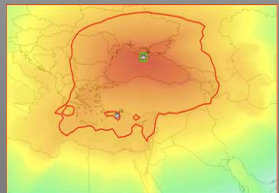
Coğrafi Bilgi Sistemi tabanlı

XML veri altyapısına sahip

NATO SMADEF uyumlu ilk ve tek Frekans Yönetim Sistemi



NATO SMADEX / 2008 uyumlu olacak



NATO ARCADE İhalesini Kazandı

- 100 Ulusal Radyo ve 100 Ulusal TV ile il ve ilçelerden gelecek toplam 210 TV ve 860 radyo yayınının kayıt altına alınması, arşivlenmesi ve bu kayıtların üzerinde istenen analizlerin yapılması
- İkinci aşamada 400 TV ve 1500 radyo yayını



- UEKAE sorumluluğundaki eylem maddeleri
 - [74] Kamuda Açık Kaynak Kodlu Yazılım Kullanımı
 - [88] Ulusal Bilgi Sistemleri Güvenliği Programı
- UEKAE'nin ilgili olduğu eylem maddeleri
 - [10] İnternet Güvenliği
 - [26] e-ticaret Güvenlik Altyapısı
 - [32] Sağlık Bilgi Sisteminin Kurulması
 - [46] Vatandaşlık Kartı, Pilot Uygulaması ve Yaygınlaştırılması
 - [62] Ulaştırma Sistemlerinde e-ödeme Standartları
 - [70] Kamu Güvenli Ağı
 - [76] Bilgi Sistemleri Olağanüstü Durum Yönetim Merkezi
 - [83] e-imza Kullanımının Artırılması
 - [87] Bilgi Güvenliği ile İlgili Yasal Düzenlemeler

- DPT projesi
- Kamu kurumları bilgi sistem güvenliđi gereksinimlerinin belirlenmesi
- Gereksinimlerin pilot projeler ile uygulamaya geçirilmesi
- Çalışmanın kamu kurumları geneline yayılması

- Bilgi Güvenliđi Yönetim Sistemleri
- Güvenlik Test ve Deđerlendirmesi
- Sızma Testleri
- Güvenli Sistem Kurulumu
- İş Sürekliliđi Çalışmaları (Olası Kaza ve Felaketlere Hazırlık)
- Ortak Kriter (CC) Standardı Deđerlendirmesi
- Haberleşme Güvenliđi (COMSEC) Deđerlendirmesi
- Güvenlik Eğitimleri



Yurtdışı ve NATO ile İlişkiler

NATO Çalışmaları

- NATO SC/4 ve SC/7 etkinliklerine aktif katılım
- RTO, CNAD and NATO Bilim Komitesi'ne katılım
- NATO tatbikatlarında güvenli deniz iletişiminin sağlanması
- NATO onaylı kriptografik ürün ve algoritmalar
- NATO'da kullanıma giren UEKAE ürünleri

Geleceğin Büyük Uçağı (FLA) Projesi

- Bilgi güvenliği ve TEMPEST

Joint Strike Fighter (F35) Projesi

- Bilgi güvenliği

Avrupa Birliği Çerçeve Programı Projeleri

- 6.ÇP projeleri
- 7.ÇP projeleri

BLACKSEAFOR Tatbikatlarına Aktif Katılım

- Tatbikatlarda güvenlik anlamında başvuru noktası ve destek

NATO UNCLASSIFIED



Allied Maritime Component Command
Naples
Via Nuova Nisida No1
80124 Naples
Italy



IVSN: 433 6310
Comm: 0039 081 721 6333

2033.56/NSCEF/05

TO: Mr Yonder Yetis
Manager of the Institute
TUBITAK UAKAE
National Research Institute of Electronics & Cryptology
Gebze
Kocaeli
TURKEY

SUBJECT: EVALUATION OF FORESC DURING PASSEX DEPLOYMENT
ONBOARD RBSF MOSKVA AND SPS NAVARA

DATE: 24 February 2006

1. I would like to take this opportunity to express my sincere gratitude to the team of technicians consisting of Mr Kiziltan, Cikikci, Akyol, Recep and Uslu deployed to the Russian Black Sea Fleet unit MOSKVA from 8 – 16 February 2006.
2. Their sterling efforts and high degree of co-operation to the CC-MAR Mobile Training Team, with particular regard to the members of the team from N6, in the fitting, setting to work and the subsequent conduct of the operational trials onboard the MOSKVA. Not all was plain sailing, but your technicians took the adversities in their stride, using innovative solutions and ideas to ensure that the trials were a resounding success.
3. It is through their efforts that the milestone achievement has been made of the first secure communications between a Russian and NATO ship, a truly historic event.



R D Leaman OBE
Rear Admiral UKN
Chief of Staff

2007 yılında 10 takım
FORESC, MİLON-4A, KAYC-10, KAOC-8 satışı



Türkiye'den NATO envanterine giren ilk bilgi güvenliği cihaz seti

SECAN tarafından Onaylanmış Ürünler

- Tüm Gizlilik Düzeylerinde Kullanım için Kripto Algoritmaları (SEA, İNAL)
- On-line Veri Kripto Cihazları
MİLON-4A,
ISDN-BRI kripto cihazı,
ISDN-PRI kripto cihazı,
ISDN telefon
- Off-line Veri Kripto Cihazı (MİLOF)
- Anahtar Yükleme Cihazları (KAYC-10, KAOC-8)



Onay Süreci Devam Edenler

- Kripto Algoritması (OCEAN)
- Kriptolu USB Bellek

Onay Süreci Başlayacak Olanlar

- Elektronik Kripto Anahtar Üretim ve Yönetim Sistemi
- Yeni Nesil IP Kripto Cihazı

- Milli Gizli Gizlilik Dereceli Tesis Güvenlik Belgesi
- NATO Gizli Gizlilik Dereceli Tesis Güvenlik Belgesi
- ISO 9001:2000 Kalite Belgesi
- ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemi (KSM)
- ISO 17025 TURKAK Akreditasyon Belgesi (ETTM)
- ISO 17025 TURKAK Akreditasyon Belgesi (OKTEM)
- AQAP 2110 Kalite Belgesi
- AQAP 2130 Kalite Belgesi
- AQAP 160 Kalite Belgesi
- Üretim İzin Belgesi



- Bilgi güvenliği konusunda tam bağımsızlık
- Ülke ekonomisine sağlanan yüz milyonlarca doları aşmış katkı
- Üstün yetenekli araştırmacılara istihdam imkanı

Müşteri İlişkileri ve İş Geliştirme Bölümü

T : (0262) 648 1000, (0262) 648 1163

F : (0262) 648 1100

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