TÜBİTAK Informatics and Information Security Research Center (BİLGEM) is a R&D center of Turkey which provides the country with innovative and original solutions on informatics, information and advanced electronics. With its experience exceeding 40 years and human resources surpassing 1700, BİLGEM conducts scientific and technological researches in compliance with international standards.

The institutes within TÜBİTAK BİLGEM have so far attained a remarkable number of successful projects in the fields of information technologies, information security, electronic intelligence, electronic warfare, cyber security, software technologies and cryptology. These institutes are namely the National Research Institute of Electronics and Cryptology (UEKAE), Information Technologies Institute (BTE), Advanced Technologies Research Institute (İLTAREN), Cyber Security Institute (SGE) and Software Technologies Research Institute (YTE).

Thanks to the projects of these institutes, Turkey has become one of the few countries declaring its independence in the areas of informatics and information security.

Products and technological solutions developed by BİLGEM have reached beyond the country’s borders, being used by many European and Asian countries along with NATO. Thanks to these contributions of the Center, Turkey has become an exporting and competing country in the areas of informatics and information security.

This catalog hereby aims to make you much familiar with the technologies and solutions developed within TÜBİTAK BİLGEM.
BİLGEM, operating in the fields of information technologies, information security and advanced electronics, stands out as the biggest and one of the most important research centers of TÜBİTAK.
BİLGEM, founded in 1968 under the name of Electronics Research Unit (ERU), is the most efficient R&D center of Turkey.
BİLGEM conducts technological R&D activities for Turkey’s technological independence in the fields of information security and informatics, and for the maintenance and advancement of military and civilian information’s security and integrity.
With its personnel exceeding 1700, BİLGEM has 6 institutes mainly operating in the fields of advanced electronics, information technologies, cryptology, cyber security, software technologies, information security, electronic warfare and telecommunication.
BİLGEM FIELDS OF OPERATION

The center produces national solutions for both military and civilian needs within the context of information systems and technologies.

- Information Technologies
- Information Security Systems
- Cryptology Systems
- Cyber Security Technologies
- Secure Communications Technologies
- Homeland Security Systems
- Explosive Detection Systems
- Electronic Warfare Technologies
- Underwater Defense Systems
- RF and Microwave Systems
- Radar Systems
- Antenna Systems
BİLGEM develops original and high value-added technologies in order to sustain the competitive capacity of the country/Turkey for high-tech products.
BİLGEM LABORATORIES WITHIN TESTING AND EVALUATION VICE PRESIDENCY

BİLGEM, with the technological laboratories forming its infrastructure, meets technological needs of the country and has a huge impact on the current technology abroad.
UEKAE / NATIONAL RESEARCH INSTITUTE OF ELECTRONICS AND CRYPTOLOGY

National Research Institute of Electronics and Cryptology (UEKAE) is a R&D organization which develops information security and electronic system projects that are vital for strategic public institutions. Additionally, making significant contributions to Turkey’s ability in information security, UEKAE aims at decreasing foreign dependency of the country. For this end, every critical part in strategic devices from general design to manufacturing of integrated circuits is developed within the institute.

UEKAE carries out its projects by using state-of-the-art methods and technology with more than 40 years of experience, professional manpower, advanced laboratories and test systems, secure facilities, quality and process infrastructures approved by ISO, AQAP and CMMI.

Moreover, UEKAE has Turkey’s largest library in cryptology and information security.

BTE / INFORMATION TECHNOLOGIES INSTITUTE

Information Technologies Institute (BTE) within TÜBİTAK BİLGEM aims at improving welfare and security of the public through the realization of projects in the areas of Intelligent Transportation Systems, Homeland Security, Defence Technologies, and Sensor and Radar Systems. With its experience exceeding 20 years, the Institute has to date realized many projects for both the private and public sectors, universities and research institutes, and has made notable contributions to the information technologies sector.

In compliance with BİLGEM’s strategic mission, BTE adopts a customer driven project-based approach. The institute was also appraised to CMMI Maturity Level 3 in 2008. Additionally, BTE holds NATO AQAP 160 (NATO Integrated Quality Requirements for Software throughout the Life Cycle) certification.

İLTAREN / ADVANCED TECHNOLOGIES RESEARCH INSTITUTE

Advanced Technologies Research Institute (İLTAREN) is an institute operating in the field of Electronic Warfare (EW).

Its research activities mainly focus on the fields of modelling and simulation, spectrum management and also the development of embedded system prototypes as part of RF, IR optical systems. Apart from its software development activities, laboratory structures, which include system prototypes of Electronic Warfare and hardware elements of these systems, are developed within the institute. Wide-ranging activities are also carried out in the field of submarine defence. These activities are as follows: Submarine combat management system, submarine active/passive sonars, expendable acoustic counter measure systems that are launched from submarine launchers, light/heavy torpedo models, dynamic modelling, usage of decision support system for tactical pictures including torpedo, solution of fire control problem within submarines along with the activities regarding target motion analysis.
SGE / CYBER SECURITY INSTITUTE

Cyber Security Institute (SGE), with the purpose of improving the national cyber security, was first established as the IT Systems Security Division under the National Electronics and Cryptology Research Institute in 1997. Since 2012, it has been operating as a separate institute under TÜBİTAK BİLGEM.

Cyber Security Institute conducts research and development activities within the context of cyber security, and provides public, private and military organizations with solutions within this scope. The Institute, with its successful projects, has so far remarkably contributed to the accumulation of information on cyber security. Among the main activities of the Cyber Security Institute are Advanced Cyber Security R&D Activities, Activities about the Determination of Cyber Security Strategy and Cyber Security Solution Projects.

YTE / SOFTWARE TECHNOLOGIES RESEARCH INSTITUTE

Software Technologies Research Institute (YTE) mainly conducts R&D activities in the field of software technologies and e-government thereby meeting the R&D-based needs of the public and private sectors and providing these institutions with e-government solutions. Within this context, by highly contributing to the software development of the country, the institute aims at being the leading one in Turkey.

Among the main activities of YTE are case analyses within the context of e-transformation of public management, designation of roadmaps and development of strategic and critical software systems for the public. In this context, it carries out social and statistical analyses and conducts R&D activities in the fields of spatial information technologies and business intelligence. In addition to these, the institute provides state institutions and organizations with technical consulting for the procurement of information technologies.

YTE, thanks to its well-experienced and dynamic researchers, meets the afore-mentioned needs and expectations in compliance with the CMMI L 4 and ISO/IEC 27001. In these processes, the institute acts in close collaboration with universities, research organizations, non-governmental organizations and private sector.
### Secure Communication Solutions

<table>
<thead>
<tr>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>MILSEC-3 / Secure Voice Device for HF/VHF/UHF Radios</td>
</tr>
<tr>
<td>22</td>
<td>MILSEC-4 / Secure IP Terminal</td>
</tr>
<tr>
<td>23</td>
<td>IPKC-T / Tactical Network Security Device</td>
</tr>
<tr>
<td>24</td>
<td>AGC-T / Tactical/Mobile Network Security Device</td>
</tr>
<tr>
<td>25</td>
<td>IPKC-G2 / Gigabit Network Security Device</td>
</tr>
<tr>
<td>26</td>
<td>AGC-G / Gigabit Network Security Device</td>
</tr>
<tr>
<td>27</td>
<td>IPKC-GX / 10 Gigabit Network Security Device</td>
</tr>
<tr>
<td>28</td>
<td>IP-YM / IP Crypto Management Center</td>
</tr>
<tr>
<td>29</td>
<td>IP-AYM / IP Key Management Center</td>
</tr>
<tr>
<td>30</td>
<td>SIR / Secure USB Flash Memory Storage Device</td>
</tr>
<tr>
<td>31</td>
<td>SIR-D / Ruggedized, Sec. Usb Flash Mem. Storage Device</td>
</tr>
<tr>
<td>32</td>
<td>SIR-S / Secure Portable Harddisk</td>
</tr>
<tr>
<td>33</td>
<td>VERİSAR / Portable Offline Crypto Device</td>
</tr>
<tr>
<td>34</td>
<td>SVKC / Synchronous Data Encryption Device</td>
</tr>
<tr>
<td>35</td>
<td>FASD-1 / Fax Analog Digital Converter</td>
</tr>
<tr>
<td>36</td>
<td>TAHSİS / Radio Network Communication Systems</td>
</tr>
<tr>
<td>37</td>
<td>MİS / Message Operating System</td>
</tr>
<tr>
<td>38</td>
<td>GMS / Secure Messaging System</td>
</tr>
<tr>
<td>39</td>
<td>GMİ / Secure Messaging Client</td>
</tr>
<tr>
<td>40</td>
<td>DSS / Directory System Server</td>
</tr>
<tr>
<td>41</td>
<td>SRC155A / Point-to-Point SDH/PDH Eth. Dig. Radio Device</td>
</tr>
<tr>
<td>42</td>
<td>SRCYM / SDH Radio Device Management Center</td>
</tr>
<tr>
<td>43</td>
<td>SRC400 / New Gen. High Speed Dig. Radio Link Device</td>
</tr>
<tr>
<td>44</td>
<td>SRCYM400 / SDH Radio Device Management Center</td>
</tr>
<tr>
<td>45</td>
<td>SATEL / Underwater Telephone</td>
</tr>
<tr>
<td>46</td>
<td>KMA / Cryptographic Architecture &amp; Algorithm Design</td>
</tr>
</tbody>
</table>

### Crypto Key Management Systems

<table>
<thead>
<tr>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>49</td>
<td>EKADAS / Electronic Crypto Key Distribution System</td>
</tr>
<tr>
<td>50</td>
<td>EKMI (EKADAS KMI) / Electronic Key Management Infrastructure</td>
</tr>
<tr>
<td>51</td>
<td>KAYC-S / Crypto Key Loading Device</td>
</tr>
<tr>
<td>52</td>
<td>KAYC-S/N / Crypto Key Loading Device/NATO</td>
</tr>
<tr>
<td>53</td>
<td>HVTC / Classified Data Transfer Device</td>
</tr>
<tr>
<td>54</td>
<td>QUANTUM RNG / Quantum Based Random Number Generator</td>
</tr>
<tr>
<td>55</td>
<td>GM / Security Module</td>
</tr>
</tbody>
</table>

### Smart Card and ID Verification Systems

<table>
<thead>
<tr>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>59</td>
<td>NATIONAL IDENTITY CARD / TC &amp; KKTC Identity Card</td>
</tr>
<tr>
<td>60</td>
<td>GGM / Embedded Security Module</td>
</tr>
<tr>
<td>61</td>
<td>AKİS / Smart Card Operating System</td>
</tr>
<tr>
<td>62</td>
<td>AKİS GEZİN e-PASSPORT / Electronic Passport</td>
</tr>
<tr>
<td>63</td>
<td>AKİS GEZİN e-DRIVER LICENSE / Electronic Driver License</td>
</tr>
<tr>
<td>64</td>
<td>AKİS BİLET / Ospt Cipurse Based Smardcard for Electronic Ticketing&amp;Payment Applications</td>
</tr>
<tr>
<td>65</td>
<td>KYS / Card Management System</td>
</tr>
<tr>
<td>66</td>
<td>EKDS / Electronic Authentication System</td>
</tr>
<tr>
<td>67</td>
<td>KEC / Card Access Device</td>
</tr>
<tr>
<td>68</td>
<td>KIOSK-KEC / Kiosk Card Access Device</td>
</tr>
<tr>
<td>69</td>
<td>GEM / Secure Access Module</td>
</tr>
</tbody>
</table>
TUĞITEK BİLGEM / CONTENTS

ELECTRONIC CERTIFICATION MANAGEMENT SOLUTIONS
73 ESYA SM / Certification Authority
74 KERMEN / Public Key Infrastructure Desktop Client
75 ESYA API / Electronic Signature Libraries
76 ESYA ZD SERVER / ESYA Timestamp Server
77 İMZAGER / Implementation of Desktop Signing
78 SECURE PDF / Implementation of PDF Signing / Encryption

ELECTRONIC INTELLIGENCE SOLUTIONS
81 SGS 4.0 / Spectrum Monitoring System
82 FDC101 / Broadband Elint Frequency Converter
83 FDC201 / Broadband Frequency Extender
84 FD300A / IF Converter
85 YTA-018D / Software-Based Wideband Receiver
86 YTS2000 / Non-Linear Junction Detector 2000MHz

DATA VALORISATION SOLUTIONS
89 IYON SUITE / Forensic Image Enh. & Restoration Software
90 Allied Radio Frequency Computer Aided Data Exchange & Spectrum Management Information Repository Online

CIVIL AVIATION SOLUTIONS
93 HATS / Helicopter Tracking System
94 HATC / Helicopter Tracking Device
95 atcTRsim / Air Traffic Control Tower and Radar Simulator
96 ATCSES / ATC Selection Tool
97 KUŞRAD / Avian Radar
98 MGR / PSR Radar
99 ASTERIXCARE / Radar Test Software

RAILWAY TRANSPORTATION SYSTEMS
103 DTKM / Railway Traffic Control Center
104 DAS / Railway Interlocking System
105 TRENŞİM / E 43000 Locomotive Simulator

BIOELECTRONIC DEVICES AND SYSTEMS
109 MİSENS - BİSENS / Fully-Auto. Mobile Biosensor Device
110 SOBE / Transcutaneous Optic Jaundice Measurement

ELECTRONIC DOCUMENT AND ARCHIVING SOLUTIONS
113 EBRU / Document Tracking System
114 SKAAS / Digital Storage Archive and Analysis System
115 e-BELGEM / Archive Management System
## ELECTRO-OPTICS AND LASER SYSTEMS

- 119 UMKC / National Marker Control System
- 120 FORENSIC XP-4010D / Next Generation Questioned Doc. Exam.
- 121 DDA-1 / Quadrant Photodectedors
- 122 GEZKIT / Real-Time IR Track Prediction and Management Sys.
- 123 FKDS / Fiber Optical Cable Monitoring System

## CYBER SECURITY

- 127 STAMPS / Centralized Cyber Threat Sensor System
- 128 SORT / Cyber Space Trap System
- 129 VKOS / Data Leakage Prevention System
- 130 SİBERMEYDAN CTF / Cyber Sec. Sim. and Comp. Environment
- 131 Cyber Security Services

## UNDERWATER DEFENCE SYSTEMS

- 137 DATAS / Submarine Tactical Simulator
- 138 SEDAVER / Scenario Based Submarine Data Package Gen.
- 139 DAKA / BTBM / Acoustic Decoy Development for Submarine / Quest of Acoustic Reactions for Anti-Torpedo

## DEFENSE SYSTEM SOLUTIONS

- 143 DRT TABLE / Digital Dead Reckoning Table
- 144 GİS / Real-Time Operating System
- 145 ETMTS-2 / Hand-Held Mine Detection System
- 146 TAKSİS / Tactical Training System
- 147 SHIPBOARD D/G / Shipboard Automatic Degaussing System

## ELECTRONIC WARFARE SYSTEM SOFTWARE SOLUTIONS AND SYSTEM SOLUTIONS

- 151 SİMA / Simulation Modelling Infrastructure
- 152 MARSys / Management and Analysis of Radio Spectrum Sys.
- 153 IRDMAS / IR Meas. Data Base Man. and Analysis Software
- 155 RASES / Radar Cross Section Computation
- 156 Electronic Warfare Systems Design & Development
- 157 Electronic Warfare Analysis, Test & Evaluation

## CLOUD COMPUTING SOLUTIONS

- 161 DAMLA / National Search Engine Prototype
- 162 B3LAB / Safir Product Family
- 163 B3LAB / Big Data Analytics Solutions

## IDENTIFYING NEEDS AND PLANNING SOLUTIONS

- 167 Identifying Needs and Planning Solutions
- 168 National E-Government Strategy and Action Plan Project
- 169 The Project of Preliminary Analysis of Integrated Public Financial Management Information System
- 170 Pre-Analysis of Sme Information System
- 171 Pre-Analysis of TEİAŞ Information Management System
- 172 Pre-Analysis of BTK Information Management Sys. Project
### SOFTWARE DEVELOPMENT

<table>
<thead>
<tr>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>175</td>
<td>Software Development</td>
</tr>
<tr>
<td>176</td>
<td>Product Tracking System Project</td>
</tr>
<tr>
<td>177</td>
<td>Development Agencies Management System Project</td>
</tr>
<tr>
<td>178</td>
<td>Integrated Social Assistance Services Project</td>
</tr>
<tr>
<td>180</td>
<td>It System Development of Emra (EBİS)</td>
</tr>
</tbody>
</table>

### MODEL DEVELOPMENT AND COMPETENCE BUILDING

<table>
<thead>
<tr>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>183</td>
<td>Model Development and Competence Building</td>
</tr>
<tr>
<td>184</td>
<td>Guidelines for Governmental Web Sites and Diss. (KAMİS) Prj.</td>
</tr>
<tr>
<td>186</td>
<td>Enterprise Architecture / The Open Group &amp; Togaf</td>
</tr>
<tr>
<td>187</td>
<td>Digital Maturity Model and Guidance Project</td>
</tr>
</tbody>
</table>

### GOVERNANCE PLANNING

<table>
<thead>
<tr>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>191</td>
<td>Governance Planning</td>
</tr>
<tr>
<td>192</td>
<td>Data Center Modernization Project</td>
</tr>
</tbody>
</table>

### POLICY AND STRATEGY MONITORING AND EVALUATION

<table>
<thead>
<tr>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>197</td>
<td>Policy and Strategy Monitoring and Evaluation</td>
</tr>
<tr>
<td>198</td>
<td>Digital Transformation Research Series</td>
</tr>
</tbody>
</table>

### DEVELOPMENT OF R&D PROJECT ON NEW TECHNOLOGY AND TRENDS

<table>
<thead>
<tr>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>203</td>
<td>Development of R&amp;D Project on New Technology and Trends</td>
</tr>
<tr>
<td>204</td>
<td>National Database R&amp;D</td>
</tr>
</tbody>
</table>

### DISASTER AND EMERGENCY MANAGEMENT SOLUTIONS

<table>
<thead>
<tr>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>207</td>
<td>İKAS / Warning and Alarm Integrated System</td>
</tr>
<tr>
<td>209</td>
<td>KGHS / Continuous and Secure Communication System</td>
</tr>
</tbody>
</table>

### ADVANCED TECHNOLOGIES RESEARCH INFRASTRUCTURE

<table>
<thead>
<tr>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>211</td>
<td>ATAM / Antenna Test and Research Laboratory</td>
</tr>
<tr>
<td>212</td>
<td>COMSEC / Communications Security Laboratory</td>
</tr>
<tr>
<td>213</td>
<td>KDTM / Speech &amp; Language Technologies Laboratory</td>
</tr>
<tr>
<td>214</td>
<td>Electro-Optics &amp; Laser Systems Laboratory</td>
</tr>
<tr>
<td>215</td>
<td>KAMTAM / CATHODE and Microwave Vacuum Tube Research Lab.</td>
</tr>
<tr>
<td>216</td>
<td>CRYPTANALYSIS Laboratory</td>
</tr>
<tr>
<td>217</td>
<td>KYAS / Spherical Near Field Measurement System Laboratory</td>
</tr>
<tr>
<td>218</td>
<td>OKTEM / Common Criteria Test Laboratory</td>
</tr>
<tr>
<td>219</td>
<td>RADAR-RDL / Radar Research &amp; Development Laboratory</td>
</tr>
<tr>
<td>220</td>
<td>RAPSİM / Radar Performance and Signature Analysis Laboratory</td>
</tr>
<tr>
<td>221</td>
<td>RF- RDL / RF Research &amp; Development Laboratory</td>
</tr>
<tr>
<td>222</td>
<td>TEMPEST Test Laboratory</td>
</tr>
<tr>
<td>223</td>
<td>YİTAL / Semiconductor Technologies Research Laboratory</td>
</tr>
<tr>
<td>224</td>
<td>YTKDL / Software Test and Quality Assessment Laboratory</td>
</tr>
<tr>
<td>225</td>
<td>KİTAL / Wireless Communication Techn. Research Laboratory</td>
</tr>
<tr>
<td></td>
<td>TÜTEL / VLSI Design and Education Laboratory</td>
</tr>
</tbody>
</table>
SECURE COMMUNICATION SOLUTIONS

* Due to ongoing research and development, specifications in this catalogue and its content may change without prior notice.
MILSEC-3
SECURE VOICE DEVICE FOR HF/VHF/UHF RADIOS

SECURE COMMUNICATION SOLUTIONS

SECURE VOICE SOLUTION FOR HF/VHF/UHF TACTICAL COMMUNICATIONS
MILSEC-3 is a half-duplex secure communication device that can transmit and receive plain and cipher voice or data over HF/UHF/VHF radio links. Due to its configurable interface, it can work with many voice, data and radio devices. Additionally, MILSEC-3 can communicate with other MILSEC-3 equipment using the national crypto algorithm and communicate with KY58 and KY100 devices by using NATO crypto algorithm.

SECURITY FEATURES
- National algorithm (National mode)
- NATO Crypto Mode
- Preservation of crypto keys up to 60 days emergency backup mode

ENVIRONMENTAL CONDITIONS
- Operating temperature: -40°C / +71°C
- Storage temperature: -57°C / +85°C
- Shock: MIL-STD-810E, Method 516.4
- Temperature shock: MIL-STD-810E, Method 503.3
- Vibration: MIL-STD-810F, Method 514.5
- Gunfire vibration: MIL-STD-810F, Method 519.5
- Altitude: MIL-STD-810F, Method 500.4
- Humidity: MIL-STD-810E, Method 507.3
- Salt fog: MIL-STD-810F, Method 509.4
- Acceleration: MIL-STD-810F, Method 513.5
- Solar radiation: MIL-STD-810F, Method 505.4
- Rain: MIL-STD-810F, Method 506.4
- Sand and dust: MIL-STD-810F, Method 510.4
- Explosive atmosphere: MIL-STD-810F, Method 511.4

Subject to Approval of Turkey Ministry of National Defence for Selling.
SECURE IP TERMINAL

MİLSEC-4 secure IP phone provides state of the art capabilities for both secure and non-secure calls over IP and PSTN networks, providing interoperability with legacy solutions while realizing the future of secure and reliable communications. MİLSEC-4 devices can be configured, monitored, and updated via the Secure Management Center (SMC) over IP networks using NATO SCIP protocol. Unlike older generation secure communication devices, MİLSEC-4 is capable of Over the Network Keying (OTNK) via SMC.

MİLSEC-4 devices are interoperable with MİLSEC-1A and MİLSEC-2 secure phones. MİLSEC-4 provides a smooth transition while replacing MİLSEC-1A and MİLSEC-2 legacy phones during the migration of PSTN to IP networks.

MİLSEC-4 terminal offers a new generation secure communication solution for IP and PSTN networks, at the same time compatibility with legacy phones, which assures seamless communication service.

FEATURES

▪ Secure voice communications over PSTN networks
▪ Secure end-to-end voice, video, and data transfer over IP networks
▪ NATO SCIP compliant for VoIP
▪ Interoperable with commercial SIP products
▪ Interoperable with MİLSEC secure phones
▪ National and AES crypto algorithms
▪ Remote configuration/software updates
▪ Easy-to-use interface with LCD touchscreen

Subject to Approval of Turkey Ministry of National Defence for Selling.
SECURE COMMUNICATION SOLUTIONS OVER TACTICAL NETWORKS

IPKC-T is the latest low-power solution for tactical secure networks. IPKC-T is especially designed in small sizes and light weight, for user friendly and resistant to tactical environmental stress. IPKC-T provides secure communications at network level between IP local area networks, which communicate over insecure networks. The device is located between local network and edge router and establishes a secure gateway. IPKC-T has a data processing capacity of up to 180 Mbps.

SECURITY SPECIFICATIONS
- "SECRET" level data security
- Authentication
- Data integrity
- Emergency-erase feature against tampering
- Hardware-based implementation
- Hardware-based random number generator
- Encryption: Approved National Encryption Algorithm
- Authentication: Approved National Authentication-Algorithm
- Key exchange: ECDH
- Signing: ECDSA
- Automatic key exchange with IKE protocol
- X.509 certificate-based study
- Two-stage access control with smart-card and password, role-based device access control
- Smart-card-based Crypto Ignition Key and User Card
- Logging events, alarms and user commands
- Offline key loading in MILAY modes by using key loader
- Online key loading by IP Key Management Center and EKADAS

TECHNICAL SPECIFICATIONS
- Provides secure communication of IP/Ethernet Networks over insecure and unprotected networks
- Enables data transmission from one point to multipoint simultaneously
- Performance: 90 Mbps (red to red, one direction)
- 500 automatic/manual tunneling
- IPv4, IPv6, TCP, UDP, ICMP, SNMP, FTP
- 2 x 10/100 Mbps Fast Ethernet (IEEE 802.3), auto sense, auto crossover
- Command-based configuration by Local management (console) port, user-friendly command set
- SNMP-based remote management by IP Management Center
- Configuration Backup
- VRRP support for providing device redundancy
- Local and remote software update
- COMSEC, EMI/EMC and TEMPEST

Subject to Approval of Turkey Ministry of National Defence for Selling.
AGC-T

TACTICAL/MOBILE NETWORK SECURITY DEVICE

SECURE COMMUNICATIONS OVER TACTICAL/MOBILE NETWORKS
AGC-T is the latest low-power solution for tactical secure networks. AGC-T is especially designed in small sizes and light weight, for easy usage and resistant to tactical environmental stress. AGC-T provides secure communications at network level between IP local area networks, which communicate over insecure networks. The device is located between local network and edge router, and establishes a secure gateway. AGC-T has a data processing capacity of up to 180 Mbps.

SECURITY SPECIFICATIONS
▪ "SECRET" level data security
▪ Authentication
▪ Data integrity
▪ Emergency-erase feature against tampering
▪ Hardware-based implementation
▪ Hardware-based random number generator
▪ Algorithm set providing "SECRET" level encryption and authentication
▪ Key exchange: EC-DH
▪ Signing: EC-DSA
▪ Automatic key exchange with IKE protocol
▪ X.509 certificate-based security
▪ Two-stage access control with smart-card and password
▪ Role-based access control
▪ Smart-card-based Crypto Ignition Key and User Card
▪ Logging events, alarms and user commands
▪ Smart card-based offline key loading
▪ Online key loading by IP Key Management Center

TECHNICAL SPECIFICATIONS
▪ Provides secure communications between IP/Ethernet Networks over insecure and unprotected networks
▪ Enables data transmission from one point to multipoint simultaneously
▪ Performance: 90 Mbps (red to red, one direction)
▪ 500 automatic/manual tunneling
▪ IPv4, IPv6, TCP, UDP, ICMP, SNMP, FTP
▪ 2x 10/100 Mbps Fast Ethernet (IEEE 802.3), auto sense, auto crossover
▪ Command-based configuration by local management (console) port, user-friendly command set
▪ SNMP-based centralized remote management by IP Management Center
▪ Configuration Backup
▪ VRRP support for providing device redundancy
▪ Local and remote software update
▪ COMSEC, EMI/EMC and TEMPEST

Subject to Approval of Turkey Ministry of National Defence for Selling.
IPKC-G2
GIGABIT NETWORK SECURITY DEVICE

SECURE COMMUNICATIONS ON IP NETWORKS
IPKC-G2 provides secure communications at network level between IP local area networks, which communicate over insecure networks. The device is located between local network and edge router and establishes a secure gateway. It provides data confidentiality, authentication and integrity. IPKC-G2 has a data processing capacity of up to 1.8 Gbps.

SECURITY SPECIFICATIONS
▪ "SECRET" level data security
▪ Authentication
▪ Data integrity
▪ Emergency-erase feature against tampering
▪ Hardware-based implementation
▪ Hardware-based random number generator
▪ Encryption: Approved National Encryption Algorithm
▪ Authentication: Approved National Authentication-Algorithm
▪ Key exchange: ECDH
▪ Signing: ECDSA
▪ Automatic key exchange with IKE protocol
▪ X.509 certificate-based study
▪ Two-stage access control with smart-card and password, role-based device access control
▪ Smart-card-based Crypto Ignition Key and User Card
▪ Logging events, alarms and user commands
▪ Offline key loading in MILAY modes by using key loader
▪ Online key loading by IP Key Management Center and EKADAS

TECHNICAL SPECIFICATIONS
▪ Provides secure communication of IP/Ethernet Networks over insecure and unprotected networks
▪ Enables data transmission from one point to multipoint simultaneously
▪ Performance: 900 Mbps (red to red, one direction)
▪ 2000 automatic/manual tunneling
▪ IPv4, IPv6, TCP, UDP, ICMP, SNMP, FTP
▪ 2 x 10/100/1000 Mbps Gigabit Ethernet (IEEE 802.3), auto sense, auto crossover
▪ Command-based configuration by Local management (console) port, user-friendly command set
▪ SNMP-based remote management by IP Management Center
▪ Configuration Backup
▪ VRRP support for providing device redundancy
▪ Local and remote software update
▪ COMSEC, EMI/EMC and TEMPEST

Subject to Approval of Turkey Ministry of National Defence for Selling.
AGC-G
GIGABIT NETWORK SECURITY DEVICE

SECURE COMMUNICATIONS ON IP NETWORKS
AGC-G provides secure communications at network level between IP local area networks, which communicate over insecure networks. The device is located between local network and edge router and establishes a secure gateway. It provides data confidentiality, authentication and integrity. AGC-G has a data processing capacity of up to 1.2 Gbps.

SECURITY SPECIFICATIONS
- “SECRET” level data security
- Authentication
- Data integrity
- Emergency-erase feature against tampering
- Hardware-based implementation
- Hardware-based random number generator
- Algorithm set providing “SECRET” level encryption and authentication
- Key exchange: EC-DH
- Signing: EC-DSA
- Automatic key exchange with IKE protocol
- X.509 certificate-based security
- Two-stage access control with smart-card and password
- Role-based access control
- Smart-card-based Crypto Ignition Key and User Card
- Logging events, alarms and user commands
- Smart card-based offline key loading
- Online key loading by IP Key Management Center

TECHNICAL SPECIFICATIONS
- Provides secure communications between IP/Ethernet Networks over insecure and unprotected networks
- Enables gigabit data transmission from one point to multipoint simultaneously
- Performance: 600 Mbps (red to red, one direction)
- 2000 automatic/manual tunneling
- IPv4, IPv6, TCP, UDP, ICMP, SNMP, FTP
- 2x 10/100/1000 Mbps Gigabit Ethernet (IEEE 802.3), auto sense, auto crossover
- Command-based configuration by Local management (console) port, user-friendly command set
- SNMP-based Centralized remote management by IP Management Center
- Configuration Backup
- Local and remote software update
- COMSEC, EMI/EMC and TEMPEST

Subject to Approval of Turkey Ministry of National Defence for Selling.
SECURE COMMUNICATION SOLUTIONS

IPKC-GX
10 GIGABIT NETWORK SECURITY DEVICE

SECURE COMMUNICATIONS ON IP NETWORKS
IPKC-GX is the latest solution for high-speed secure communications. IPKC-GX provides high bandwidth applications at 10Gbps speed. IPKC-GX acting as a security gateway is located between local network and edge router to establish VPN (Virtual Private Networks). IPKC-GX secures IP traffic by means of data confidentiality, authentication and integrity.

SECURITY SPECIFICATIONS
- "SECRET" level data security
- Authentication
- Data integrity
- Emergency-erase feature against tampering
- Hardware-based implementation
- Hardware-based random number generator
- Encryption: Approved National Encryption Algorithm
- Authentication: Approved National Authentication-Algorithm
- Key exchange: ECDH
- Signing: ECDSA
- Automatic key exchange with IKE protocol
- X.509 certificate-based study
- Two-stage access control with smart-card and password, rolebased device access control
- Smart-card-based Crypto Ignition Key and User Card
- Logging events, alarms and user commands
- Offline key loading in MILAY modes by using key loader
- Online key loading by IP Key Management Center and EKADAS

TECHNICAL SPECIFICATIONS
- Provides secure communication of IP/Ethernet Networks over insecure and unprotected networks
- Enables data transmission from one point to multipoint simultaneously
- Performance: 9 Gbps (red to red, one direction)
- 8000 automatic/manual tunneling
- IPv4, IPv6, TCP, UDP, ICMP, SNMP, FTP
- 10 GbE (10 Gigabit Ethernet) Bakır veya Fiber
- Command-based configuration by Local management (console) port, user-friendly command set
- SNMP-based remote management by IP Management Center
- Configuration Backup
- VRRP support for providing device redundancy
- Local and remote software update
- COMSEC, EMI/EMC and TEMPEST

Subject to Approval of Turkey Ministry of National Defence for Selling.
IP-YM is a server-based system with a web-based user-friendly interface which enables administrators to manage IPKC-G and AGC-G IP Encryptors centrally. It is capable of managing devices, configurations, alarms, and logs in a secure manner. IP-YM has advanced features which help network administrators to perform their daily operations easily.

**SECURITY FEATURES**
- Smart card-based user authentication
- Role-based user authorization
- SSLv3
- SNMPv3
- Dedicated IPKC-G/AGC-G used for management communication
- Grouping of devices in a hierarchical manner
- Tree-based view of managed devices and groups
- Periodic device connection checking
- Automatic device recognition and management
- Device remote PING
- On demand device date-time configuration
- Detailed device IPSEC configuration management
- Device IPSEC configuration error detection and reporting
- Remote device software upgrade
- Device configuration backup and recovery
- Key groups management in participation with Key Management Center
- Device network configuration management
- Device network elements management
- Device local user management

**GENERAL FEATURES**
- Remote management of devices from a single point
- Multi-browser support
- Web-based AJAX-based user interface
- Client-server architecture
- Multi-user support
- Role and permission-based user management
- Log and report generation
- E-mail notification
- Device Alarm, Monitoring, and Log Management
- Device performance management with throughput monitoring
- Graphical monitoring of device MIBs (network parameters)
- Alarm management and reporting
- Device log management with SYSLOG support
- Built-in FTP server for file transfers to/from device

Subject to Approval of Turkey Ministry of National Defence for Selling.
IP-AYM
IP KEY MANAGEMENT CENTER

IP CRYPTO - KEY MANAGEMENT CENTER
IP-AYM performs IPKC-G/AGC-G devices key management operations centrally. IP-AYM is compatible with IPKC-G/AGC-G Management Center (IP-YM). The Symmetric and Asymmetric Keys of IPKC-G/AGC-G devices are generated by IP-AYM. For key generation, IP-AYM uses IPKC-G/AGC AU&IC device. Distribution, accounting, and management functions are included. Web based user interface enables management from any secure location. The system has been designed to operate on a 7/24 basis and physical and geographical backup is possible. The design of the architecture enables expandability.

GENERAL FEATURES
- Key generation by AU&IC device
- Key Distribution
- Key account management
- Key Destruction
- Certificate generation by AU&IC device
- Online certificate distribution
- Certificate account management
- Certificate Revocation List and erase management
- Alarm management and configuration
- User account management and update operations
- Dynamic role management
- Smart card-based user identification
- User and system logs
- Geographical and physical backup

MINIMUM REQUIREMENTS
- 3 GHz Dual Core Processor
- 4 Gbyte RAM
- 4 Gbyte Hard disk
- PostgreSQL
- Windows 7/2008 Server
- CPU, RAM and Hard disk requirements may vary according to number of managed devices

⚠ Subject to Approval of Turkey Ministry of National Defence for Selling.
SIR
SECURE USB FLASH MEMORY STORAGE DEVICE

SIR is an encrypted USB flash memory storage device which keeps data and fulfills the security requirements on a full hardware-based architecture, operated by a single user. The device has the storage capacity options of 2 GB/4 GB/8 GB flash memory with the ability of 10 MB/s writing & reading speeds.

The device protects data stored on itself, not while reading from or writing to the host.

SIR provides security for a single user. No other user can access the protected data using his/her own user token. Additional security measures like emergency erase and tamper switches are employed in the device.

The user is informed about any change about the status of the device by the help of visual indicators (login, key pressed, token, USB connected warnings) and an audio indicator. There is a write protect switch on the device to disable writing to the device if needed. The device is powered from single USB interface of the host computer. The embedded battery is charged via the USB interface of the host to preserve key memory for maximum 6 months without any power.

Designed to be commercial grade, tactical, ruggedized, portable equipment. SIR is fully compatible with the COMSEC, EMI/EMC, TEMPEST standards.

SECURE COMMUNICATION SOLUTIONS
SIR-D
RUGGEDIZED, SECURE USB FLASH MEMORY STORAGE DEVICE

SIR-D is an encrypted USB flash memory storage device that is designed for rugged and harsh environments. It has a rubber enclosure to prevent against shock and splash.

The device has the storage capacity options of 2GB/4GB/8GB flash memory with the ability of 10MB/s writing & reading speeds. The device protects data stored on itself, not while reading from or writing to the host.

Data security and device/user authentication requirements are provided by means of a user token and a user password. The device employs a hardware implementation of a confidentiality protection algorithm type for providing data security for data classified as NATO SECRET and below. 256-bit hardware AES encryption block is used to provide data security. Device generates the keys using its own Random Number Generator, eliminating the need for key loading.

SIR-D supports plug and play operation for Windows and Linux based host computers. The user is informed about any change in the status of the device by the help of the visual indicators (initialization, user authentication, keypressed, token, battery charging) and an audio indicator.

There is a write protect switch on the device to disable writing to the device when requested.

The device is powered from one slot USB interface of the host computer, which it is connected to. There is an embedded battery inside which is charged via USB interface of the host, for supplying key memory for minimum 6 months period without any power.

SIR-D is fully compatible to the COMSEC, EMI/EMC, TEMPEST standards.

Subject to Approval of Turkey Ministry of National Defence for Selling.
SIR-S
SECURE PORTABLE HARDDISK

SIR-S is an encrypted hard disk device which keeps and fulfills the security requirements on a full hardware-based architecture. The device serves for a single user and holds USB and Esata interfaces. It has the storage capacity options of 250 GB/500 GB with the ability of 40MB/s writing & reading speeds via eSATA Gen2 and USB 3.0 interfaces.

The device protects data stored on itself, not while reading from or writing to the host.

Secure portable hard disk provides security for a single user. No other user can access the protected data using his/her own user token. Additional security precautions like emergency erase and tamper switches are employed in the device. The user is informed about any change in the status of the device by the help of the visual indicators (login, key pressed, token, eSATA/USB connected warnings) and an audio indicator.

The device is powered from the USB interface of the host computer. There is an embedded battery inside which is charged via USB interface of the host. The device keeps key memory for 6 months period with a fully charged battery without any external power source.

Designed to be commercial grade, tactical, ruggedized, portable equipment, SIR-S is fully compatible with the COMSEC, EMI/EMC, TEMPEST standards providing RED-BLACK data separation.

USER INTERFACE
▪ 12-key piezo ceramic keypad, two coloured 5 indicators
▪ 1 buzzer, 1 emergency erase switch
▪ 1 user token reader slot

HOST INTERFACE
▪ Platform independent - USB 3.0, USB 2.0, eSATA Gen2

FEATURES
▪ 250 GB/500GB Data Storage Capacity
▪ Plug & Play
▪ Dimensions: 80 x 175 x 20 mm
▪ Weight: 420 gr

Subject to Approval of Turkey Ministry of National Defence for Selling.
VERİSAR is a portable single user offline file encryption device. An insecure computer can be used for classified message/file encryption and decryption by using VERİSAR.

VERİSAR contains a secure Linux-Based operating system to establish a secure working environment for cryptographic operations and this operating system is kept in encrypted partition.

When user wants to encrypt or decrypt a file, what s/he needs is a USB bootable computer (desktop or notebook). Host computer will be booted from encrypted Linux-Based read-only operating system. All network capabilities of the host computer will then be disabled by default.

VERİSAR has online and offline operation modes. The corresponding softwares running on the computer provide communication between computer and VERİSAR device. The offline mode which is used for message encryption and decryption is active, when the computer is booted from encrypted built-in operating system.

The online mode which is used for sending and receiving the encrypted messages is active, when the device is used from another insecure operating system. VERİSAR works with Security Management Center (SMC) software. SMC is used for initialization and renewal of VERİSAR certificates.

FEATURES
- 2GB Offline, 2GB Online User Storage capacity
- 2GB Outbox Partition, 2GB Inbox Partition
- Total 8GB data storage capacity
- Dimensions (WxDxH): 51 x 91 x 14 mm
- Weight: 90gr.

USER INTERFACE
- 12-key piezo ceramic keypad, two colored 4 indicators
- 1 buzzer, 1 emergency erase switch, 1 write protect switch
- 1 user token reader slot

OPERATING SYSTEMS
- Platform independent (Offline mode) - Windows, Linux platforms
- Windows 7/VISTA/XP/2000, Linux Kernel 2.4 and newer versions

Subject to Approval of Turkey Ministry of National Defence for Selling.
SVKC
SYNCHRONOUS DATA ENCRYPTION DEVICE

FEASIBLE SOLUTIONS TO ACHIEVE YOUR COMMUNICATION AND SECURITY GOALS

SVKC provides secure synchronous communication over E1 PCM links and leased lines at high data rates up to 2 Mbit/s. With ITU-T V.11 (RS-530) compatible interfaces, SVKC is able to transmit and receive synchronous data up to 2 Mbits at multiples of 64 Kbits.

SVKC also has ITU-T G.703 compatible interfaces. It encrypts and decrypts framed or unframed data at 2 Mbit/s over E1 PCM links.

Traffic keys are loaded into SVKC with either MILAY-1 (Fill Gun) or TELAYS (Electronic Key Management System)

INTERFACES
• ITU-T G.703 compatible interfaces (2,048 Mbit/s)
• ITU-T V.11 (RS-530) compatible interfaces (up to 2,048 Mbit/s)

SECURITY FEATURES
• National algorithm
• Periodically changing crypto keys
• Encrypting of all 32 channel of E1 PCM link
• Framed or unframed operation for E1 PCM interface
• Selecting of clock source (DTE clock or DCE clock) in synchronous mode

Subject to Approval of Turkey Ministry of National Defence for Selling.
SECURE FAX SOLUTIONS
FASD-1 is not an encryption device in itself but acts as an interface between the fax equipment, the data encryption device and the telephone exchange (PABX). It thus provides RED-BLACK data separation for encryption of PC based fax communication. FASD-1 is a low cost solution for secure fax communication when data encryption device is available.

SECURITY FEATURES
- It can be connected to any crypto device compatible with RS-232 standard, 19200/38400 asynchronous N-8-1 protocol

FEATURES
- Secure interface for fax devices without crypto interface and using T.30 protocol
- RJ-11 input for telephone line
- RJ-11 input for fax device
- 14400, 9600, 7200, 4800 and 2400 bps
- MIL-STD-461E EMC compliance
- AMSG-720B TEMPEST compliance
TAHSİS
RADIO NETWORK COMMUNICATION SYSTEMS

RADIO NETWORK COMMUNICATION SYSTEMS
TAHSİS is a set of national systems which includes the required technologies for strategical and tactical radio network communication.

CAPABILITIES

- Secure, reliable voice and data communication in suitable radio frequencies
- Compliant with different antenna systems among 2 MHz – 20 GHz
- Compliant with modem systems which are suitable for RF transmission conditions for narrow and wide band.
- Easy integration of different communication systems (synchronous and asynchronous serial devices, ethernet, USB, MIL-1533 etc.)
- Data processing for different systems (portable / in vehicle / fixed station)
- System development capability for ACP 127 messaging
- Implementation of STANAG 5066 protocol which aims efficient HF data transmission
- TCP/IP, X.200, SMTP, XMPP, AdapP35, Tactical X.400 (STANAG 4406 Annex E), ACP 142, X.500 protocol support
- Design and development of application specific protocols (GeoMesh, WiMesh, GeoPredictor)
- Concurrent usage of a radio device for different purposes

⚠ Subject to Approval of Turkey Ministry of National Defence for Selling.
MESSAGE OPERATING SYSTEM (MIS)
MIS is a national integrated command system for fulfilling the requirements of national and NATO military messaging systems in both tactical and strategic fields. It consists of client and server components which can work together and separately. MIS has 3 configuration types:

- MIS Communication Center
- MIS Workstation
- MIS Mobile

CAPABILITIES
- National Integrated Message Operating System
- Tactical Military Messaging Capability for National and NATO requirements
- Supports ACP 127, STANAG 5066, Tactical X.400 (STANAG 4406), ACP 142, X.500 standards
- Compatible with BRASS (Broadcast Release and Ship-Shore System) infrastructure
- HF, VHF, Satellite, Ethernet bearer support
- Command control property
- 8 synch/asynch data channels
- Simultaneous message sending and receiving on multiple channels
- Archiving and Backup
- High Availability (Instant Replication)
- Sharing common data among operators
- Multi-user support
- SYS, GEBIS, Ethernet Switching Unit, Command Control System Integration
- Half-duplex, simplex and full-duplex operation
- ALE and GPS support
- Optional Communication Applications
  - GeoPredictor: Analyzes and chooses ideal medium, frequency and antenna for communicating with a remote receiver
  - HF E-Mail: Provides Internet Mail (SMTP) communication over HF radio
  - XMPP Client and Tactical Chat Gateway: STANAG 5066 Annex E compliant chat protocol applications
  - Virtual DTE: Provides the use of a wireless device with multiple applications concurrently
  - VoHF – Voice Over HF: Provides secure voice message transmission through low speed connections
  - COSS – STANAG 5066 Serial Channel Emulator: Serial channel data function over STANAG 5066 protocol to handle ARQ
  - BFTP – Binary File Transfer: File transport protocol over HF and VHF radio connections

Subject to Approval of Turkey Ministry of National Defence for Selling.
SECURE COMMUNICATION SOLUTIONS

GMS
SECURE MESSAGING SYSTEM

TRUSTWORTHY SOLUTIONS FOR MILITARY AND CORPORATE MESSAGING

Secure Messaging System (GMS) developed by TÜBİTAK BİLGEM is suitable for use in military and corporate strategic, operative and tactical field messaging requirements. GMS meet messaging requirements in an uninterrupted, fast, accurate, reliable and secure way through a single system.

GMS provides integrated messaging of strategic and tactical environments which have low bandwidth and high data loss. GMS consists of Message Transfer Servers (MTS), Directory System Servers (DSS), Messaging Clients which can work in both strategic and tactical field, and also Gateway Software developed for a more efficient and integrated messaging.

CAPABILITIES

▪ X.400 and SMTP/IMAP Message Transfer Servers
▪ Messaging Clients supporting corporate and military
▪ Messaging forms
▪ X.500 Directory System Server
▪ LDAP Gateway
▪ ACP 127-X.400 Gateway
▪ Mail List Agent for message delivery to Address Lists
▪ STANAG 4406 (Ed.2) support
▪ STANAG 4406 Annex E support for messaging in tactical field
▪ Advanced message reporting and tracking
▪ Extendable directory schema
▪ Advanced management tools

SECURITY FEATURES

▪ Transport Layer Security
▪ Authentication
▪ Smart card and HSM support
▪ Message security (signing and encryption)
▪ Access control
▪ PKI support
▪ PMI support
▪ Audit log
▪ Security policy

Subject to Approval of Turkey Ministry of National Defence for Selling.
SECURE COMMUNICATION SOLUTIONS

GMİ
SECURE MESSAGING CLIENT

NATIONAL MESSAGING CLIENT FOR SECURE MESSAGING
Messaging Client is a platform independent software for message transfer and directory access. Allows messaging in varying levels of security by providing signed and/or encrypted message submission capability. Users are managed and authorized to access restricted screens and functionality. Messaging Client has a modular, customizable architecture and provides military and corporate messaging features through different modules.

Tactical Messaging Client, a separate application, allows operation in low bandwidth environments (e.g. ships and submarines) and is the modified version of Messaging Client which is targeted for operation in medium to high bandwidth. Tactical Messaging Client provides a lighter user interface and guarantees transmission of minimum required data only.

CAPABILITIES
- ITU X.400 and SMTP/IMAP messaging support
- ITU X.500 and LDAP directory access
- Local address book support
- Secure messaging interfaces
- Messaging Client for Tactical military purposes
- Customizable military and corporate message form support
- Priority mechanism
- Per-recipient reports
- Alternate recipient
- Daily message reporting, advanced message tracking
- Deleted message recovery
- Platform independent

SECURITY FEATURES
- Transport Layer Security
- Authentication
- Smart Card, PFX and HSM support
- Message security (signing, encryption)
- Message access control
- Local certificate store

Subject to Approval of Turkey Ministry of National Defence for Selling.
DIRECTORY SYSTEM SERVER FOR SECURE MESSAGING

Directory System Server (DSS) is a nationally developed directory server, which stores user and certificate information at different levels hierarchically in a secure and consistent way and serves the actual information reliably, securely and uninterrupted. DSS provides fast access to the user, device, department and organization information, which is stored in a defined hierarchy. DSS supports detailed security policies, which enables detailed management of users access and messaging authorization.

DSS has been developed in accordance with international standards. It is compatible with the most detailed directory standards cluster ITU X.500, as well as supports the simplified LDAP protocol to access directory information. This way, DSS can be used with different military and commercial directory applications.

Since DSS is a nationally developed product, without any licensing dependencies to other commercial products, it can easily be customized in accordance with corporate requirements.

**CAPABILITIES**
- Secure directory services in ITU X.500 standard
- Extensible directory schema (ACP 133, LDAP, X.500)
- Gateway Interface to support LDAP v3
- LDIF support
- Advanced replication facility
- Advanced Management Tool
- Backup and failover recovery
- Platform independent

**SECURITY FEATURES**
- Transport Layer Security
- Authentication
- Access Control
- Audit Log
- Security policy
The SRC 155A series of Point-to-Point digital radio devices deliver highly flexible and reliable solutions for nxE1 (up to 64xE1) and nxE3 (up to 4xE3) in PDH hierarchy; STM-1 in SDH hierarchy; up to 156 Mbps in Layer 2 Ethernet communication. The operating frequency bands are 7, 8, 10.5, 15 and 26 GHz (ITU).

**CAPABILITIES**

- Software based selection of data capacity, modulation type, RF channel frequency, transmission mode (redundant or non-redundant), output power and test facilities for operator needs
- Thanks to plug&play modules, already established links can have required capacity and interfaces
- Flexible installation and operation thanks to separated IDU (Indoor Unit) and ODU (Outdoor Unit) structures.
- Low infrastructure requirement and cost thanks to efficient built-in control system and optional RF Network Management System Software
- PDH data transmission at 16xE1, 32xE1 and 64xE1, 1xE3, 2xE3, 4xE3 without a need of additional multiplexer thanks to scaleable PDH multiplexer interface cards
- SRC155A system can be managed and monitored by using any SNMP-based network or device management system.

**FEATURES**

- Standard ITU-R licensed frequency bands (7, 8, 10.5, 15 and 26 GHz)
- Mixed Mode working capability, PDH and SDH communication (16-32-64xE1, 1-2-4xE3, STM1-o, Gigabit Ethernet)
- IEEE 802.3, ITU-T G.703 compliant data interface cards
- Suitable architecture for (1+0), (1+1) frequency diversity, (1+1) HSB Tx, (1+1) space diversity Rx, (2+0) working modes
- In the separated architecture, base band circuits (IDU: Indoor Unit) and Tx/Rx (ODU: Outdoor Unit) are connected with single coaxial cable connection for (1+0) and two coaxial cables for (1+1 and 2+0).
- Optimization of bandwidth efficiency with adjustable modulation type depending on data rate
SECURE COMMUNICATION SOLUTIONS

SRCYM
SDH RADIO DEVICE MANAGEMENT CENTER

SRCYM is a software solution for remote management of SRC 155A Digital Radio Devices. It provides effectiveness which is a basic need in communication networks. This means quick and easy diagnosis of problems, cost savings from personnel, hardware and training, and high service quality.

SRCYM Users can easily register and manage all SRC 155A devices within network. User can perform different operations on management center depending on their authorization level with multi-user support. Since it is a web based system, there is no need for a software setup in client computers. The only need is a computer with a modern browser having access to the server.

FEATURES
- Web based dynamic user interface
- Logical and location based grouping of devices
- Automatic device discovery and registration
- Alarm management
- Configuration Management
- Advanced reporting functions
- SNMP based management
- User operation logs
- Advanced role based and device group based access control
- Password based authentication
- E-mail notification
- English and Turkish language support

MAIN BENEFITS
- Managing devices remotely from single point
- Checking alarm and connectivity status of devices
- Monitoring instant status of devices
- Changing device configurations easily and quickly
SRC400 is a new generation, high-speed microwave point-to-point radio system. Design is optimized for Ethernet data transmissions up to 400 Mbps at L2. It is not only for the existing GSM and Telecommunication infrastructure but also for new generation LTE/4G networks that require high speed data package transmission capabilities. STM1 and E1 interfaces can be adapted to the system if required. Operating frequency bands are 7, 8, 10.5, 15 and 26 GHz (ITU bands).

**TECHNICAL FEATURES**
- Operation at licensed ITU-R frequency bands (7 & 8 GHz)
- “Native Ethernet” airframe structure
- Automatically shifting modulation types between QPSK and 256QAM due to Adaptive Modulation (ACM) feature
- 1+0, 1+1 HSB Tx, 1+1 FD, 2+0, 4+0 operating modes
- Separated structure as Indoor (IDU) and Outdoor (ODU) units; ODU integrated antenna
- Direct integration to antenna via RF combiners for 1+1 and 2+0 structures
- Transmission capability up to 800 Mbps with XPIC feature (optional)
- 4 ODU’s can be connected to one IDU (4+0)

**CAPABILITIES**
- Configurable data-rate, modulation type, RF frequency, operating mode (redundant/non-redundant), output power via software
- User-friendly test tools; embedded performance monitoring (BER, ES, SES...) feature
- Flexible installation and operating by the help of separated structure
- Easy operation by the help of effective and robust embedded control software
- SNMP agents are used for Central Management
- Robust and user-friendly M&C software (optional)
SRCYM400 is a software solution for remote management of SRC 400 and SRC 155A SDH Radio Devices. It is the new generation of previous SRCYM software, and provides effectiveness which is a basic need in communication networks. This means quick and easy diagnose of problems, cost savings from personnel, hardware and training, and high service quality.

SRCYM400 Users can easily register and manage all SRC 400 and SRC 155A devices within network. Users can perform different operations on management center depending on their authorization level with multi-user support. Since SRCYM400 is a web based system, there is no need for a software setup in client computers. Only need is a computer with a modern browser having access to the server.

FEATURES
- Web based modern and easy to use user interface
- Logical grouping of devices
- Automatic device discovery and registration
- Device status monitoring
- Alarm management
- Configuration Management
- Advanced reporting functions
- SNMP based management
- User operation logs
- Advanced role based and device group based access control
- Password based authentication
- E-mail notification
- English and Turkish language support

MAIN BENEFITS
- Managing devices remotely from single point
- Checking alarm and connectivity status of devices
- Monitoring instant status of devices
- Changing device configurations easily and quickly
UNDERWATER TELEPHONE

Underwater Telephone is a microprocessor controlled communication system which allows communication between surface/subsurface vessels through underwater acoustic waves.

The use of the upper or lower sideband respectively with suppressed carrier frequency (SSB-operation) guarantees a high signal-to-noise ratio at a high transmission bandwidth. The carrier frequency is designed as fixed (quartz stabilized) for NATO frequency or tunable from 1 kHz to 57 kHz for USB and from 4 kHz to 60 kHz for LSB.

While sailing in convoy, it is possible to communicate with suitable station using different frequencies.

Transmission bandwidth is reduced in telegraphy mode for optimum signal-to-noise ratio. Three transducer groups are selectable for nearly omni-directional or sectoral operation. Transducers in the system are placed in the bow and sail.

Inboard connection box which is attached to the pressure hull penetrator is placed in the vicinity of the Combat Information Center. The outboard cables are pressure-resistant and laid in separate cables ways.

The operation and display units are placed in the integrated navigation rack.

Hydrostatic pressure: Equipment exposed to the hydrostatic pressure is resistant to 5 MPa (50 bar). The test pressure can be up to 6.25 MPa (62.5 bar).

TECHNICAL SPECIFICATIONS

- Standard frequency: NATO frequency; quartz stabilized
- Tunable carrier frequency (in 3 Hz steps)
- Frequency indicated as numerical value and by a marker on Integrated LCD-display
- Upper side band (USB): 1 kHz to 57 kHz
- Lower side band (LSB): 4 kHz to 60 kHz
- Power output: 100W at 35 Ω

Subject to Approval of Turkey Ministry of National Defence for Selling.
Cryptography is the science of information security by means of mathematical techniques. It provides solutions for the security needs such as data security, integrity, non-repudiation, authentication, and access control. These solutions are implemented in very wide range of areas where security and privacy are necessary; to name a few: smart cards, satellites, network security devices, sensors. The building blocks of these solutions are the cryptographic structures (algorithms, protocols, and architecture).

To develop genuine cryptographic structures, it is mandatory to have qualified researchers who have expertise in the fields of mathematics, statistics, and electronics. TÜBİTAK BİLGEM has been working on cryptography to provide national solutions since 1980’s.

In this context, the following activities are carried out:

- Design of cryptographic algorithms (encryption, hash, key wrapping, message authentication codes, etc.)
- Design of cryptographic protocols (authentication, key agreement, etc.)
- Design of cryptographic architecture (all cryptographic structures in a device and/or system)
- Design of noise processing functions (for random number generators)
- Education and consultancy

Subject to Approval of Turkey Ministry of National Defence for Selling.
EKADAS generates and stores symmetric/asymmetric keys to crypto devices for secure communication. Furthermore, it securely distributes encrypted keys and saves their accounting information.

EKADAS consists of Electronic Crypto Key Generation System (EKAUS), Electronic Crypto Key Distribution Center (EKADAM), Electronic Crypto Key Distribution Terminal (EKADAT), Electronic Crypto Key Loading Device (EKAYUC), Electronic Crypto Key Transport and Loading Device (EKATAC), Crypto Key Loading Device (KAYC-S) and Line Encryption Device (EKAHAK) and provides solution for all key distribution needs.

FEATURES
- Automatic key generation
- Changeable Hierarchical distributed architecture
- Dial-up/radio/satellite communications
- Non-electrical connections with other EKMS
- Automatic monitoring of accounting information

SECURITY FEATURES
- Double encryption for key packages
- Offline encryption between EKAUS and EKAYUC/EKATAC
- Pre-encryption for the new generation cryptographic devices
- Encryption for all information prior to the communication channel
- Cryptographic authentication between devices
- Role-based user access control

Subject to Approval of Turkey Ministry of National Defence for Selling.
EKADAS KMI supports central or distributed generation of key materials. It also automatically delivers any type of crypto key materials to pre-planned end crypto units, in a scalable, fast, and secure way.

EKMI have been designed with the primary goals of pre-planned locations, modularity and flexibility. Different security protocols and crypto algorithms can be applied with ease thanks to its updatable Security Module. Along with traditional EKMS scenarios, it also provides interfaces to work with other management systems, which facilitates constructing an umbrella key management system.

HVTC, new generation key transfer and fill device of EKMI, provides additional capabilities on top of the ones provided by most known key fill devices.

For reliability purpose, the system can be operated two redundant management sites. It also supports delivering crypto keys to remote locations using PSTN, H/F, Satellite and Ethernet connections.

KEY FEATURES

- Support for any kind of classified data (old keys, modern keys, certificates, codebooks, firmware, mission data, etc)
- High quality and controlled key generation (Quantum and true RNG combinations)
- Transition from EKMS to KMI
- Infrastructure for key management of new generations ECUs
- ECU Inventory-based keymat distribution and accounting
- Constructing a Common Key Management Framework
- National key management umbrella
- Key management in cooperation with mission management systems of ECUs
- Integrating existing key/mission management systems
- Replaces redundant EKMS components/systems,
- Central and/or distributed keymat generation
- Policy-based key management
- Built-in key generation capability for over hundred ECU types
- On-the-fly custom key format design capability
- Intelligent and automated key accounting
- Ability to define cryptographic and managerial relations between keymats
- Ability to create operational and cryptographic relationship between key materials
- Supports complicated key scenarios such as IFFMode5, and Link-16.
- Secure and remote software/firmware update for KMI devices
- Centrally managed ECU Fill Profile database of Tier3 devices
  - Platforms, ECUs, Key types, slots, segment assignments
  - Fill interfaces, fill parameters, Key fill groups
- Fast responses with on-line, 3-layered, star backbone
- NATO IEKMS interoperability
- Supports Platform Key Management Systems such as JSF and A400M.
- Reliable architecture
- Built-in secure e-Mail support
- Compromise reporting mechanism

Subject to Approval of Turkey Ministry of National Defence for Selling.
NATIONAL KEY LOADING SOLUTIONS
KAYC-S is a crypto device which is used for storing the crypto keys and data received from standard interface and protocols (DS-101, DS-102, MILAY) securely, transporting them and key loading/data transmitting to cryptographic terminals.

KAYC-S, which is identified and activated through EKADAS (Electronic Crypto Key Distribution System), can take keys from EKADAS or other systems. KAYC-S has ability to take cryptographic data and keys from EKAYUC (Key Loading Device) and EKATAC (Key Transport Device) which are EKADAS terminals or other data transfer devices (AN/CYZ-10 (DTD), DTD2000 (SDS), Simple Key Loader (SKL)) and key loading devices (KYK-13, KAYC-10, KAYC-32, KAOC-8, KOI-18, MILAY EAYC) with supported standard interfaces. It processes cryptographic data and keys with safety enhancer like integrity checking and encryption. KAYC-S can also store cryptographic data and keys safely and load to several cryptographic key loading/transfer terminal devices. KAYC-S is capable of keeping account information of the keys safely. Moreover, KAYC-S supports the device-specific loading applications with infrastructure development.

Data security in the device is provided by system architecture based on red/black separation, filtering, tamper protection and emergency deleting. KAYC-S is a tactical device and it is compliant with COMSEC, EMI/EMC, TEMPEST standards.

INTERFACES
On 6-pin connector
- DS-102 (EKMS-308F)
- DS-101/RS-485 (EKMS-308F)
- DS-101/RS-232-D (EKMS-308F)
- MILAY

FEATURES
- Storage and loading of national formatted keys
- Keys and cryptographic data receiving/transmission with the help of the user interface
- Cryptographic data receiving from EKADAS System
- Secure key and storing data
- 8 MB storage memory
- Ability to create and store accounts
- Turkish General Staff approved crypto algorithms

![KAYC-S / CRYPTO KEY LOADING DEVICE](image)

Subject to Approval of Turkey Ministry of National Defence for Selling.

51
KAYC-S/N
CRYPTO KEY LOADING DEVICE/NATO

NATO KEY LOADING SOLUTIONS
KAYC-S/N is a crypto device which is used for storing the crypto keys and data received from interfaces and protocols identified by EKMS-308F standard securely, transporting them and key loading/data transmitting to cryptographic terminals in NATO inventory.

KAYC-S/N has SECAN security approval for all NATO security levels, and is considered as a NATO product since it is approved by “Military Committee”.

KAYC-S/N can securely store the red/black keys and cryptographic data which are received from local management devices (LMD/KP, DMD), data transportation devices (AN/CYZ-10 (DTD), DTD2000 (SDS), Simple Key Loader (SKL), EKATAC/EKAYÜC) and key loading devices (KYK-13, KAYC-10, KAYC-32, KAOC-8, KOI-18). In addition, the device can transfer the keys to data transfer devices as black or red and load them to cryptographic terminals.

KAYC-S/N is capable of keeping account of information of the keys safely and transfer the account information to local management devices such as LMD/KP, DMD. Moreover, the device supports CT3 (Common Tier3) application software substructure.

Data security in the device is provided by system architecture based on red/black separation, filtering, tamper protection and emergency deleting. KAYC-S/N is a tactical device and it is complaint with COMSEC, EMI/EMC, TEMPEST standards.

FEATURES
▪ “NATO TOP SECRET” and below confidentiality levels
▪ User Access Control by smart card and password
▪ User-friendly interface
▪ Electrical and mechanical red/black isolation
▪ 320x240 TFT liquid crystal display and 7 stokes keypad
▪ External keyboard interface (PS/2)
▪ Led and audible warnings
▪ Emergency erasable permanent memory to protect cryptographic data
▪ Emergency erase feature while it is on or off

INTERFACES
On 6-pin connector
▪ DS-102 (EKMS-308F)
▪ DS-101/RS-485 (EKMS-308F)
▪ DS-101/RS-232-D (EKMS-308F)

Subject to Approval of Turkey Ministry of National Defence for Selling.
PVTC

CLASSIFIED DATA TRANSFER DEVICE

CRYPTO KEY MANAGEMENT SOLUTIONS

HVTC is a dual mode device that acts both as key processor and cryptographic data transfer device. It stores electronic keys and related COMSEC accounting data, by receiving from KMI (Key Management Infrastructure) or various fill-gun devices/media and transfer them to other fill-gun or crypto equipments in a secure manner.

HVTC is designed to operate as a fill device and/or end equipment of the Turkish KMI (EKADAS) which generate, distributes electronic cryptomaterials in secure and timely manner to many layered destinations through wired, wireless and satellite environments. HVTC receives electronic keys and COMSEC accounting data from fill-gun devices or EKADAS System by communicating with EKADAS SMC (Security Management Center) Servers. HVTC processes these electronic keys & cryptographic data with advanced security features like mutual identity authentication, electronic signature, encryption and loads them to fill-gun, crypto equipments and various types of transfer media such as smart cards,usb memory sticks, CD/DVD, paper (A4/papertape). It also prepares and stores accounting & auditing data and transfers to the EKADAS System. In addition to the flexible access control mechanism for operators, HVTC can also enforce centrally defined policies related to the key management operations. HVTC also transfers keys to NATO Fill Devices and End Cryptographic Units (ECUs). The fill device is also capable of transferring its accounting records to Security Management Center. Designed to be commercial/industrial grade, tactical, portable equipment, HVTC is fully compatible to the COMSEC, EMI/EMC, TEMPEST standards.

TECHNICAL SPECIFICATIONS

- Supports electronic keys in NATO and National formats and modes
- Secure transferring keys to/from EKADAS, NATO & national fill devices and crypto equipments
- Electronic keys and cryptographic data transfer/receive controlled by user interface
- Supports legacy and modern crypto materials
- Accounting records for cryptographic key and device activities
- Remotely managed ECU Fill Profile database of Tier3 devices
- Secure communication interfaces (between Tier2 and Tier3)
  - PSTN, HF/UHF, SATCOM, Ethernet
- Fill interfaces
  - DS101, DS102, MİLAY, RS232, TapePuncher, USB (Smartcard, USB Memory, CD/DVDRW, Printer), Ethernet
- High storage capacity (32 GB)
- Policy and Role based access control
- Two factor authentication (pin -token)
- User friendly, icon based user interface (Multi language support)
- Rugged, scratch resistant PCAP+ multi-touch-screen (16:9, 7 inch Color TFT WSVGA)
  - High resolution GUI (1024x600)
  - Gesture capable screen
  - Direct sunlight visibility
  - Works with hand and gloves
- Built in crypto-processor supporting upto 1000+ crypto algorithms
- Agile cryptography (crypto algorithm upgrade)
- Remote software and firmware upgrade capability
- Tamper-proof
- EMI/EMC compatible (MIL-STD-461F, DO-160E & CISPR 25 EMI)
- TEMPEST Compliant (SDIP-27 Level A (AMSG-720B) standard)
- Water and dust-proof (IP67)
- Temperature range (nominal condition): -20°C to +60°C
- Physical sizes (22cm x 13cm x 4cm, 1.8 Kg)

Subject to Approval of Turkey Ministry of National Defence for Selling.
QUANTUM RNG

QUANTUM BASED RANDOM NUMBER GENERATOR

QUANTUM RANDOM NUMBER GENERATOR
The main advantage of the quantum random number generator is the randomness obtained in accordance with the nature of the quantum-mechanical processes.

Especially security systems which need high security, employing quantum number generator provide better results related to the other type of number generators.

Quantum random number generator device increases the randomness by applying several mathematical tests and mixer functions to the random data produced by using builtin quantum source. The QUANTUM RNG provides generated data via USB interface.

TECHNICAL SPECIFICATIONS
- Input voltage: 12 V
- Power consumption: 4 W
- Interface: USB 2.0
- Maximum throughput (tested data): 12 Mbps
- Dimensions: 80mm x 80mm x 150mm
- Weight: 500 gram
- Temperature range: 0 - 35 °C
- TEMPEST: Compliant
- Mechanical case: Monoblock aluminium

Subject to Approval of Turkey Ministry of National Defence for Selling.
GM is a general purpose hardware security module that provides cryptography and secure data storage functionalities. Designed to be military/and commercial grade, tactical, portable equipment, GM is fully compatible to the COMSEC, EMI/EMC, TEMPEST standards. Thanks to USB interface it can be easily integrated as a security facilitator device with any host platform. Data or keys can be loaded both from host platform and various fill-gun devices/media in a secure manner. Data exchange is supported with fill-gun, crypto equipments and various types of transfer media such as smart cards, usb memory sticks, CD/DVD, paper (A4/papertape).

TECHNICAL SPECIFICATIONS

- Filling electronic keys through fill interface
- MCAF key format support
- Electronic keys and cryptographic data transfer/receive controlled by user interface,
- Supports legacy and modern crypto materials
- Accounting records for cryptographic key and device activities, and specific device events.
- Remotely managed ECU Fill Profile database of Tier3 devices
  - Platforms, ECUs,
  - Key types, key slots, segment assignments
  - Fill interfaces, fill parameters
  - Key fill groups
- Secure communication interfaces (between Tier2 and Tier3)
  - PSTN, HF/UHF, SATCOM, Ethernet
- Fill interfaces
  - DS101,
  - DS102,
  - MILAY,
  - RS232, TapePuncher
  - USB (Smartcard, USB Memory, CD/DVDRW, Printer)
  - Ethernet
- Internal hardware RNG
- Extentable RNG capability with an external RNG
- High storage capacity (32 GB)
- Built in crypto-processor supporting upto 1000+ crypto algorithms
- Agile cryptography (crypto algorithm upgrade)
- Software and firmware upgrade capability
- Tamper-proof
- EMI/EMC compatible (MIL-STD-461F, DO-160E & CISPR 25 EMI)

- TEMPEST compliant (SDIP-27 Level A (AMSG-720B) standard)
- COMSEC compliant
- Water and dust-proof (IP67)
- Temperature range (nominal condition): -20°C to +60°C
- Physical sizes (11cm x 8cm x 3cm, 0.3 Kg)

Subject to Approval of Turkey Ministry of National Defence for Selling.
SMART CARD AND ID VERIFICATION SYSTEMS

* Due to ongoing research and development, specifications in this catalogue and its content may change without prior notice.
IDENTITY CARD APPLICATION (Contact Card Feature)
- Visual Authentication
  - Photo, Signature, Guilloche, Rainbow Printing, Multiple Laser Image, Microprinted Text, Raster Printing, Relief Printing, Optical Variable Ink, Ultraviolet Inks, OVD/DOVID
- Electronic Identity Authentication
  - Electronic Certificate, Digital Photo, PIN
- Biometric Authentication
  - Finger Print, Finger Vein Print, Palm Vein Print
- Role Based Access
- Secure Messaging
- Cryptographic Algorithm
  - RSA-2048, SHA-256, AES-256

INFRASTRUCTURE OF ELECTRONIC SIGNATURE APPLICATION (Contact Card Feature)
- Qualified Electronic Certificate and Private Key Loading

TRAVEL DOCUMENT APPLICATION (Contactless Card Feature)
- ICAO 9303 Standard Compliant
- Ability to Travel to Bilateral Agreement Countries without Passport and Visa
- Machine Readable Zone (MRZ)
- Basic Access Control (BAC)
- Active Authentication (AA)
EMBEDDED SECURITY MODULE

Embedded security module is developed to be used in security applications, such as secure storage, access control, authentication for tablet PCs, mobile phones and similar devices. Embedded security module uses UKTÜM-Hv7.0 integrated circuit having EAL5+ certificate and is a reliable alternative from the aspects of functionality, performance, and price.

Embedded security module is used in production of tablet PCs with its QFN package and implements the authentication function which enables the access of only authorized persons to a tablet PC.

FEATURES

- Microprocessor: 8051 based (Internal memory: 256 B)
- Flash Memory: Total 192 KB shared between ROM and data as
  - 64 KB ROM and 128 KB data memory or
  - 128 KB ROM and 64 KB data memory
- SRAM: 8 KB
- Interface: Compatible with ISO/IEC 7816 standard
- Hardware implemented crypto functions resistant to side-channel attacks:
  - DES and 3-DES coprocessors
  - AES-256 coprocessor
  - RSA-1024 and RSA-2048 coprocessor
- RNG: Hardware true random number generator compatible with FIPS 140-2 standard
- Security: Common Criteria EAL5+ certified
  - Security sensors: High-low supply voltage/clock frequency/temperature
  - Efficient protection of integrated circuit surface against attacks
  - Detection of laser and fault attacks
  - Resistant to side-channel attacks
SMART CARD OPERATING SYSTEM & AKİS
Smart Card Operating System is a firmware in ROM or flash memory, which communicates securely with the outer world via several standards (ISO 7816, ISO 14443) and makes it possible to store and manage data in a secure way using several enciphering methods supplied by the smart card firmware.

AKİS (Smart Card Operating System), is a national operating system developed by TÜBİTAK BİLGEM UEKAE and it operates information security, ID recognition, digital signature and secure information exchange applications on smart card chips.

SMART CARD
A smart card module consists of a microprocessor, memory, and a crypto engine. Comprised of only one chip, it has contact-based and/or contactless communication with the outer world while consuming minimum power. When smart card modules are bonded onto PVC, PET or PC cards, the resulting product is called a smart card.

Smart card hardware units are;
- Microcontroller (microcomputer) unit
- File system memory (permanent EEPROM, transient RAM)
- Crypto engine for encryption/signature operations
- Communication unit to communicate with the environment (contact-based or contactless)

FEATURES
- Communication with a card reader by using ISO 7816 (contact-based) and ISO 14443 (contactless)
- ISO 7816 and ICAO 9303 (passport) instruction set support.
- Secure messaging
- Symmetric and asymmetric encryption techniques (3DES, RSA, AES)
- Digital signature (RSA)
- Proprietary File Management System
- Proprietary Memory Management System
- Secure key management and structured security architecture
- Role-based access
- PC/SC, PKCS11, CSP support
- CC EAL 4+ certificate
- Supports UKTÜM, Infineon and NXP chips
AKİS GEZGİN e-PASSPORT

ELECTRONIC PASSPORT

**e-PASSPORT APPLICATION**
AKİS e-passage application is compatible with ISO/IEC 9303 standards. The application that runs on the contactless chip is protected from cloning. Forgery is prevented and the confidential information of the passport holder is stored securely on the chip. The reader can read the information stored on the chip via secure communications only. The information is stored in 11 data groups defined as Logical Data Structure (LDS) on the chip. The Data Group 1 (DG1) is mandatory and the rest are shaped according to local needs of each country.

**FEATURES**
- ISO/IEC 9303 LDS
- Basic Access Control (BAC)
- Active Authentication (AA)
- Extended Access Control (EAC)
- ISO/IEC 14443-3 Type A
- 424 Kbps / 848 Kbps transmission speed
- Secure messaging (3DES and AES)
- Digital signatures (RSA and ECC)
- SHA-1, SHA-256, SHA-384, SHA-512 hash algorithms
- CC EAL5+ Certification

**AKİS GEZGİN E-PASSPORT API**
- AKİS e-Passport Software Development Kit (SDK) supports easy application development through the use of API, DLL and software libraries.

**SUPPORTED HARDWARES**
- Infineon SLE78v2 Series
- NXP P71D320 chip

**PERSONALISATION**
- AKİS e-passage application manages the personalization process of data groups that are compatible with ISO/IEC 9303 standards.
- Command set compatible with ISO/IEC 7816-9
- Flexible and dynamic file management

**AUTHENTICATION**
- e-Passport application supporting ISO/IEC 9303 LDS data groups and digital signature
- Command set compatible with ISO/IEC 7816-4
- Basic Access Control (BAC) support
- Active Authentication against cloning
- Supplemental Access Control (SAC) support
- Extended Access Control (EAC) support

**BASIC ACCESS CONTROL (BAC)**
BAC is a mechanism that ensures only an authorized access from a terminal is allowed for accessing the data stored in the contactless chip via secure messaging only.

**EXTENDED ACCESS CONTROL (EAC)**
EAC is a security mechanism that allows access to biometric data groups stored in the chip through role-based certificates.

**ACTIVE AUTHENTICATION (AA)**
AA is based on digital signatures and prevents cloning e-passage chip.
AKİS GEZGİN e-DRIVER LICENSE

ELECTRONIC DRIVER LICENSE

e-DRIVER LICENSE APPLICATION
Akış Gezgin e-driver license application is compatible with ISO/IEC 18013 standards. The application that runs on the contactless chip is protected from cloning. Forgery is prevented and the confidential information of the driver is stored securely on the chip. The reader can read the information stored on the chip via secure communications only. The information is stored in 24 data groups defined as Logical Data Structure (LDS) on the chip. The Data Group 1 (DG1) is mandatory and the rest are shaped according to local needs of each country.

FEATURES
▪ ISO/IEC 18013 LDS
▪ Basic Access Protection (BAP) (config-1 through config-4)
▪ Active Authentication (AA)
▪ Extended Access Protection (EAP)
▪ ISO/IEC 14443-3,4 Type A
▪ 424 Kbps / 848 Kbps transmission speed
▪ Secure messaging (3DES and AES)
▪ Digital signatures (RSA and ECC)
▪ SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 hash algorithms

AKİS GEZGİN E-DRIVER LICENSE API
▪ Akış e-Driver License Software Development Kit (SDK) supports easy application development through the use of API, DLL and software libraries.

SUPPORTED HARDWARES
▪ Infineon SLE78v2 Series
▪ NXP P71D320 chip

PERSONALISATION
▪ Akış e-driver license application manages the personalization process of data groups that are compatible with ISO/IEC 18013 standards.
▪ Command set compatible with ISO/IEC 7816-9
▪ Flexible and dynamic file management

AUTHENTICATION
▪ e-driver license application supporting ISO/IEC 18013 LDS data groups and digital signature
▪ Command set compatible with ISO/IEC 7816-4
▪ Basic Access Protection (BAP) support
▪ Active Authentication against cloning
▪ Extended Access Protection (EAP) support

BASIC ACCESS PROTECTION (BAP)
TBAP is a mechanism that ensures only an authorized access from a terminal is allowed for accessing the data stored in the contactless chip via secure messaging.

EXTENDED ACCESS PROTECTION (EAP)
EAP is a security mechanism that allows access to data groups stored in the chip through role-based certificates.

ACTIVE AUTHENTICATION (AA)
AA is based on digital signatures and prevents cloning e-driver license chip.
AKİS BİLET
AKİS Bilet is an open specification, multi-application contactless smartcard technology, based on OSPT CIPURSE specifications, developed by TÜBİTAK BİLGEM, member of OSPT Alliance since 2013.

FEATURES
- ISO/IEC 14443 Type A Level 3 - 4
- Data rate up to 848 kbps
- Up to 4 Kbyte user memory
- Up to 8 application support
- Up to 32 files support per application
- Binary, Linear Record, Cyclic Record and Value file types
- Consistent Transaction Mechanism
- Multi-application support
- Random UID support
- True random number generator (TRNG)
- Secure messaging with AES-MAC or AES-ENC
- Data exchange protocol inherently DPA and DFA resistant
- ISO7816-4 based Secure Messaging modes (Plain, MACed, ENced)
- ISO 9798-2 based 3 pass Mutual Authentication (AES128)

APPLICATIONS
- e-ticketing applications
- Closed scheme payment systems
- Personnel attendance control systems
- Access control systems
- Car-park systems
- Libraries
- Health, social relief and loyalty applications
KYS consists of applications capable of managing all the life cycle for official documents such as identity card, driving license, passport etc.

KYS offers applicable solutions for different requirements based on Inventory, Reporting, Personalization and Recording modules available in KYS.

KYS has safely met the requirements of many medium and large scale organizations until today.

GENERAL FEATURES
- **Server:** KYS is independent from platform and database management system and easily integrated to exterior systems via web-services. It realizes the operation logic significantly. It offers role-authority based access and back-up operation support.
- **Smart Card:** KYS is compatible with National Smart Card Operation System (AKİS/UKİS) and JCOP. It is integrated with identity, passport and driving license implementations.
- **Security:** KYS has features including authority based access, safe storage of sensitive data, SSL connection between terminals, operational records with electronic signature and card access to system.
- **PKI:** KYS operates in integration with National Public Key Infrastructure (MA3).

PERSONALIZATION
- Creating application package
- Managing application package
- Customization of application package
- Quality control
- Capability of operation integral with industrial and desktop customization machines
- Terminal and use management
- Announcement management

ENROLLMENT
- Receipt of application records
- Card and application status monitoring
- Accepting mobile (online/off-line) application records
- Accepting bio-metric application records in accordance with standards

REPORTING
- Reporting in accordance with roles
- Card based reporting
- Machine based reporting
- Reporting based on operational records
- Parametric inquiry options
- Output capability in PDF, MS Excel and MS Word formats

INVENTORY
- Enrollment with/without card serial numbers
- Card return, cancellation and destruction operations
- Dissemination of cards to the personalization environment
- End of Day operations
- Safe receipt and delivery
- Declaration of card status summary
This system performs authentication feature while a public service is served to a citizen. By this way, the system verifies whether the citizen who attends the service and the person who serves it are the ones that are declared to be.

**ELECTRONIC AUTHENTICATION SYSTEM COMPONENTS**

**ELECTRONIC IDENTITY CARD**
Identity Card is an official document issued by the Government that authenticates the holder as genuine and justifies the holder's identity in governmental electronic services. Identity Card is a smart card used for personal identity authentication in order to make use of services provided by public service supplier institutions.

**CARD ACCESS DEVICE**
Card Access Device (KEC) is one of the terminal devices of the EKDS. It provides services over electronic media in order to verify that the identity card (ID card) was issued by the authorized institution and the card really belongs to the cardholder.

**IDENTITY AUTHENTICATION SERVER**
Authentication Server is a server that is used to verify the assertions generated by KEC(s).

**IDENTITY AUTHENTICATION POLICY SERVER**
Authentication process is done by each institution according to their policy which depends on the provided service. Some institutions may require only PIN, while others may require both PIN and biometry data for authentication. Authentication policies can be defined on Authentication Policy Server by the institutions.

**SOFTWARE APPLICATION INTERFACES**
The softwares used by institutions can be integrated to the EKDS with the help of software application interfaces. Software Application Interfaces can be either desktop application or server application. Automation Software Interface (OYA/ WIA) is used to integrate the softwares of institutions with the KEC devices.

**IDENTITY AUTHENTICATION FACTORS**
- Physical Authentication
- Secure Message
- Electronic Certificate
- Password (PIN CODE)
- Biometric
- Digital Photo
Card Access Device (KEC) is one of the terminal devices of the Electronic Authentication System (EKDS). It provides services over electronic media in order to verify that the identity card (ID card) is issued by the authorized institution and the card really belongs to the cardholder.

There are two smart card slots on the device. Thus, it is ensured both the service requester (citizen) and the service attender (operator), if required, to be at the same place at the same time. With the help of the Secure Access Module (SAM) included in the device, KEC can get access to the data fields such as the personal message and biometric data of the cardholder, which cannot be accessed with the Standard card reader.

KEC displays the photograph of the cardholder within the card on its colored graphic display. This feature is one step of the identity authentication and requires confirmation of the photograph by the operator at the registration unit. KEC, with the keyboard on it, provides the users to enter their PIN in a secure way. After the secure messaging session is established with the card, the device can read the personal message inside the card, belonging to the citizen and display it on its screen. This is a proof for the users that the operation is performed by using an authorized device. The device is tamper-proof and its application software has CC EAL4+ (ALC _ DVS.2) security level certificate.

**SECURITY FEATURES**
- Authentication using certificate
- Authentication using certificate and PIN
- Authentication using certificate and biometrics
- Authentication using certificate and photograph
- Authentication using certificate, photograph and PIN
- Authentication using certificate, photograph and biometrics
- Authentication using certificate, photograph, PIN and biometrics
KIÖSK-KEC (KIÖSK Card Access Device) is one of the terminal devices of the Electronic Authentication System. Using KIÖSK-KEC, the service requester, on their own, can test their ID card, change their personal message and PIN, remove PIN blockage and display the information within the card.

With the help of the Secure Access Module (SAM) included in the device, KIÖSK-KEC can get access to the data fields such as the personal message and biometric data of the card holder, which cannot be accessed with the standard card reader. The device is tamper-proof and the card access application inside has CC EAL+ (ALC _ DVS.2) security level certificate.

With KIÖSK-KEC, the operation of both contact and contactless interfaces of the card can be tested; authentication certificate, PIN and biometric data inside the card can be verified. Additionally, personal identity information and photograph of the citizen within the card can be displayed on the screen. KIÖSK-KEC allows the users to change the PIN of the card and remove PIN blockage as well. The PIN can be changed by entering the current PIN of the card or through biometric verification. For the PIN blockage removal operation, it is required for the citizen to enter the card’s PUK information. If the citizen doesn’t know the PUK information of the card, this procedure can be done also by biometric verification without the need of the PUK.

SAFETY FEATURES AND FUNCTIONS
- Card test (certificate, photograph, PIN and biometric verification)
- PIN Verification
- Defining the new PIN with the current PIN
- New PIN assignment with biometric verification
- PIN blockage removal with PUK verification
- PIN blockage removal with biometric verification
- Displaying personal identity information (after PIN verification)
- Personal message change
- Displaying contactless interface information
GEM is the security module of Card Access Device which is developed to verify National Identification Card in electronic applications and authenticate the owner of that card. In other words, GEM implements the cryptographic functions of Card Access Device. By means of GEM, it becomes possible to access data fields such as the biometric data of the card owner, and to execute READ/WRITE operations on these fields. Besides, the use of certificates and keys embedded in GEM enables a secure communication with National Identification Card. Concisely, GEM is the module which provides the secure use of Card Access Device and consequently enables the secure authentication of identity information in electronic environment.

**SPECIFICATIONS**
- Communication with ISO 7816 (with contact) standard message sets
- Support of ISO 7816 command set
- Secure messaging
- Symmetric and asymmetric encryption (3DES, RSA, AES)
- Genuine file and memory management system
- Security architecture and secure key management
- Role based access
- Support of PKCS11, CSP
- Common Criteria CC EAL4+ certified
- Compatible with UKTUM, Infineon, and NXP chips
ELECTRONIC CERTIFICATION MANAGEMENT SOLUTIONS

* Due to ongoing research and development, specifications in this catalogue and its content may change without prior notice.
Public key infrastructure (PKI) is a technology built on electronic certificates. Certification Authority (CA) and other supporting software are required in order to create electronic certificates. CA creates certificates for other CA’s, users, servers and devices.

ESYA certification authority is the basic product of National Public Key Infrastructure (MA3) project. ESYA Certification Authority supports industrial electronic certificates standards (X.509, CVC etc.) and provides certificate service providers (CSP’s) with all services required throughout the life cycle of electronic certificates (creation, renewal, revocation, etc.) via a user-friendly interface.

PUBLIC KEY INFRASTRUCTURE SERVICES
▪ X.509 v3 Certificates, X.509 v2 Certificate Revocation Lists (CRL)
▪ Online Certificate Status Protocol (CISDUP/OCSP)
▪ Key Recovery and Update
▪ Qualified Electronic Certificate
▪ SSL (Host and Client), VPN
▪ Windows Smart Card Logon Certificate, Windows Domain Controller Certificate

CRYPTOGRAPHIC FEATURES
▪ RSA algorithm (1024, 2048, 4096 bit key lengths)
▪ ECDSA algorithm (163, 192, 256, 368, 431, 512 bit key lengths)
▪ SHA1, SHA256, SHA384, SHA512 hash algorithms

CRYPTOGRAPHIC HARDWARE SUPPORT
▪ PKCS11 compliant smart cards and tokens
▪ HSM (Hardware Security Module) support
Thanks to widely used internet and computer systems, companies and organizations can require their employees cooperate together and share information extensively even if they are located at different places. E-mail services play significant role as means of information sharing and they gain importance day by day. It has become very usual to have reports, plans and design documents containing proprietary corporate data flowing over e-Mail servers. These e-Mails and documents mostly remain accessible to unauthorized people. Having accessed by malicious people, the leakage of those valuable e-Mails can cause severe commercial damage and weaken the brand power of the company which makes e-Mail protection and desktop computer security solutions clear requirements for desktop and portable computer.

**MAIN COMPONENTS**
- Secured e-Mail module
- Desktop computer security module
- Kermen Sur

**SECURITY SERVICES**
- Secure E-mail (SMIME)
- File signing/encrypting
- Secure index
- Certificate validation
- Secure deletion

**CRYPTOGRAPHIC FEATURES**
- Work with X.509 v3 Certificates which are prepared by using RSA, DSA and Elliptic Curve algorithms
- Using 3DES, AES algorithms for PKCS7/CMS
- SHA-1 and SHA-2 family, message abstract algorithms
- PKCS12 and PKCS5, password based encryption algorithms

**CRYPTOGRAPHIC HARDWARE SUPPORT**
- Work with PKCS11 compliant smart cards and tokens
- In the absence of smart cards and tokens, the keys are taken by PFX files and securely stored/used in local storage
ELECTRONIC SIGNATURE LIBRARIES

IT investments of institutions/organizations increase day after day and hardware and software parks grow like a snowball. One of the biggest challenges of this growing up is that every new hardware and product needs to be integrated with existing systems. While using information security products the integration needs more attention since ensuring the security of the systems requires lots of expertise. Hence, institutions/organizations generally prefer experts when they are seeking information security solutions.

ESYA e-Signature libraries, developed with TÜBİTAK BİLGEM’s more than ten years of e-signature experience, enable fast and secure electronic signing. Also, they are fully compatible with international standards and pass the security tests successfully. The libraries are implemented in JAVA and .NET platforms in order to provide easy and convenient integration with e-signature technology.

SUPPORTED STANDARDS
- ETSI TS 101 733 CAdES electronic signature format (ASN data structure)
- ETSI TS 101 903 XAdES electronic signature format (XML data structure)
- ETSI TS 102 918 Associated Signature Containers

SUPPORTED SIGNATURE TYPES
- Basic Electronic Signature (ES-BES)
- Electronic Signature with Time (ES-T)
- Explicit Policy-based Electronic Signature (ES-EPES)
- ES with Complete Validation Data References (ES-C)
- Extended Electronic Signature with Time (ES-X)
- Extended Long Electronic Signature (ES-XL)
- Archival Electronic Signature (ES-A)

CRYPTO HARDWARE SUPPORT
- Working with PKCS11 compatible smart cards and sticks
- Working with Hardware security modules (HSM)

CRYPTO FEATURES
- RSA, DSA, and Elliptic Curve algorithms designed to work with X.509 v3 certificates
- SHA-1 and SHA-2 family message digest algorithms

ADVANTAGES PROVIDED
- e-Signature Standards: International and national e-Signature standards, laws, regulations and full compliance with the regulations
- Full compliance with PKI certificates and effortless access to key services
- High Technology: Security smart card in order to maximize/bar use
- National software compatible with international safety standards
- Mobile Technology: Android devices, interoperability, Avea/Turkcell mobile signature to use
- Smart Card Support: smart card transactions from different brands. APDU smart with the Flow faster processing to make the cards
- Ease of use: alter the approach to your habits. Support in Turkish.

TIME STAMP SUPPORT
- Authentication of time stamp information can be checked like signatures.
- All information related to the time stamp of a document can be reached.

ANOTHER KEY INFRASTRUCTURE SERVICES
- X-509 certificate validation
- X-509 certificate-based encryption
- Mobile signature
Timestamp, as defined in international standards, provides legal proof of existence of a digital data at a particular time. Timestamp Server creates timestamps for received digital data compatible with these international standards. For e-documents such as a signed agreement, a transaction or an application etc., proof of the existence at a particular time is very crucial for current e-trade and e-government applications. Timestamp is also required for varying kinds of digital data that need copyright including a new idea, photograph, model, drawing, research, book formula or an algorithm.

According to the Turkish Law No: 5070 on Electronic Signature, Timestamp refers to “the record which is verified by the electronic certification service provider with electronic signature so that the time when an electronic data is manufactured, modified, sent, received and/or recorded could be determined.”

ADVANCED CUSTOMER MANAGEMENT
Timestamp server provides the ability for defining customers with prepaid credit by an advanced customer management interface. Timestamp server creates responses to timestamp requests based on customer information.

TIMESTAMP FILE ARCHIVING
Timestamp Server stores timestamp responses so that they could be verified afterwards.

HIGH PERFORMANCE OPERATION
Timestamp Server processes simultaneous client requests in parallel and responds with high performance.

FEATURES
- RFC 3161 compatible timestamp creation.
- NTP support
- High performance by using HSM (Hardware Security Module)

CRYPTO FEATURES
- RSA and ECDSA algorithms, support for the signature timestamp
- AES encryption algorithms
- SHA-1 and SHA-2 family of hash algorithms

SECURITY SERVICES
- Timestamp using X.509 certificates and public key signing algorithms
- Client authentication using PKCS5

CRYPTO HARDWARE SUPPORT
- The process of signing takes place in secure hardware module (HSM)
IMPLEMENTATION OF DESKTOP SIGNING

With the increasing use of computers, many business processes are carried out via electronic media, and this has led to a decline in paper use. Electronic signature, which is taking place of paper signature, is one of the technologies that has brought about this trend. It enables digital documents to be signed and stored securely with protected integrity. Nowadays, electronic signature has become a security mechanism defined by international standards and gained legal validity. For an electronic signature to be legally valid, it must be created in the correct way and be compatible with those standards, which are quite detailed and frequently updated. For the end-users to follow and stay in accordance with those standards is a difficult and time consuming process. Therefore a simple application for creating signed documents compatible with the standards has become a very valuable tool. Also, Electronic writing (e-Writing) standard package which supports public enterprise’s correspondence among themselves by using electronic signing becomes more and more widespread with time. For those reasons, the tool has been considered necessary for creating and verifying e-writing package. İMZAGER meets those requirements with modern user friendly and comprehensive interface.

SUPPORTED STANDARDS
- ETSI TS 101 733 CADES e-signature format
- ETSI TS 101 903 XADES e-signature format
- ETSI TS 102 778 PADES e-signature format
- Support of e-Writing package
- X.509 v3 certificates
- Cancel list of X.509 v2 certificate (CRL)
- RFC 5280 certificate verification
- RFC 2560 online certificate status protocol (CISDUP/OCSP)
- RFC 3161 Time stamp

CRYPTOGRAPHIC FEATURES
- Work with X.509 v3 Certificates which are prepared by using RSA, DSA and Elliptic Curve algorithms
- SHA-1 and SHA-2 family, message abstract algorithms

CRYPTOGRAPHIC HARDWARE SUPPORT
- Work with PKCS11 compliant smart cards and tokens
- Work with Hardware Security Modules (HSM)
PDF FILE SIGNING
Supported by many operating systems, PDF file format has gained a wide ranging acceptance and is now a commonly used de-facto standard. Besides, the security of electronic documents has become more important as they take the role of paper. That is why, signing a document is one of the basic security operations that preserves its integrity and identifies the author of the document in a secure way. Secure PDF is one of the applications supporting widely accepted digital signature standards on PDF files.

SECURE PDF
Secure PDF supports ETSI PAdES compliant e-signature by using HSM or smart card and X.509 Certificate based encryption for PDF files in a directory.

FEATURES
▪ Password Based System
▪ Bulk PDF File Signing
▪ Bulk PDF File Encryption
▪ Multiple Signature
▪ Timestamp Support
▪ Keyword Filter
▪ HSM and Smart Card Support
▪ Logging with Configuration File and Database

SUPPORTED STANDARDS
▪ X.509 v3 Certificates
▪ ETSI 102 778 PAdES
▪ RFC-3161
▪ PKCS7/CMS Structure

CRYPTOGRAPHIC FEATURES
▪ Work with X.509 v3 Certificates which are prepared by using RSA, DSA and Elliptic Curve Algorithms
▪ SHA-1 and SHA-2 Hash Functions

CRYPTOGRAPHIC HARDWARE SUPPORT
▪ Work with PKCS11 Compliant Smart cards and HSM
With its unique RF hardware and spectrum monitoring software SGS 4.0 provides wideband monitoring capability in the 9 kHz - 2.7 GHz frequency range. The upper limit of the frequency range can be easily upgraded to 18 GHz. SGS simultaneously demodulates and records the outputs of 64 analog signals in a 40 MHz span using the Multi-Channel Signal Monitoring and Analysis (CITA) algorithm.

SGS has many spectrum monitoring capabilities like setting alarms for target frequencies, masking signals that are not of interest, spectrogram analysis and controlling multiple receivers through serial and Ethernet connection. SGS can also be accessed remotely over network. The system outperforms its competitors with a frequency sweeping rate over 15 GHz/s and extraordinary reception sensitivity.

FEATURES
- Frequency Range: 9 kHz-2.7 GHz (Can be upgraded to 18 GHz)
- Real Time Bandwidth: 40 MHz
- Number of Demodulator Channels: 64 (in 40 MHz span)
- Supported Modulation Types: FM, AM, LSB, USB, CW
- Sensitivity: < -140 dBm (270 Hz RBW, Pre-Amplifier enabled)
- Pre-Amplification: 0/20 dB
- Dynamic Range: > 80 dB @ 100 kHz IFBW
- Adjustable Input Attenuation: 0–60 dB (in 5 dB steps)
- Frequency Sweep Rate: 15 GHz/s @ 100 kHz RBW
- Phase Noise: < -90 dBc/Hz (10 kHz)
  - < -90 dBc/Hz (100 kHz)
  - < -115 dBc/Hz (1 MHz)
- Dimensions: 2U height, 19 inch width

Subject to Approval of Turkey Ministry of National Defence for Selling.
FDC101 is a frequency converter which detects signals in 30 MHz-18 GHz frequency range and down-converts them into 3 different intermediate frequency (IF), 70 MHz, 140 MHz and 160 MHz, selectable by the user. In addition to 3 different IF, output of L-Band is at 1 GHz. Real-time bandwidth is 500 MHz at L-Band output. There are 8 bandwidths at 70 MHz IF output: 0.5, 1, 2, 5, 10, 20, 30 and 40 MHz. Only 80 MHz bandwidth is provided at 140 and 160 MHz IF output. In addition to them, PAN IF output also is given at 70, 140 and 160 MHz.

Technical specifications of FDC101 satisfies the requirements of a high performance microwave receiver. FDC101 is designed to detect high data rate PCM/TDM signals and radar signals which require high pulse accuracy. Modern digitally modulated signals, like high level QAM, can be detected by FDC101 having low group delay distortion and ultra-low phase noise.

**FEATURES**
- Frequency range: 30 MHz-18 GHz
- Real time bandwidth: 500, 40, 30, 20, 5, 2, 1, 0.5 MHz
- IF output frequency: 70, 140, 160 MHz and 1 GHz L-Band output
- Gain from RF to IF: > 42 dB
- Dynamic range: 60 dB @ 40 MHz IF Bandwidth
- Adjustable input attenuation: 0-70 dB (every each step: 10 dB)
- Frequency locking time: 1 ms
- Phase noise: < -110 dBc/Hz (100 kHz offset)
- Dimensions: 2U height, 19 inch width
- Remote Control: Ethernet
FDC201 is designed to extend the operating frequency range of downconverters such as FDC101. Signals between 18 – 40 GHz are down-converted to the 2.5 – 17.5 GHz range so that signals fall to the FDC101 frequency band. The device’s superior technical specifications allow it to support SIGINT applications.

The device has 3 RF inputs and one RF output. The first input band is 0.1 – 18 GHz and is bypassed to the output directly without any frequency conversion. 2nd and 3rd input connectors cover 18 – 26.5 GHz and 26.5 – 40 GHz bands respectively, and these frequencies are downconverted to the 2.5 – 17.5 frequency band and transmitted to the output port. 10 MHz reference in&out connectors are also found on the rear panel.

The FDC201 is a 2U height, 19” standard rack-mount device. In addition to front panel controls, RS232 and Ethernet connections enable the device to be controlled remotely.

ÖZELLİKLER
- Frequency band: 18 GHz – 40 GHz
- Noise figure: 10 dB (typical)
- IF output frequency band: 2.5 GHz – 17.5 GHz
- RF to IF gain: 12 dB (typical)
- Input P1dB: -5 dBm (typical)
- Image rejection: 75 dB (typical)
- Phase noise: 0.4° RMS (typical)
- Dimensions: 1U height, 19” width
- Remote control: Ethernet and RS232
FD300A is designed to solve incompatibility issue between microwave receivers with multiple frequency outputs and devices that record, digitize, display and analyze IF outputs used in electronic intelligence systems.

Besides the FD300A converts 10-300 MHz carrier frequencies to 70, 140, 160, 10.7, 21.4 MHz standard intermediate frequencies and frequencies between 10-65 MHz in steps of 5 MHz, it can also convert 1 GHz carrier frequency to the specified intermediate frequencies. Moreover, in bypass mode, the input signal is transferred to the output either filtered or unfiltered. The device has a filter block, offering the user to choose eight different bandwidths around 70, 140, 160 MHz, at the output and provides automatic and manual gain control.

With the help of video output at 160 MHz, FD300A makes it easy to measure pulse modulated signals. All the functions of the device can be controlled via its keypad or a computer connected to the device through its Rs-232 or Ethernet interface.

**SPECIFICATIONS**

- Input Frequency Range: 10 MHz-300 MHz & 1 GHz (Resolution: 100 kHz)
- Output Frequencies: 70, 140, 160 MHz (IF OUT);
  70, 140, 160, 10.7, 21.4, 10 > 65 MHz (PAN IF OUT)
- Noise Level: 14 dB (typical)
- OIP3: +18 dBm (minimum)
- P1dB: +17 dBm (typical)
- Max. Gain from RF to IF: 45 dB (minimum)
- Phase Noise @100 kHz Offset: -109 dBc/Hz
- Image Frequency Suppression: 90 dBc
- Device Management: Via keypad or a computer connected to RS-232/Ethernet interface
- Connector Type: BNC
- Power Supply: 198-242 VAC, 47-53 Hz
- Weight: 9.5 kg
- Operating Temperature: 0-50°C
- Input-Output Impedance: 50 Ohm (IF In & Out), 93 Ohm (Video Out)
- Dimensions: 2U height, 19 inch width, 53 cm depth
YTA-018D
SOFTWARE-BASED WIDEBAND RECEIVER

YTA-018D is a software receiver which detects the signals between 10 kHz-18 GHz frequency range and then demodulates the common modulation types such as AM, FM, ΦM, SSB, DSB, PSK, QAM. The system can process and monitor the signals coming from antenna and also it can down convert them to 70 MHz and give off through IF output at the front panel. Therefore, this system is a spectrum monitoring system and a highly sensitive receiver, as well.

As the dynamic range of YTA-018D is high (12 dB typical noise level, 0 dBm IIP3) and as it has a highly sensitive performance (130 dBm/Hz), the system can be used to receive the radar and other communication signals too. Moreover, the system has high image frequency suppression by suppressing minimum 90 dB, typically 100 dB through whole working band.

In addition to self test and calibration functions, the system can also be controlled remotely through Ethernet interface.

The power consumption of the system is 80W at spectrum scanning mode. The power is supplied from a battery and the system operates 2 hours continuously.

SPECIFICATIONS
- Frequency Range: 10 kHz-18 GHz
- Real time Bandwidth: 40 MHz
- Sensitivity: < -130 dBm
- Gain from RF to IF: > 45 dB
- Dynamic Range: 65 dB at 40 MHz IF Bandwidth
- Adjustable Input Attenuation: 0-70 dB with 10 dB steps
- Frequency Scanning Speed: 10 GHz/s @ 100 kHz CBG
- Phase Noise: -115 dBc/Hz (100 kHz Offset)
- Size: 7 cm x 28 cm x 43 cm
- Remote Control Interface: Ethernet
**YTS2000**

**NON-LINEAR JUNCTION DETECTOR 2000MHZ**

**SYSTEM FEATURES**
- Semiconductors can be detected in high accuracy and precision.
- Hand-held and user friendly.
- Hidden any electronic devices (audio/video record systems etc.) can be detected in high performance.
- High RF transmit power and receive sensitivity. Hence most of the electronic devices can be detected.
- High operation frequency gives opportunity to find smaller electronic devices.
- Circular transmit and receive antennas. This feature provide both less scanning time and high accuracy.
- Touchscreen LCD display.
- Provides both audio and display indicators to alert the operator.
- Provides signal analysis algorithm to operator for detailed evaluation.
- Both English and Turkish interface.

**APPLICATIONS**
- Detection of any hidden electronic record systems.
- Detection of any active/passive RF transmitter/receiver.
- Detection of any hidden open/closed mobile phones.
- Localization of detected electronic devices.
- Detection of electronic controlled explosives.

**TECHNICAL SPECIFICATIONS**

<table>
<thead>
<tr>
<th>Component</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RF Transmitter</strong></td>
<td>Operating Frequency Range 2000MHz - 2050MHz</td>
</tr>
<tr>
<td></td>
<td>Channel Number 50</td>
</tr>
<tr>
<td></td>
<td>Frequency Hopping Range 1MHz</td>
</tr>
<tr>
<td></td>
<td>RF Transmit Power 33dBm (15dB tune range)</td>
</tr>
<tr>
<td></td>
<td>Modulation Pulsed/CW</td>
</tr>
<tr>
<td></td>
<td>RF Transmit Antenna Circular polarized, 6dBi</td>
</tr>
<tr>
<td><strong>RF Receiver</strong></td>
<td>Operating Frequency Range 4000MHz – 4100MHz (2. Harmonic)</td>
</tr>
<tr>
<td></td>
<td>6000MHz – 6150MHz (3. Harmonic)</td>
</tr>
<tr>
<td></td>
<td>RF Sensitivity -135dBm</td>
</tr>
<tr>
<td></td>
<td>RF Receiver Antenna Circular polarized, 4dBi</td>
</tr>
<tr>
<td><strong>HMI</strong></td>
<td>Video 3.2” coloured touchscreen LCD display</td>
</tr>
<tr>
<td></td>
<td>Audio Buzzer and headphone</td>
</tr>
<tr>
<td><strong>Power and Mechanic</strong></td>
<td>Battery Li-ion battery (1 hour life-span), spare battery</td>
</tr>
<tr>
<td></td>
<td>Size About 20cm x 30cm x 11cm</td>
</tr>
<tr>
<td></td>
<td>Weight About 2kg.</td>
</tr>
<tr>
<td></td>
<td>Extension Range 1m (Telescopic Extension Arm)</td>
</tr>
</tbody>
</table>

Subject to Approval of Turkey Ministry of National Defence for Selling.
DATA VALORISATION SOLUTIONS

* Due to ongoing research and development, specifications in this catalogue and its content may change without prior notice.
IYON SUITE
FORENSIC IMAGE ENHANCEMENT & RESTORATION SOFTWARE

TECHNICAL SPECIFICATIONS
IYON SUITE presents solutions and tools as a software package in the field of image and video processing. This software has advanced video/image filters that are designed dedicatedly for needs of criminal image investigation labs.

IYON SUITE for video and images:

▪ Enhancement/Reparation
▪ Focus distortion/Noise removal
▪ Geometric distortion removal
▪ Interpolation/Dimensional change
▪ Compaction error removal
▪ Video fixation
▪ Domain conversion
▪ Video moving estimation
▪ More than 70 advanced filters, for instance, super resolution filters

APPLICATION PROPERTIES

▪ Update with Novel Methods
The application is not limited to the present image enhancement methods and algorithms. Due to the ability of adding novel methods as plug-ins, the methods and algorithms can always be updated, included or excluded to satisfy the current requirements.

▪ Defining New Methods in Block Applications
While enhancing distorted images, usage of multiple methods may be required in certain cases. The developed application has the capability of combining many methods into a single method and by this feature, which is called Block Application, the user is provided with creative and flexible solutions.

It is distinguished from similar softwares with following features:

▪ Block-based filter interface
▪ Advanced ability of adding new algorithms as plug-ins
▪ Advanced tools for image/video processing
ARCADE (ALLIED RADIO FREQUENCY COMPUTER AIDED DATA EXCHANGE)
Developed to simplify the process of construction, synchronization, querying and management of spectrum data in SMADEF-XML format by NATO Spectrum Management Community and NATO SMB (Spectrum Management Branch).

GENERAL ABILITIES
- Packaging, downloading and querying SMADEF-XML formatted data in a local database
- Displays frequency assignments on a geographic map
- Intermodulation calculations
- Spectrum analyzer
- Assignment usage periods, occupancy charts
- Synchronization of local database from a central database

SMIR-ONLINE (Spectrum Management Information Repository - ONLINE)
Developed using SOA architecture to access central SMIR database and manage spectrum assignment processes using up to date data through network, using web services and web interface.

GENERAL ABILITIES
- Access to up to date data in central SMIR database
- Provides all abilities of ARCADE without a setup, through a web browser over a network
- Simplifies application of NATO spectrum management processes
- Easy SMADEF-XML data construction via Dataset Wizards
- Frequency Nomination Tool
- Peer-to-peer HF and VHF analysis
- VHF Coverage Analysis
- Ability to display map background from online map servers
CIVIL AVIATION SOLUTIONS

* Due to ongoing research and development, specifications in this catalogue and its content may change without prior notice.
Low altitude aircrafts in VFR flight such as helicopters are not trackable by RADAR systems. Fatal helicopter crashes in the past have underlined the need to track and locate such low altitude flights. The Helicopter Tracking System (HATS), which was developed with the General Directorate Of State Airports Authority (DHMİ), is expected to aid in the quick determination of aircraft’s exact location after accidents.

**FEATURES**
- Uninterrupted data acquisition, processing and recording
- An extendible server architecture with back-up features
  - Double back-up server stack
  - Data storing with back-up
  - Double back-up firewall
  - Back-up network and power connections
- Secure Access through intranet with defined user/client authorization
- Desktop clients supported by high performance geographical information system and vector maps
- Authorized continuous tracking and retrospective querying capability
- Authority groups and aircraft groups determination capability
- Push-to-talk (PTT) voice communications with aircrafts
- Automatic Emergency Declaration for loss of communications with an aircraft
- Declaration of emergency status with SMS and e-Mail

**HELICOPTER TRACKING SYSTEM**
The Helicopter Tracking System consists of a Helicopter Tracking Device (HATC) fitted to the aircraft, and a Helicopter Tracking Center (HATM) on ground. Aircraft location, speed and altitude data is periodically transmitted to the monitoring center where it is displayed on a map. Aircraft in distress are highlighted on the monitoring center map display and an audio warning is sounded. Voice communication between aircraft unit and the monitoring center using a “push-to-talk” interface is made possible over GPRS.

As both GSM and satellite links are used for communications, system is both cost effective and reliable. Even if the aircraft unit discontinues functioning after a crash, the last reported location will greatly help search and rescue efforts.
HATC is the vehicle mounted part of the Helicopter Tracking System. The device gets the location, speed and altitude data from the air vehicle sensors and sends these data to the Helicopter Tracking Center through GSM and LEO Satellite communication interfaces. HATC, which was developed with the General Directorate of State Airports Authority (DHMİ), HATC, also brings availability to make push to talk based voice communication through GPRS network.

HATC is a EASA certified equipment under STC 10045303.

MECHANICAL INTERFACES
HATC is designed to be placed in the operator console by 4 DZUS screws

- Width: 145.50 mm
- Height: 104.00 mm
- Depth: 144.95 mm
- Weight: 2700gr

ENVIRONMENTAL CONDITIONS

<table>
<thead>
<tr>
<th>DO-160G Characteristics</th>
<th>Section</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Height</td>
<td>4.6.1</td>
<td>BT</td>
</tr>
<tr>
<td>Temperature Variation</td>
<td>5.0</td>
<td>C</td>
</tr>
<tr>
<td>Shock &amp; Crash Safety</td>
<td>7.0 A</td>
<td>A</td>
</tr>
<tr>
<td>Vibration</td>
<td>8.0</td>
<td>U(G)</td>
</tr>
<tr>
<td>Waterproof</td>
<td>10.0</td>
<td>W</td>
</tr>
<tr>
<td>Salt &amp; Fog</td>
<td>14.0</td>
<td>S</td>
</tr>
<tr>
<td>Magnetic Effect</td>
<td>15.0</td>
<td>Z</td>
</tr>
<tr>
<td>Power Input</td>
<td>16.0</td>
<td>B</td>
</tr>
<tr>
<td>Voltage Spike</td>
<td>17.0</td>
<td>B</td>
</tr>
<tr>
<td>Radio Frequency Energy Emission</td>
<td>21.0</td>
<td>M</td>
</tr>
<tr>
<td>Electrostatic Discharge</td>
<td>25.0</td>
<td>A</td>
</tr>
</tbody>
</table>

HATC has internal and external crash sensors for automatic emergency notification. The device also has a manual emergency feedback button. Furthermore, LED warning indicators provide feedback regarding the emergency situation and device self-test results.

HATC is powered from 28VDC power supply located in the air vehicle. In case of a power loss, there is an internal battery which allows the device to operate for a minimum of 30 minutes. The battery is regularly charged by a smart charging unit. The power loss during the flight is evaluated as emergency and reported to the Helicopter Tracking Center.
atcTRsim
AIR TRAFFIC CONTROL TOWER AND RADAR SIMULATOR

GENERAL FEATURES

▪ Each controller working position can work with a required pilot working position independently.
▪ In each exercise, each controller working position can work in required sector with required number of controller and pilot working position.
▪ Parallel runway training
▪ 360 degree visual tower ambiance
▪ Integrated work for whole working positions in one exercise
▪ Instructions can be set by FMS to the air and ground vehicles from user interface by using mouse and keyboard.
▪ Push-back, taxiing and ground movements
▪ SID, STAR and procedure application
▪ Parallel and sequential command processing for air and ground vehicles.
▪ Transponder functions such as Mode-C, Mode-3/A, Mode-S etc.
▪ Electronic strip method
▪ Flight plan management and available flight plan database.
▪ Automatic exercise preparing.
▪ AIP compatible air space, AIXM and ARINC-424-18 standard air space support.
▪ Navigation device model and simulations such as VOR, DME, ILS, NDB
▪ SSR, PSR and meteorology radar simulations
▪ ADS-B and A-SMGSC simulations
▪ AIP compatible lighting according to ILS category I-II-III
▪ 3D models for Istanbul Ataturk, Antalya, Ankara Esenboga and Erzincan Airports
▪ Airport control special effects
▪ 3D air and ground vehicle models
▪ 3D organic models such as bird flock, human etc.
▪ Developed with the General Directorate of State Airports Authority (DHMİ).
ATCSES, which was developed with the General Directorate of State Airports Authority (DHMİ), tests skills that are required for being an air traffic controller (reflex, three-dimensional thinking, quick decision making, memory, attention, etc.) in an electronic platform. 17 test applications for measuring 9 different skills and one character analysis test are developed.

**TEST PRODUCTS**
- Mind Picture Test: The ability of mind picturing of possible results of a scenario, according to given data
- Visual Memory Test: The subject’s ability to memorize numbers, letters or objects
- Reasoning Test: The subject’s ability to make correct inferences with analysis
- Cross-check test: The ability to fulfill the intended duty with following multiple cases
- Complex Attention Test: The ability to follow the situation without breaking concentration in altering conditions
- Audial Memory Test: The subject’s ability to memorize heard sounds
- Psychomotor Test: The subject’s ability of hand-eye coordination and reaction speed
- Mathematical Insight Test: The ability to perform fast arithmetic operations
- English Listening Comprehension Test: The ability to understand spoken English
- Personality Test: Subject’s personality traits (extraversion, neuroticism, openness, agreeableness, conscientiousness) and other features like self-confidence, team work, emotional stability.

**EXAM FEATURES**
- Production of test question without storing in a data base
- Determination of order of questions in a test
- Adjustment of level of hardness, number, percentage and duration of questions
- Following state of candidates
- 3 sessions for each test group; introducing video, practice questions and test

**OTHER FEATURES**
- Supporting all platforms (Win, Linux, Pardus)
- Turkish-English language support
- Access to the system over web
- Addition and removal of new tests
- Automatic session making according to the number of candidates
- Flexible user authorization infra-structure

**SECURITY FEATURES**
- Dynamic question production for each test
- Database security and encryption
- Test on only identified computers
- No interference to questions and results of test
- Questions can be seen by candidates only

**VALIDATION STUDIES**
- Application to different groups
- SPSS analysis of results
- Item analysis
- Test-Retest method
The KUŞRAD system, which was developed with the General Directorate of State Airports Authority (DHMİ), is designed to operate uninterruptedly 24 hours a day with a coverage volume of a maximum 40 km range in horizontal axis. It can detect targets and classify them as “Bird”, “Flock of birds” and “Aircraft”. It provides operator(s) target data including target range, altitude, heading, route/trajectory and velocity. The system can be used to track migratory bird movements in critical airspaces around civilian airports to evaluate their treat to safety, and can help in the planning of scheduled flights to reduce accident risk.

TECHNICAL FEATURES

- Horizontal Radar (HR): S-Band pulse radar
- Vertical Radar (VR): X-Band solid-state, Frequency Modulated Continuous Wave (FMCW)
- Working mode:
  - Mod 1: 3D volume detection and tracking
  - Mod 2: 2D HR detection and tracking, VR sectoral high resolution Doppler analysis
- Antenna Beam width: 1.8° horizontal, 25° vertical (HR); 0.8° vertical, 10° horizontal (VR)
- Antenna Rotation Speed: 21 rpm (VR); < 100°/sec (VR)
- Detection & Tracking Range: 40 km (HR); 20 km (VR)
- Resolution: < 20 m (HR); < 6 m (VR)
- Output Power: 60 kW peak (HR); 20 W continuously (VR)
- Pulse Width: 0.2 - 0.6 μs (HR)
- PRF: 1100 - 600 Hz (HR), > 3200 Hz (VR)
- Doppler Processing: > 32 filter banks (VR Mode 2)
- Tracking Speed Limits: 2-100 m/sec
- Number of Targets: < 500

COMPONENTS

- Radar Location/Shelter(HR, VR, signal processing unit of detection & tracking configuration & maintenance FC, GPS receiver, meteorological measurement sub-system, UPS)
- Operation Center (Data Recording Unit, Operator Graphical Interface Console, server and storage units, printer and UPS)

FEATURES

- 3D Detection & Tracking of avian targets
- Classification of avian targets (as Bird, Flock of birds and Aircraft)
- Visual and/or audio warning upon detection of targets classified as “Bird” or “Flock of birds” in operator defined critical region(s)
- Detailed (Doppler) analysis of any operator designated target(s)
- Recording and statistical analysis of detection and tracking data
- Remote access to statistical data and network connection
- Vertical and Horizontal Radar data fusion
- Reporting outputs in ASTERIX standard
- Video recording and replay
This primary surveillance radar (PSR) system, which was developed with the General Directorate of State Airports Authority (DHMİ), is an S-Band solid state pulse Doppler radar. It has been developed for civil or military air traffic control and precipitation status determination. The system has been designed in accordance with ICAO and EUROCONTROL standards and guidelines. By using coherent advanced signal processing, aircrafts up to 60 nautical miles under different weather conditions can be detected and tracked. The system can simultaneously track up to 1,000 targets via Moving Target Detection (MTD) and Clutter Reduction capability by using low/high beam selection, sensitivity time control (STC), adaptive clutter map and Doppler filters. Also, the weather channel can provide 6 levels of rain strength information at 1,4° to 0,95 nautical miles resolution and 2D location of rain zones. The system has a clear spectrum output in accordance with the limits defined by NTIA.

**TECHNICAL PROPERTIES**
- S-Band solid state pulse Doppler radar
- Coherent signal processing
- Pulse compression (Nonlinear FM)
- PRI/PRF Staggering
- Frequency Staggering
- Doppler filter banks and MTI
- Weather channel with 6 levels of precipitation reporting
- Antenna beam (modified cosecant squared 45° vertical (low and high beam), 1,45° horizontal)
- Circular and linear polarization
- Antenna rotation speed >= 12 rpm
- Max. Range: 60 nmi
- Range resolution < 200 m
- Power >=18 kW peak
- PRF: staggered PRF (830 Hz average)
- Doppler processing: > 4 bank Doppler filtering
- Target tracking speed interval 60–300 m/s
- Maximum number of targets 1,000
- Weather channel resolution 1,4°–0,95 nmi / 6 levels rain information
- Interface PPI console
- System interface EUROCONTROL ASTERIX CAT240 video, CAT34 service messages, ASTERIX CAT48 plot/track

**CAPABILITIES**
- Detection and tracking of airborne targets
- Detection of precipitation level and zones
- User friendly GUI design
- Static (ground) clutter reduction
- Radar remote management and monitoring
- Video recording and playback
- Output reporting in ASTERIX format
AsterixCARE, which was developed with the General Directorate of State Airports Authority (DHMI), is a powerful and extendible tool set for testing, analysis and validation of surveillance data. The software enables recording, replay and export of recorded data into different formats such as excel, txt, etc.

AsterixCARE has user-friendly graphical interface and flexible software for ATC environments and radar system operators. Data is decoded according to ASTERIX which is a Eurocontrol referenced standard.

**Key Features**

- Online monitoring: Simultaneous recording and synchronized replay of multiple data streams
- Plug-in based software: New categories can be added
- Exportable radar data into other formats (excel, txt etc.)
- Offline running is possible by replaying record files
- Radar data recording in ASTERIX final format (Eurocontrol standard)
- Radar data filtering by different parameters
- Traffic and track informations can be displayed in 2D or 3D
- Weather data display
- Alerts and notifications for invalid and non-compliant data to standard
- Mode S, ADS-B, ASMGCS and Multilateration data format support
- Different map layers can be added (i.e. airspace layers)
- Accessing to all ASTERIX data fields
- Zoom, distance measurement, history trail and track labels
RAILWAY TRANSPORTATION SYSTEMS

* Due to ongoing research and development, specifications in this catalogue and its content may change without prior notice.
DTKM provides monitoring and control capability for rail traffic on the railway network. Traffic Control Operators, also known as Dispatchers, are able to fulfill their duties using this system safely and efficiently.

**GENERAL CAPABILITIES**

**FIELD MONITORING AND CONTROL**
- Real-time monitoring of the railway network
- Management of train traffic
- Single and group control of trackside equipment
- Real-time visual/audible warnings and alarms
- Coordination with timetables, instant monitoring of delays
- Authorization based user identification
- Communication with neighboring traffic control centers

**TRAINGRAPH**
- Storage and graphical display of the location-time data of all trains on the network
- Capability to analyze the traffic density in the network
- Monitoring of train synchronization between stations
- Detection of red light violation of the trains

**PROTOCOL DATA RECORD**
- All events on the network, commands given to the system and system responses are securely logged for later examination
- Logs may be retrieved using a wide range of filtering criteria
DAS has been developed to meet the need for reliable, safe and cost-effective interlocking systems for conventional railway lines using commercial off-the-shelf hardware.

The open interfaces of the system provide interoperability with different manufacturers and trackside equipment thus providing the flexibility necessary to meet the interlocking needs of varied railway lines.

The scalable and functional architecture of the system makes it applicable for extensive station regions, whereas the modular architecture leads to expandability. Comprehensive failure detection capabilities provide instant fault diagnosis contributing to the sustainability of system operation.

Safety standards: CENELEC SIL4 EN 50126, EN 50128, EN 50129
TRENSİM is an E 43000 electric locomotive simulator using advanced virtual environment technologies for the purpose of carrying out driver training comprised of basic driver training, advanced driver training in varying weather conditions, development of fault and risk avoidance techniques, and monitoring and improvement of driver performance.

The E 43000 model locomotive simulator has been delivered to Turkish State Railways Eskişehir Training Center.

**FUNCTIONS**

- To improve train driver skills
- To assure the proper use of cab instruments
- To impart skills necessary in all types of road and climate conditions
- To provide familiarity with operational procedures, speed limits and safety regulations
- To improve use of traction motor and brake for energy efficiency
- To impart experience in handling equipment malfunctions
- To objectively evaluate and score driver’s performance
- To provide distance learning facilities in support of simulator training

**GENERAL FEATURES**

- 3-D locomotive, wagon, rail line and environment modeling
- Real-time simulation
- Mathematical models of locomotive behavior (movement, electric, air brake, etc.)
- Cab movement simulator on moving platform
- Integrated distance learning
- Real-time and offline performance evaluation
BIOELECTRONIC DEVICES AND SYSTEMS

* Due to ongoing research and development, specifications in this catalogue and its content may change without prior notice.
MiSens® is a mobile, fully-automated biosensor device that can be used in vehicles or on a desk. MiSens, its plug and play biochips (patent application no: PCT/IB2015/052479) can be used to detect target analytes in liquid samples. It has uses in medical diagnostics, biodefense, food, environmental safety and R&D.

MiSens device can be controlled from the remote control app on a tablet / PC or its on-device touchscreen with minimal training of the user. The platform is flexible and allows users to design their own tests with ease.

**FEATURES**
- Lab-on-a-chip technology
- High-precision tests using nanotechnology
- Multiple use of the biochips with surface regeneration
- Rapid results using new REP™ (Real Time Electrochemical Profiling) platform
- Controlled by MiCont™ software over WiFi
- Easy to use with on-device 4.3” LCD touchscreen

BiSens™ is a handheld, on-site biosensor device, which allows the detection of analytes without any necessity of an expert user or a laboratory owing to its single use cartridge system.

The device can be used for on-site medical diagnostics, biodefense, food and environmental safety. It can be easily adapted to detect new targets thanks to its easily adaptable single use cartridge mechanism.

**FEATURES**
- Single use cartridges
- Lab-on-a-chip technology
- High-precision results with nanoparticles
- Rapid results using new REP™ platform
- On-device 4.3” LCD touchscreen
- Battery operated for the field use

**TECNOLOGICAL INNOVATIONS**
- Single use cartridges with integrated biochips
- Real time sensing by Real Time Electrochemical Profiling™
**SOBE™** is an optical, handheld, transcutaneous bilirubin measurement device which helps in the diagnosis of jaundice seen in the newborn babies (patent application no. PCT/IB2016/050375).

The medical professional can easily see and make sense of the results in a graph screen, store the results for future reference or transfer them to the patient database in a medical IT infrastructure. The device has a small and ergonomic footprint and requires low maintenance for easy care.

**FEATURES**

- Measuring wide range optic spectra
  - Reflectance spectrum between 400-750nm
- Easy to use and evaluate
  - Touch gently on patients to measure
  - Results on the risk curve
- Long battery life
  - 1200 mAh battery enables up to 500 measurements
- 2.4” easy to read touch-screen
ELECTRONIC DOCUMENT AND ARCHIVING SOLUTIONS

* Due to ongoing research and development, specifications in this catalogue and its content may change without prior notice.
Ebru is a document tracking system designed for the security of printed documents. Documents are stamped before print with a specified pattern generated by Ebru system. The stamp process is applied automatically when the document is sent to print within any document processing application. The algorithm of the pattern generator is uniquely developed by TÜBİTAK BİLGEM. With the capabilities of Ebru, it is possible to acquire answers to these specific questions; the document was printed by “whom”, “when” and using “which” printer.

**GENERAL PROPERTIES**

<table>
<thead>
<tr>
<th>Speciality</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stamping the Document</td>
<td>Any document is stamped with the generated pattern before print.</td>
</tr>
<tr>
<td>Decoding the Pattern</td>
<td>With the Stamp Decoper Desktop Application, details of the printed document can be extracted; i.e. the document was printed by whom, when and using which printer, etc.</td>
</tr>
<tr>
<td>Pantograph</td>
<td>Invisible specific pattern is used to stamp document to increase the document security. The pattern becomes clear when the document is reproduced with any photocopier.</td>
</tr>
<tr>
<td>Improved User Interface</td>
<td>With friendly interfaces users can get results easily.</td>
</tr>
</tbody>
</table>

**SYSTEM MANAGEMENT PROPERTIES**

<table>
<thead>
<tr>
<th>Speciality</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adding New Printers</td>
<td>New printers can easily be added into the Ebru system with New Printer Wizard.</td>
</tr>
<tr>
<td>User Profiles and Groups</td>
<td>System allows to add unlimited user profiles and groups.</td>
</tr>
<tr>
<td>Printer Profiles and Groups</td>
<td>System allows to add unlimited printer profiles and groups.</td>
</tr>
<tr>
<td>User Management</td>
<td>New users can be added easily with the wizard. System allows to assign printer devices for each user or group. System allows to migrate existing users from any user management system into Ebru system. User authorization can be done easily with the friendly interface. System allows to deactive any user/user group or printer/printer group</td>
</tr>
<tr>
<td>Monitoring</td>
<td>User’s printing behaviours and Ebru usage frequency can be monitored.</td>
</tr>
<tr>
<td>Search within the Printed Document</td>
<td>Full text search in printed documents can be done.</td>
</tr>
<tr>
<td>Additional properties for System Administrators</td>
<td>Definition of multiple system administrators Compatibility for integration with Active Directory</td>
</tr>
</tbody>
</table>
Digital Storage, Archive and Analysis System (SKAAS) digitally stores and analyzes TV and radio channel live contents (video and audio) of satellite, cable, terrestrial and IPTV broadcasters. The system is compatible with international standards and adaptable to future broadcast technologies. It is capable of streaming, archiving and analyzing up to 400 TV and 1500 Radio channels simultaneously. It has almost unlimited storage capacity.

**GENERAL FEATURES**
- TV and radio channels can be received from satellite, cable, terrestrial and internet medium continuously and hierarchically
- IP streaming (IPTV) for operators at the local network
- Media files can be stored for unlimited time
- Scene boundaries, channel logos can be detected, video clips can be searched on video files, texts can be extracted from video and keywords can be captured from audio files
- High Availability; observation of signal level and state of broadcast, and automatic switching to redundant device
- Hundreds of users can watch/listen stream and archive, and give analyzing orders at the same time without any bottleneck
- Two-step archive architecture; short term files are stored with high resolution in primary storage, long term files are stored with lower resolution in secondary storage
- Checking of archive records against damage and distortion
- Authorized users can upload or extract record
- Support to any size of TV Wall for both live streams and recorded content

**RECEIVER INPUT**
- SD and HD broadcasts in DVB-S, DVB-S2
- Encrypted broadcasts
- Analog TV and radio broadcasts
- DVB-T terrestrial digital broadcasts
- Analog and digital Cable (DVB-C) broadcasts
- Internet TV and radio (IPTV Streams)

**RECEIVER OUTPUT**
- H.264 coded IPTV streams in selected bitrate and resolution
- MP3 coded Radio streams in selected sample rate and bitrate
- MPEG2 Transport Stream support (ISO/IEC 13818-1)
- File Recording according to time duration or size
ARCHIVE MANAGEMENT SYSTEM THAT COMPLY WITH TSE STANDARDS
Records in paper form can be digitally recorded in the Electronic Record Management System (E-BELGEM) using fast and precise scanners. E-BELGEM provides advanced features such as metadata modifications and record modifications on the records for operators.

DOCUMENT DIGITIZATION
- Drag and drop
- Microsoft Office and Email import integration
- Optical Character Recognition (OCR)
- Advanced precision and fast scanner integration

RECORD SHARING
- Common Work Area and Folder Sharing
- E-Government integration
- Document and Workflow Management
- Preview
- Record Content Annotation
- Electronic Record Management
- Institution-specific Taxonomy Tree
- User-specific Control Panel

EFFECTIVE AND FAST ACCESS TO ARCHIVE RECORDS
- Simple search
- Custom search
- Detailed search

E-SIGNATURE AND VIRTUAL NAVIGATION
- E-signature screen
- Virtual Navigation
- Detailed Search

SYSTEM MANAGEMENT
All system management configurations are performed on the system management page that can be accessed from the main page. Only the system administrators are authorized to use this feature. A few tasks that can be executed on this page:
- Users and Groups definition
- User Role and Authorization
- Record-flow definition, Record Type metadata and Record Type group definition
- Repository definition
- System Settings and List
ELECTRO-OPTICS AND LASER SYSTEMS

* Due to ongoing research and development, specifications in this catalogue and its content may change without prior notice.
National Marker Control System is used to prevent distribution of the fuel oil which is obtained through unregistered production or smuggling. The system is developed to control the fuel market in most efficient way and increase the tax revenues.

The system is consisted of MARKER XP National Marker Field Control Devices which are used in field controls to measure the marker concentration, MARKER K National Marker Laboratory Control Devices which are used to measure this concentration in the laboratories of fuel distribution companies and Data Collection Center.

Marker measurement results are obtained in field or laboratory conditions through 3 different optical spectroscopy method in 400-1000 nm spectrum region. Then, these results are instantly encrypted and sent to Data Collection Center through GSM-GPRS. Furthermore, a measurement report is taken from device’s printer. Measurement date, time, location, temperature, the type of the fuel, serial number of the control device and registration number of the control personnel are indicated in this report. Statistical data mining transactions are carried out to the obtained results in the Data Collection Center.

The system is used by Police, Gendarmerie, Coast Guard, Undersecretariat of Customs, Ministry of Science, Industry and Technology, oil refineries, fuel stations, transportation tankers and storage fields to detect and control fuel smuggling.
The hyper spectrum measurements technology is employed for the first time in the next generation questioned documents examination devices which are developed and produced by TÜBİTAK BİLGEM. Hence, many cases about forgery of documents which could not be enlightened by the present technological devices are able to be solved.

Forensic XP-4010 D is developed to examine the originality of documents. Forensic XP-4010 D driven by the hyper spectrum measurements technology helps reveal of forgery of documents like money, cheque, debenture and passport. Among the other important features of Forensic system one should note the non-destructive principles of examination, decision making based on objectively measured optical parameters of the document.

Forensic XP-4010 D is commercially available digital forensic imaging spectrograph for large-scale documents examination and is an advance spectrograph using hyper spectrum measurements.

**FEATURES**
- Hyperspectral imaging in 350-1100 nm spectrum range
- Revealing the presence of visually similar, but chemically different ink by original Spectral Enhancement Procedures
- Revealing invisibly embedded or deleted information
- UV activated security feature examination
- Anti-Stokes features examination
- Pen pressure visualization and trace display using 3D technology
- Numerical imaging filter
- Passport machine readable zone and chip decoder
- Revealing passport hidden data

**MEASUREMENTS**
- Sensitive reflection, absorbance and conductivity spectral measurements
- Color in any pixel FOV: XYZ, xy, uv, Lab, Statistics
- Distance, Radius, Angle: Y
- Rectangle area, any selected area: Y
- Height (3D Shadowing)
DDA-1
QUADRANT PHOTODEECTORS

QUADRANT PHOTODEECTORS
DDA-I quadrant photodetectors have four parallel PIN-diodes on the same silicon substrate. These detectors are optimized for high response at 1064 nm, the YAG laser light wavelength, and offer higher responsiveness and wider dynamic range compared to similar products on the market. DDA-I quadrant photodetector technology is developed and produced entirely by TÜBİTAK BİLGEM.

PRODUCT FEATURES
- Nd: YAG Sensitivity
- High Speed and Accuracy
- Low Capacitance, High Breakdown Voltage
- Low Dark Current
- Wide Dynamic Range
- High Responsiveness

APPLICATIONS
- Pulse Detectors
- Optical Communications
- Bar Code Readers
- Optical Remote Control
- Medical Equipment
- High Speed Photometry

Subject to Approval of Turkey Ministry of National Defence for Selling.
GEZKIY
REAL-TIME IR TRACK PREDICTION AND MANAGEMENT SYSTEM

Passive threats against floating platforms make use of the infrared radiation. GEZKIY system helps the commanding officer of the platform to see the platform itself by the eyes of the potential threats and to manage the platform accordingly. The system consists of thermal sensors mounted on various places and weather and sea water heat, wind speed and other meteorological information gathered from the ship data distribution system and calculates the infrared profile of the platform with the KISY software. KIKTY software then shows the potential threat areas of the platform to the commanding officer. GEZKIY system is being used on Heybeliada and Buyukada ships, which are produced within the MILGEM program.

GEZKIY HARDWARE FEATURES
• Low and high temperature sensors
• Signal converters
• Connection boxes
• GVDS interface
• GEZKIY main panel
• Panel computer
• Ethernet key and power unit

KISY SOFTWARE FEATURES
• Platform radiation images at desired frequencies
• 3-5 micron and 8-12 micron bad selection capability
• Suggestions for profile reduction
• System start/stop and test capability
• Warning in case of system failure
• Over-radiation alarm

KIKTY SOFTWARE FEATURES
• Showing of threat zones on polar screen
• Adding/deleting of threat models

Subject to Approval of Turkey Ministry of National Defence for Selling.
FKDS
FIBER OPTICAL CABLE MONITORING SYSTEM

FIBER OPTICAL CABLE MONITORING SYSTEM
The system is designed to manage the inventory of any fiber network with GIS (Geographical Information System) data and to monitor the network in order to detect aging, cable break and tapping conditions. F/O cables are periodically monitored with optical measurements performed by Remote Test Units (UBD) which are controlled by a Central Management Unit (MDB). Any alarm cases are reported to the system users with geographical coordinates of alarm events by voice and visually.

GENERAL CAPABILITIES
▪ Detailed F/O cable inventory management
▪ Detection of cable break, bending, aging, splice and connector losses with geographical coordinates and display of event locations on the map
▪ GIS based GUI with GIS employed
▪ Highly accurate inventory location with employment of 3D geographical coordinates
▪ Flexible configuration of GIS layers
▪ Automatically updated WEB based user interfaces
▪ Archive and statistical data reporting capabilities
▪ Reusable Show/Hide and Coloring filters
▪ Export of query results into output files
▪ Flexible data input support (draw, file upload, edit)
▪ Internal messaging capability between operators
▪ Error prone, adjustable performance system
▪ Multilanguage support (internationalization)

SECURITY MANAGEMENT
▪ User authentication with smart card and password
▪ Central User Management
▪ Adjustable role based user access management
▪ Management hierarchy for different roles
▪ TLS based secure communications
▪ Internal PKI support, internal certificate authority
▪ Centralized audit management
▪ Secure data storage
▪ Region based authorization control for users
▪ Smart card management for users and devices
▪ Online monitoring of system user logins

Subject to Approval of Turkey Ministry of National Defence for Selling.
CYBER SECURITY

* Due to ongoing research and development, specifications in this catalogue and its content may change without prior notice.
One of the biggest problems of corporate networks dispersed to multiple locations is monitoring and reacting to cyber threats in real-time from system center. Cyber attacks targeting any node on the corporate network can be detected immediately with the Centralized Cyber Threat Detection System, which is developed for this specific purpose. Installing attack detection systems on the critical nodes of the corporate network lets you monitor the cyber attacks targeting the whole network from a single center. Installed attack detection systems can be configured/managed centrally. System can be customized due to requirements of corporations working on a distributed network architecture.

**CAPABILITIES**
- Distributed attack detection system infrastructure
- Monitoring all logs from a single point, featuring cyber-threat detection interface
- Scalable architecture
- Monitoring all logs from a single point with the underlying log fusion layer
- Detecting malicious activities in real-time with blacklist and cyber-threat intelligence support
- Creating new blacklists to define rule lists for filtering systems
- Advanced report module (PDF, HTML, XML, Json)
- Centralized IDS configuration/management module
- Real-time monitoring of the logs
- Geographic awareness map that is updated in real-time
- Integrated operation with Cyber Space Trap System (SORT)
Cyber-attacks to various countries in the recent years is an indicator that Internet has become a battlefield. Cyber Threat Detection and Prevention System is based on detection of threats by systems implemented at critical network connection points and activating defense mechanisms on all systems to block the threats and is a major actor of the cyber defense. The system consists of distributed cyber traps, distributed attack detection systems, virtualization systems and central management system.

This system can be customized in accordance with the requirements and can be used by organizations which have distributed network architecture.

**CAPABILITIES**

- Capability to work with different trap systems supporting different network layers
- Distributed trap systems infrastructure
- Low cost trap system router device usage
- Management of thousands of trap systems by Cyber Trap System Management Interface
- Rule management of all attack detection systems from a single point
- Scalable architecture
- Powerful virtualization infrastructure and management
- Classification of detected harmful software by Harmful Software Screening System
- Integrated Harmful Software Dynamic Analysis Environment
- Monitoring of all logs by powerful log collection infrastructure
- Detection of harmful software distributed via e-Mails by unwanted e-Mail analysis
- Detection of harmful activities with blacklists
- Introduction of new rule sets to the filtering systems with the capability of generating new blacklists
- Advanced reporting system
- Integrated operation with Centralized Cyber Threat Sensor System (STAMPS)
FEATURES
Data Leakage Prevention System is being developed to protect corporate information and to prevent unauthorized leakage of this information from the organization. This system is one of the major security infrastructure requirements of both public and private organizations.

VKÖS will trace network traffic at corporate gateways, track information being processed at user terminals, audit whether information stored on servers is stored at proper locations and with proper policies and prevent data leakage at all locations.

The product, which currently supports Turkish language and text mining, distinguishes itself from competing systems with its performance. This system can be customized according to specific customer requirements and can be integrated with other security solutions of Cyber Security Institute.

CAPABILITIES
- Central web based management
- Online and offline functioning capability of the agents
- Controlled transfer of information to USB, CD, DVD, etc. media
- Controlled text and file transfer over HTTP/S, SMTP and FTP protocols
- Specific audits for file, WEB and database servers
- Prevention of data leakage via screenshot images
- Definition of sensitive data at folder, file, paragraph and expression levels
- Central management and reporting of data leakage incidents

SUPERIORITY
- Based on corporate software development practices
- Support for the language of customer and morphological analysis
- Detection of sensitive data using text mining
- Usage of sensitive data definitions specific to required language
- Control at operating system drivers level
- Minimal performance reduction with acceptable levels of resource allocation
One of the important approaches to assuring the security of corporate IT systems and applications is moving the IT systems to a virtual environment. All sorts of attack and defense scenarios may be executed and verified on that virtual environment. “SiberMeydan CTF” product includes scenarios featuring all kinds of vulnerabilities that may be found on network components, clients, servers and corporate services.

Common exercises or team competitions may be conducted on SiberMeydan CTF environment. Different types of competitions such as “Capture the Flag” or “Defend Yourself and Penetrate the Enemy” may be applied. Several application interfaces are available to monitor the performance of attendees and general state of the competition. SiberMeydan CTF environment has been successfully field tried in National Cyber Exercise 2013, Cyber Security Summer School with restricted set of scenarios and in SiberMeydan UNI 2013 with extended set of scenarios and all features.

**CAPABILITIES**
- Completely virtual simulation environment
- Around 120 related attack and defense scenarios
- Simulation of ALL COMPONENTS of a common corporate network
- Ability to work in the environment as a member of red or blue teams
- Detailed documentation of scenarios and correlations among scenarios, including vector diagrams.

**SUPERIORITY**
- Regular update of simulation environment and scenarios due to new experiences
- Scalable simulation environment
- Genuine content
- System designed for training
- Covers qualifications related to multiple fields of expertise.
CONSULTANCY FOR THE DEVELOPMENT OF SECURE SOFTWARE

Security is not an add-on feature that could be added to a system or software. But instead, it should be evaluated as part of the development process. Implementation of security functions during the processes of development and installation is both easier and more effective.

SGE provides the following services to public and private organizations/institutions:

- Trainings for the secure software development
- Software source code analysis in order to detect vulnerabilities during the development of software
- Risk analysis and threat modeling with the purpose of making secure software development processes more efficient
- Search and implementation of new secure software development methods
- Conduct of workshops and conferences on the development of secure software

Within the scope of these services, SGE has aided NATO in many projects related to information system development. For the security accreditation of these system and software projects, the institute has presented consultancy regarding secure system design and the preparation of accreditation documents and also carried out the security tests of the developed systems.
Cyber Security Institute (SGE) conducts penetration tests and security audits both on state institutions/organizations and private sector companies. These penetration tests and security audits encompass all components of the informatics infrastructure. Upon the completion of these tests, detailed technical reports and executive summaries are established. Additionally, to increase awareness of the personnel on security, social engineering tests are implemented along with technical security tests.

In order to carry out tests that are of highest standards and efficiency, SGE researchers seek and develop new exploitation methods and tools.

Another emphasis within this scope is on information sharing. Apart from the afore-said security tests, there are efforts to enhance the capacity of tests on information sharing. To this end, workshops are organized with the objective of determining the scope and depth of the tests, increasing the quality and objectivity of test result reports. Besides, joint projects are carried out with the organizer institutions.

Cyber Security Institute (SGE) provides institutions and organizations with consultancy on information security management system. Within the scope of the consultancy, institutions are being assisted during the risk analysis of IT systems and preparation of institutional policies conforming to the international information security standards. Consultancy may be extended to cover the full cycle of ISMS activities, including certification of the ISMS, depending on the demand of the institution for the ISO 27001 certificate.
RISK ANALYSIS
Cyber Security Institute (SGE) provides information security risk analysis service to defence, public and private sectors. Both software and system level risk analysis projects are conducted. Corporate level risk analysis service is also provided in the scope of ISO 27001 certification.

In this scope, business processes are analyzed, critical processes are identified; the assets in these processes are identified, asset dependencies are determined and evaluated. In this phase, data flow charts are created as well. Afterwards, the probability and impact values of the potential risks acting on the assets are estimated and the identified risks are documented in detail in accordance with the project context. Basing on derived risks, security requirements are identified from a list including the controls from ISO 27001 and NIST SP 800-53 standards and documented congruent with the project context. Security requirements and their maturity levels are assigned with the customer.

Lastly, the residual risks left after applying the security measures are evaluated at the final step. The MAGERIT Version 2 methodology and the PILAR tool is utilized to realize the risk analysis.
MALWARE ANALYSIS
Among the most widely seen cyber-security threats at the level of end users are viruses, trojan horses, backdoors and worms. Nowadays, malicious software is not only used for financial fraud, but also for obtaining confidential information and damaging information accessibility.

Developed countries that have a good grasp of importance of the issue, make significant investments in keeping their protection mechanisms updated. In this direction, the Cyber Security Institute Malware Analysis Unit closely follows the current malware trends and analyzes the malware which may pose a huge threat for Turkey’s infrastructure and services that are of critical importance. Results and counter measures deriving from these analyses are shared with relevant institutions via information sharing platforms.

Especially in today’s world, malicious software could pose a huge threat when used for cyber espionage under the name of Advanced Persistent Threat (APT). Countries may use malware either to negatively influence the critical infrastructure of other countries or to acquire their sensitive information. Upon demands from critical public institutions or private corporations, SGE conducts investigations to detect sensitive data leakage.
UNDERWATER DEFENCE SYSTEMS
DATAS
SUBMARINE TACTICAL SIMULATOR

DATAS is a tactical and operational training simulator for submarine commanders and combat teams. The system generates different training scenarios for search, engagement, attack and avoidance.

**USAGE**
DATAS is located on shore and consists of three physical sections.

- Training Control Room: In this room trainers control the simulation system, prepare and run training scenarios.
- Central Room: Room where the trainees take tactical and operational decisions and perform the training.
- Debriefing Room: Room for the evaluation of training results with the assistance of debriefing tools.

**GENERAL CAPABILITIES**
- Submarine central room systems and consoles simulation
- Cylindrical array sonar
- Flank array sonar
- Passive ranging sonar
- Intercept passive sonar
- Active sonar
- Radar and ESM (Electronic Support Measures)
- LINK/ROL-11
- Torpedo and guided missile

**DATAS**
- Fire Control and Target Motion Analysis (TMA)
- Submarine navigation simulation
- Dead reckoning table simulation
- Underwater environment modeling
- Platform and ambient noise modeling
- Acoustic propagation modeling (Normal Mode and Ray Trace)
- Autonomously acting target modeling
- Application of Unit Submarine Warfare (USW) Tactics

Subject to Approval of Turkey Ministry of National Defence for Selling.
SEDAVER is the software for generation of data packages of command and control, launcher, firing station, etc. systems in accordance with actual communication protocols.

**GENERAL CAPABILITIES**
- Adaptation to different submarine classes
- Defining threat status as scenario
  - Two dimensional scenario realization
  - Online scenario update
- Scenario based submarine data package generation
  - Submarine navigation data
  - Submerged environment measurement data
  - System trace data of targets
- Submarine information distribution system compatible with data package generation
- Data package transmission over RD-232/RS-422/Ethernet

**LAUNCHER SYSTEM SIMULATION**
- Launcher data package generation
- Casing status query
- Programming of decoys and jammers in casings
- Decoy and jammer launch orders
- Built-In Test (BIT)

**SSE FIRING STATION SIMULATION**
- Firing station data package generation
- Programing of decoys and jammers at firing station
- Firing station cell status information query
- Internal test

⚠ Subject to Approval of Turkey Ministry of National Defence for Selling.
Daka / BTBM is the modeling and simulation tool for decoy and jammer release and evasive maneuvers for submerged platforms and surface vessels under torpedo threat.

**Simulation Capabilities**
- Defining torpedo tactics
  - Avoidance maneuver
  - Decoy/jammer operating modes and release sequence
- Defining threat situation as scenario
- Defining sound speed profile
- Defining sea bottom type and profile
- Defining torpedo threat
  - Heavy/light torpedo selection
  - Defining torpedo guidance behavior and sonar
- Defining acoustic decoy and jammer
- Defining submerged platforms/surface vessels and sonar payloads

**Modeling Capabilities**
- 4 and 6 Degrees of Freedom (DOF) dynamical modeling
- Underwater acoustic propagation modeling (Ray Trace)
- Guidance and movement modeling in accordance with torpedo phases
- Modeling of torpedo detection, evaluation and decoying behavior of decoys
- Modeling of noise emission behavior of jammers

**Analysis Capabilities**
- Torpedo/platform/decoy/jammer dynamical analysis
- Torpedo phase change analysis
- Torpedo and platform sonar data analysis
- Acoustic decoy/jammer data analysis
- Successful/failed tactics analysis
- Most successful tactic selection
- Tactics comparison
- Forward/reverse replay on time axis
- Analysis report generation
- Data transfer to Microsoft Excel
- Defining RUN by scenario and tactics
  - Single run: Two dimensional animation and pre-analysis
  - Multiple run: Statistical analysis
- Display of online data of the simulation run
- Replay at various speeds

⚠️ Subject to Approval of Turkey Ministry of National Defence for Selling.
DEFENSE SYSTEM SOLUTIONS

* Due to ongoing research and development, specifications in this catalogue and its content may change without prior notice.
The DRT (Dead Reckoning Table) is a PC based plotting table for navigational and tactical data used in the Combat Information Center (CIC).

**PHYSICAL CHARACTERISTICS**
- 40” FULL-HD LCD Display
- Keyboard and track-ball for user input
- NMEA 0183 compliant sensor interface
- COTS hardware design
- Ergonomic design
- Easy access to internal parts
- System state indicators
- Dimensions: 1210 mm x 1200 mm x 1100 mm
- Weight: < 250 kg

**NUMERICAL PLOTTING TABLE**
The DRT displays the ship’s position, speed and heading information on its 40” displays using data gathered from various navigational sensors.

Also, plot informations received from navigation radar can be seen on display. Therefore, own ship and targets related navigation information is to be displayed, monitored and plotted on digital map.

S-57 and S-63 digital map formats are used and all informations coming from sensors are displayed in realtime.

⚠ Subject to Approval of Turkey Ministry of National Defence for Selling.
GIS is a Real-Time Operating System especially developed for hard real-time safety critical avionics applications. However, it is scalable and adaptable for embedded real-time applications in other domains as well.

GIS adheres the ARINC 653 specification for avionic applications, and fully supports the ARINC 653 Part-1 Required Services and features like Multiple-Module Schedule, Service Access Points from Part-2 Optional Services. Thus ARINC 653 is the native API of GIS, performance penalties of wrap-up functions are eliminated.

GIS adheres the POSIX® (IEEE 1003.1) standard for embedded real-time applications, and fully supports the PSE 51 Minimal Real-time System Profile, PSE 52 Real-time Controller Profile, and PSE 53 Dedicated Real-time Profile. Conformance of GIS to POSIX® standard is fully verified by the official POSIX® Conformance Test Suite.

GIS comes with an integrated development environment called TGO. TGO is an Eclipse based integrated development environment which provides features like application development, mode selection, debugging, event analysis and simulation to application developers and system integrators.

GIS is developed to be adaptable to different processor architectures and hardware configurations. It has a layered structure so that, by adapting the hardware abstraction layers, i.e. Architecture Support Package (ASP) and Board Support Package (BSP) to different architectures and hardware configurations, GIS can easily be ported on many platforms. GIS currently runs on several single core and multcore processor architectures and hardware configurations. Hardware support for new platforms is rapidly increasing.

GIS is developed fully from scratch and is not based on a present kernel. GIS is developed in accordance with DO-178B and is certifiable up to Design Assurance Level A for single core architectures. DO-178C certification pack for multicore architecture is under development.

GIS is being integrated with several platforms such as mission computer, digital flight control computer, electronic warfare systems and remote controlled weapon systems.
ETMTS-2 is a new generation dual sensor hand-held mine detection system containing both Metal Detector (EMI) and Ground Penetrating Radar (GPR). The system is capable of operating in challenging military conditions.

ETMTS-2 device runs on two main modes, which are detection and identification. Audio warnings about the detection of buried targets are given to the operator by headphone or external speaker, and visual warnings are shown on LCD screen. Therefore, user may create his own identification decision through the audio-visual information produced by the system. There is a built in test (BIT) both on start up and during operation, which provides reliability. Data from the sensors, system warnings and battery level status are displayed on the screen. The system can communicate with the outer World through an Ethernet port if needed.

The operator can detect and localize both metallic and non-metallic buried mines and IEDs along a scanning path and can visualize suspicious territory and generate a prediction about the type of the buried objects utilizing automatic classification software.

The system is compatible with the military standards MIL STD 810G and MIL STD 461F. Underground visualization can be obtained with high-gain planar antenna structure and metals can be detected with high sensitivity via optimally designed search coil.

**SENSORS**
- EMI (Electromagnetic Induction) Sensor
- GPR (Ground Penetrating Radar) Sensor

**CAPABILITIES**
- Detection of metallic mines
- Detection of non-metallic mines
- Detection of IEDs
- Detection of embedded objects
- Precise target centering by audio-visual warnings
- Self-training capability to the operators

❗ Subject to Approval of Turkey Ministry of National Defence for Selling.
DEFENSE SYSTEM SOLUTIONS

TAKSİS
TACTICAL TRAINING SYSTEM

TAKSİS (Tactical Training System) is an embedded simulation system intended for the urbanized area training of SWAT forces.

TAKSİS
Special suits with hit detection capability, weapons generating laser beam and having realistic blow-back mechanism, high accuracy positioning system, hand grenade and blast bomb, booby traps, powerful sound systems and smart camera system enabling person and room tracking are the main components of the system. Personal, team and tactics based performance evaluation can be executed by using the real-time data acquired during the operation and the results can be extracted as detailed reports. It is also possible to carry out debriefing for a more detailed analysis by simultaneously replaying the video streams and animation displayed on tactical area layout.

SPECIFICATIONS
- High level of similarity to real operational area
- Mutual combat with moving targets
- Laser beam weapons with realistic blow-back mechanism
- Specially designed training suits with hit detection capability
- Emulative hand-grenades, blast bombs and booby traps
- Powerful sound system playing high intensity explosion sounds of weapons and ammunitions
- Reusable training materials
- 2D indoor and outdoor positioning system
- Operation monitoring via video stream and simultaneous replay
- Screens for scenario creation, tactics definition, operation tracking on tactical area layout
- Individual, team and tactics based performance evaluation and analysis

HIGH LEVEL OF SIMILARITY TO REAL OPERATIONAL AREA
Equipment is same as the originals in appearance and weights such as hand-grenade, blast bombs and booby traps enable trainees to battle in a training area are same as the real ones. Realistic sounds of bombs and weapons makes up challenging battle medium for trainees. Weapons equipped with a blow-back mechanism and generating intensive explosion sounds make trainees gain realistic experience.

Subject to Approval of Turkey Ministry of National Defence for Selling.
SHIPBOARD AUTOMATIC DEGAUSSING SYSTEM

Shipboard D/G System suppresses the magnetic signature of the ship by using on-board D/G coils that generate reverse magnetic signature. The magnetic signature of the ship is kept within desired limits by applying appropriate (depending on the ship’s heading and geographical location) currents to the on-board coils. The magnetic signature of a ship with an active D/G system is greatly diminished, shortening the detection distance of a sea mine’s magnetic sensor and thereby reducing the risk of triggering an explosion.

Shipboard D/G system is at service on Island class corvettes of Turkish Navy.

Subject to Approval of Turkey Ministry of National Defence for Selling.
ELECTRONIC WARFARE SYSTEM SOFTWARE SOLUTIONS AND SYSTEM SOLUTIONS

* Due to ongoing research and development, specifications in this catalogue and its content may change without prior notice.
SiMA is a simulation modeling and execution framework that aims to significantly reduce the development time of simulation applications. SiMA provides both an abstraction for system modeling and a protocol for executing and synchronizing the simulation of the modeled system, which provides a well-defined approach for constructing modular and hierarchical models of complex systems. SiMA is primarily written for .NET environments but can interface to pure C++ simulation model code. In addition, SiMA includes a Distributed Simulation Module that can act as an adapter to various external distributed simulation infrastructures such as HLA.

GENERAL CAPABILITIES
- Discrete Event System Specification (DEVS) Formalism
- Re-usable model development
- Flexibility to develop different simulations with different model compositions
- Development of models in C++ and .NET Environments
- Fast model development processes with code generation tools
- Recording of simulation inputs and outputs
- Distributed Simulation Development support
- Interaction with HLA/RTI adapted simulations
Management and Analysis of Radio Spectrum System (MARSsys) is the unique solution satisfying both military and civil operational requirements through the integration of a wide range of spectrum management capabilities at national and international levels. Offering full support for NATO SMADEF-XML data exchange standard, thus facilitating international coordination capability in spectrum management, MARSsys is considered as one of the most advanced software in spectrum management field. MARSsys provides role based access control on underlying data and imposes authorization checks on a hierarchical organization structure. Each data item can also be masked based on security clearance level attributes of both data and the user. Frequency assignment process, frequency request and interference messaging process, interference analysis and interference-free frequency assignment process are supported. Coverage analysis for various system types and frequency bands are also provided along with many other technical analysis tools.

**SMAS (TECHNICAL ANALYSIS MODULE) CAPABILITIES**
- ITU-R compatible propagation models for LF/MF-HF-V/UHF-Radar-Radio
- Link bands (3KHz- 52 GHz)
- User-friendly, flexible, and customizable user interface
- Stand alone operation
- Database query interface
- Batch analysis for multiple systems
- GIS-based Interactive Map Interface
- DTED 0/1/2 height data usage
- Support for various vector and raster map formats
- Layered display of maps and analysis results
- Powerful report and print-out capabilities

**FIMS (DATABASE SERVICES MODULE) CAPABILITIES**
- Multi - user database
- Allocation / Allotment/ Assignment databases
- Joint Restricted Frequency List (JRFL)
- Frequency Assignment Wizard
- Inventory Database
- Advanced query interface
- Role based user access and operation control
- Interactive Map Interface
- Powerful data exchange capabilities: Import / export interfaces including NATO SMADEF-XML format
IR Data Management and Analysis Software (IR-DMAS) addresses well-known issues of IR data recording, management, and analysis and provides a unique solution satisfying both operational and engineering level military requirements through the integration of planning, measurement, analysis, and reporting phases of IR signature measurement campaigns.

IR-DMAS can be customized in accordance with user requirements. Different language options are available on user demand.

**GENERAL CAPABILITIES**

- Association of multi-modal, multi-format fragmented data via a well-defined information model
- Systematic way of capturing meta data
- Well defined procedure for recording vital auxiliary information
- Automatic data correlation
- Raw image processing for multiple camera types
- Archiving, management, and reporting of full analysis data including vital contextual information
- Shorter analysis times, more reliable analysis results
- Database connected operation – Automatic transfer of parameters from database via query interface
- Database connected planning – Automatic transfer of parameters from planning interface to database
- User specific database (IR cameras, filters, lenses, station/location)
- User specific analysis by defining user specific formula definitions
- Powerful data exchange capabilities: Import / export interfaces
- User friendly and flexible user interface

![Subject to Approval of Turkey Ministry of National Defence for Selling.](image)
REDAY is an integrated software solution providing comprehensive performance analysis regarding the interaction of Radars and Electronic Support (ES) systems. REDAY uses Electromagnetic (EM) Propagation models including environmental and atmospheric effects, to compute the expected behavior of Radars and ES systems. All crucial analysis types are provided both in horizontal plane (range vs angle) and vertical plane (range vs height). One distinct aspect of REDAY is that it features a rich set of functionality for Inventory Management of Electronic Warfare (Radar and ES) Systems. This Inventory Management Module facilitates an easy scenario creation process for the operator. Inventory and Results Export/Import features are also provided.

GENERAL CAPABILITIES
- Radar coverage analyses
- Radar systems detectability analyses
- Electronic Support Systems detectability analyses
- Empirical and deterministic (Fourier Split Step) analysis
- Inventory of systems
- AREPS Software and Database compatibility
- Batch analysis for multiple systems
- User defined study area
- GIS-based Interactive Map Interface
- DTED 0/1/2 height data usage
- Support for various vector and raster map formats
- Layered display of maps and analysis results
- Technical analysis includes antenna pattern effects, refraction profiles of the atmosphere

\! Subject to Approval of Turkey Ministry of National Defence for Selling.
RASES is a high-frequency electromagnetic simulation software which is capable of calculating Radar Cross Section (RCS) of complex targets. The computation methods that are implemented within the software are Physical Optics (PO), Shooting and Bouncing Ray (SBR) and Physical Theory of Diffraction (PTD).

- **RADAR CROSS SECTION COMPUTATION**
  Monostatic and bistatic RCS computations can be performed for different frequencies, materials, incidence and observation angles within the simulation environment. Statistical information of the evaluated RCS values can also be investigated. The variation of the RCS values of a target due to any specific maneuver can be analyzed. RASES provides reliable RCS results which have been verified by analytical solutions, numerical methods and experimental results.

- **EVALUATION OF RANGE PROFILES AND ISAR IMAGES**
  Within the RASES software, 1-D (Range Profile), 2-D and 3-D ISAR images of the targets can be constructed by using the estimated RCS values. By using Inverse Synthetic Aperture Radar (ISAR) images, dominant scattering regions on a platform could be determined.

- **DETERMINATION OF SCATTERING CENTERS**
  Positions and amplitudes of the scattering centers that can be extracted from 1-D, 2-D and 3-D ISAR images are of high importance for the RCS reduction studies of the targets. Extraction of the scattering centers is performed via the CLEAN algorithm.

- **DESIGN PROPOSALS FOR RCS REDUCTION**
  The RCS value of a platform can be reduced via structural modifications on a platform or the usage of radar absorbing materials (RAM). By using the built-in coating material types of RASES and by including the electrical specifications of new material types in the material library of RASES, the effects of the RAM application can be observed in terms of RCS variations. The structural modifications that can be performed by using several commercial CAD software, can also be input to RASES in order to investigate and design platforms with low RCS values.

Subject to Approval of Turkey Ministry of National Defence for Selling.
Within İLTAREN (Advanced Technology Research Institute), studies are carried out to develop terms for the systems of advanced EW technologies. Prototype and term representation systems are being promoted. Within this context, prototypes of various electronic attack and electronic support systems have been successfully developed by qualified groups of engineers.

**ELECTRONIC ATTACK TECHNOLOGIES**
A term representation system (TRS) developed with the intention of analyzing the efficiency of various electronic attack techniques provides electronic attack applications which are resistant to electronic jamming and deception and quite effective against modern search and tracking radars. Among the main features of the TRS are:
- Narrow-band, high powered electronic attack capacity
- Capability of applying electronic attack to any side thanks to the sealed beam dish antenna
- DRFM-based advanced technical generator
- Very low time lag
- Capacity of finding the direction of threats and polarization
- Target monitoring with a camera
- Capacity for changing polarization within receiving and transmitting antenna
- Capacity of being stationed both at land and air platforms
- Capacity of applying integrated techniques via various jamming and deception techniques

**ELECTRONIC SUPPORT TECHNOLOGIES**
A prototype system including various electronic support system features has been developed. Apart from comprising the features of a typical electronic aid and ELINT systems, the prototype includes the following as well:
- Operator-specific analysis screens
- High-driven missile detection under intense operations
- Center and operator-specific data access possibility to emitter identification
- Instant matching of contact record specifications with GPS and gyro
- Capacity of creating contact file for analysis

Subject to Approval of Turkey Ministry of National Defence for Selling.
In order to scientifically reinforce the electronic warfare system development, analysis activities are carried out within İLTAREN (Advanced Technology Research Institute). İLTAREN maintains these tasks by having various measurement, testing and evaluation infrastructures whether operating at open field or in laboratories. Additionally, studies to detect how radar, infrared systems and other platforms perform under different conditions. Thanks to the experience and expertise acquired from activities, various consultancy and engineering support services are also being presented.

**HARDWARE IN-THE-LOOP LABORATORY**

Hardware In-The-Loop Laboratories are established with the purpose of analyzing how various systems operating on RF and infrared bands perform under different conditions and scenarios. Studies to develop more reliable and loyal models via open field testing and measurement activities and to conduct analyses on system behaviors are conducted as well.

**RF & INFRARED MEASUREMENT SYSTEMS**

A system to measure infrared traces of decoys such as air and land platforms and heat shells have been developed. Two different recording system utilized for RF and infrared bands. Recording and playing back the signals on RF, IF and video bands is possible. Both of these systems are placed in a Panel van-type minibus whose components have been specifically designed for mobile usage.

**ENGINEERING SUPPORT SERVICES**

İLTAREN gives engineering support services to the Turkish Armed Forces, by using the infrastructure acquired from electronic warfare system projects that are conducted by the Turkish Undersecretariat for Defense Industries. These services include development of electronic warfare techniques and tactics, reprogramming of the electronic warfare systems in a way that will meet the operational requirements, maximizing the experience and knowledge of the personnel dealing with electronic warfare, testing, evaluating and system engineering.
CLOUD COMPUTING SOLUTIONS

* Due to ongoing research and development, specifications in this catalogue and its content may change without prior notice.
DAMLA is the National Search Engine Prototype for searching over internet content, developed by domestic resources. With Turkish grammar specific features taken into account, the search engine can analyze internet contents to determine whether they are in Turkish or not. Therefore, the search engine can provide the capability of filtering Turkish contents during indexing and searching activities for fast and efficient browsing.

DAMLA can provide;

- auto-complete
- auto-suggestion
- query correction
- stemming and stem-based searching, being Turkish grammar aware during all search processes.

FEATURES

- Identification and classification by content categories (News, Sports, Health, etc)
- Search within selected categories only
- Safe search for eliminating adult content
- Searching within content of specified time intervals
- Searching inside files and by file types (Pdf, Docx, Xls, etc)
- Advanced ranking and prioritization algorithms
- Image search
- Searching images with specified file size ranges
- Searching images by location information, if available
- Horizontally scalable, Cloud-compatible system architecture
SAFIR INFRASTRUCTURE
Safir Infrastructure is an “Infrastructure as a Service” solution provided by Cloud Computing and Big Data Research Laboratory (B3LAB). Support of multi-tenancy, resource management, security and privacy are provided in “Infrastructure as a Service” layer of cloud computing.

Safir Infrastructure presents a secure virtual information technology environment with virtual servers, storages and network devices.

SAFIR STORAGE
Safir Storage is a secure centralized cloud storage solution for accessing and storing objects like documents, papers, audios and videos distributedly.

Safir Storage is a virtual object storage under Openstack Swift infrastructure, and compatible with Amazon AWS S3 platform. It provides high speed writing, reading and deleting features to the integrated systems. It scales in vertical with both running nodes and disk capacity.

The system distributes each object added to the storage among the nodes with 3 duplicate copies. Thus, damage on one of the disks or servers does not affect the stability of the system.

SAFIR IDENTITY
Safir Identity provides an authentication mechanism to the cloud components with SSO (Single Sign On) support. It also provides single sign on and authorization with smart cards.

SAFIR LIBRARY
Safir Library provides a platform-independent Application Programming Interface (API) to access and use the functionalities of all of the cloud services.

FEATURES
- Safir Infrastructure
  - OpenStack Controller, Neutron, Compute infrastructure
  - Web based management interface
- Safir Depot
  - OpenStack Swift infrastructure
  - Fast and reliable object access and storage
- Safir Identity
  - Role based secure access layer
- Safir Library
  - RESTful API support
  - Easy cloud usage with client scripts
The amount of created, inspected and analyzed data is increasing every day, and the term "digital world" surrounds the reality of daily life. In fact, every form of data has its own importance. "Big Data Analytics Solutions" developed by Cloud Computing and Big Data Research Laboratory (B3LAB) can analyze big data and turn this bulk data into information.

Big Data Analytics Solutions include:

- Hadoop cluster setup and consultancy
- NoSQL database setup, configuration and optimization
- Big data file systems’ configuration and optimization
- Configuration and optimization of Linux based operating systems used for big data solutions
- Designing, building and implementing network architectures for big data solutions
- Implementing big data code (e.g. Map Reduce code)
- Turnkey solutions for big data problems
- Optimization of big data code
- Hadoop cluster optimization
- Big data training
IDENTIFYING NEEDS AND PLANNING SOLUTIONS

* Due to ongoing research and development, specifications in this catalogue and its content may change without prior notice.
As part of the information society the TÜBİTAK BİLGEM Software Technologies Research Institute (YTE) provides comprehensive services for identifying digital transformation needs on the subject of Identifying Needs and Planning Solutions with an architectural perspective and planning solutions with an innovative approach so that public agencies and institutions can benefit from an institutional and national level of information and communication technologies at the highest level and operate with high service quality and a productive, efficient and transparent structure.

- TÜBİTAK BİLGEM Software Technologies Research Institute determines the realizable and sustainable e-Transformation vision and corresponding goals in line with agency and institution needs and conduct Current State Analysis of Agencies and Institutions with a multifaceted and multidisciplinary approach.
- Based on the decisions made after the current state analysis the needs of the agencies and institutions are identified and Needs Analysis is conducted to develop goals and strategies in the scope of determining Targeted Status.
- The Road Map consisting of projects and activities with short, mid and long term solutions is brought to the forefront. If necessary Technical Specifications of these projects are also defined.
- Institutional and/or National Monitoring and Assessment Work and System Models that secure the needs of the present and near future are being met.

In this field of service YTE provides public agencies and institutions with the following services:

- Current State Analysis
- Needs Analysis
- Targeted Status Determination
- National, Thematic and Strategic Planning and Policy Making
- IT Strategy Planning
- Determining a Road Map
- Defining Technical Specifications
GOAL
The objective is to prepare Turkey’s first comprehensive and integrated national e-Government strategy and action plan in the framework of Turkey’s 2023 vision, the Tenth Development Plan and the 2015-2018 Information Society Strategy and Action Plan with national competences to guide the e-Government work covering years 2016-2019; shaped by a common mind and scientific perspective in which the analysis work of central government units, local governments, citizens, private sector, professional organizations, non-governmental organizations and universities are included; and to develop an action plan monitoring and assessment model.

SCOPE

GAINS
- Increase in the efficiency of e-Government services,
- Popularization of e-Government service use,
- Increase of satisfaction with e-Government services,
- Increase in the perception of public benefit achieved with e-Government,
- Increase in the placement of Turkey among international e-Government indexes
GOAL
It is aimed to analyze the existing processes and systems executed by the Ministry of Finance and related stakeholders and also to identify the needs within the scope of Integrated Public Financial Management Information System and to determine the roadmap in order to achieve an integrated infrastructure providing effective data for decision making processes in public financial management in Turkey.

SCOPE
- Investigation of similar practices
- Analysis of the current status and determine the target status
- Preparation of an integrated system architecture
- Identification of the roadmap and the preparation of the preliminary analysis report

GAINS
- More effective, efficient and economical way of acquisition and allocation of public resources
- Increase the control level of expenditure processes
- Improve the capabilities of public financial reporting
- More widespread use of statistical analysis in the decision-making process
- Faster fulfillment of the processes related to financial transactions
- Reduction of the cost occurred by paper-based processes and use of paper due to increased use of electronic documents.
- Increase the level of satisfaction about the public service as a result of less time required to complete a transactions that is transferred into electronic environment.
- Increased use of computer-assisted audit techniques in internal and external audits
GOAL
The aim of the project is conducting as-is and to-be analysis, defining the roadmap and reporting the KOSGEB e-Transformation Plan within the scope of digital transformation of KOSGEB in line with Turkey’s 2023 vision and managing support programs of KOSGEB more efficiently.

SCOPE
- Analysis of current and target situation
- Defining the roadmap and preparation of KOSGEB e-Transformation Plan

GAINS
- Suggesting a solution which ensures managing support programs of KOSGEB more efficiently
- Constructing solutions applied by KOSGEB and institutions of other countries which KOSGEB is a model
GOAL
Turkish Electricity Transmission Company (TEİAŞ) plans to build an enterprise spatial data infrastructure in order to manage the high voltage substations and transmission lines. The infrastructure shall be utilized as the main tool for all the processes from planning to operations including construction of transmission lines and substations', environmental impact assessment and expropriation. The IT infrastructure shall be compliant to international and national standards and be integrated to Turkish National Spatial Data Infrastructure (TUCBS) and shall serve to both central and regional organizations of TEİAŞ.

The technical consultancy project serves for the purpose of analyzing the current state of TEİAŞ, by determining the requirements, establishing a road map, and defining the technical specifications of the system.

SCOPE
▪ Establishing a GIS roadmap based on the analysis results
▪ Proposing a technical solution of GIS based software
▪ Identifying technical specifications and designing high level architecture of GIS based software

GAINS
▪ Determining the processes related to high voltage substations and transmission lines
▪ Identifying bottlenecks in the current processes
▪ Specifying GIS requirements related to substations and transmission line projects
▪ Increasing awareness of the staff in central and provincial organizations of institution in GIS
▪ Determining similarities and differences of application methods among central and provincial organizations of the institution
▪ Contributing the development of the vision and goals of the institutions, by investigating and analyzing examples with similar issues in other countries, transferring knowledge and experiences about GIS and project management practices.
IDENTIFYING NEEDS AND PLANNING SOLUTIONS

PRE-ANALYSIS OF BTK INFORMATION MANAGEMENT SYSTEM PROJECT

GOAL
The objective is to identify needs and determine a road map in the scope of the Information Technologies and Communication Agency (BTK) Information Management System so that the organization and audit process of the electronic communication sector can be conducted more efficiently.

SCOPE
- Current and targeted state analysis work
- Work to develop suggestions for solutions and a road map
- Work to develop draft technical specifications

GAINS
- More efficient management of the electronic communication sector’s organization and auditing processes
SOFTWARE DEVELOPMENT

* Due to ongoing research and development, specifications in this catalogue and its content may change without prior notice.
TÜBİTAK BİLGEM Software Technologies Research Institute will provide services in software development of strategic, critical and R&D digital solution development projects for realization of the actions, which are situated in the national agenda and defined in high level strategic and political documents that are giving directions to the e-Government ecosystem.

Within software development lifecycle, below activities will be practiced:

- Analyze the as-is situation, define the target system and compose the software requirements also compatible with the prioritized work packages, to identify the needs and plan an optimal solution,
- Configure architectural designs,
- Carry out coding, Code reviews and test activities,
- Provide better user interface designs for the software systems developed taking into account the human-computer relationship during the usability tests done in our in-house usability lab and ensure user’s comfort,
- Provide practical training to the users, to promote the usage of the system, prepare the training materials according to the needs and expectations of the target audience, provide support to the users,
- Provide project monitoring and assessment and supervision counseling, with the help of change management, to ensure realization of the provided road maps and working models,
- Provide assurance activities with subcontractor management, project and program management perspective, during the solution realization transitioning points, not only for the projects defined within the road maps, but also for the projects according to the demands of the organization.

Within this service area, YTE provides below services to public institutions and organizations:

- Software Development
- Project and Program Management
- Monitor and Assessment Consultancy
GOAL
It is aimed to develop an infrastructure in order to track medical devices and cosmetic products from end to end, conduct surveillance mechanisms and execute clinical engineering processes in efficient and effective manner, to develop a national and original Product Tracking and Monitoring Model and a compatible information system.

SCOPE

GAINS
- To provide easy identification of unique products through recall of unsafe products
- To contribute to ensure patient safety and protect public health
- To improve the standards of medical devices and cosmetic products by monitoring of product quality with feedback mechanism
- To create an infrastructure to enable Medicines and Medical Devices Agency of Turkey to swiftly respond to risks that may result from the use of medical devices and cosmetic products
- To contribute to prevent the unregistered economy through the tracking of medical devices and cosmetic products
GOAL
This project aims to ensure the transparency, accountability, coherence and coordination in the Development Agencies’ financial management; increase efficiency of the main business processes, productivity of developing an integrated central information system.

SCOPE
Information system is being developed in order to strengthen the corporate operations of Development Agencies and the main business processes and improve the effectiveness, efficiency in the management of the support.

GAINS
▪ All funding given by agencies is monitored and reported in real time.
▪ Implementation differences between Development Agencies in the process of project application, evaluation and monitoring is minimized.
▪ The business processes are made faster with the use of a system and the errors that can occur due to human factor are minimized.
▪ The system provides only authorized personnel to see the relevant data. Thus, information privacy and security level has been increased.
▪ By forming Independent Evaluator (IE) pool throughout Turkey, IA process is more transparent, effective and accountable.
▪ The system provides decision support capabilities by managing funding with more transparent, effective and accountable way; and reporting to decision makers for effective and efficient management of funding.
INTEGRATED SOCIAL ASSISTANCE SERVICES PROJECT

GOAL
It is intended to centralize all information regarding the social assistance programs provided by the government, develop an information system that leads to more fair resource distribution, and increase the effectiveness of decision-making processes by the help of integrated management of social assistance information.

GAINS
- About social assistance services;
  - Increasing the quality and effectiveness
  - Improving the traceability and auditability
- Implementation of the Income Test Process of General Health Insurance
- Integration with Public Institutions (Integration is accomplished with 16 Institutions).
  - Regulation and verification of data structures
  - Contribution to standardization
  - Ensuring cooperation between Public Institutions
  - Acceleration of application, analysis and decision-making processes
- Technology
  - High-capacity concurrent user architecture
  - System virtualization and cloud-based hardware infrastructures
  - Fast batch data processing
  - Infrastructure support for public institutions
GOAL
In the field of efficient management of natural resources, it is aimed to develop “Basin Monitoring and Evaluation System” on the purpose of providing infrastructure for integrative policies by evaluating the themes like Desertification, Erosion, Flood and Overflow which are interactive each other.

SCOPE
- Modeling Desertification and Producing Risk Map for Turkey
- Development of Basin Monitoring and Evaluation System

OUTPUTS

- Desertification Risk Map
- Pilot Field Study
- Basin Monitoring Screen
GOAL
EBIS is IT System Development of EMRA (Energy Market Regulatory Board). Energy market data from 4 markets (Petroleum, LPG, Electricity, and Natural Gas) are managed with a central software system. Online license applications and data notifications of license owners are made by using e-signature through e-Government Gateway. A reporting system has been developed in the project, it is used for detailed data analysis, reporting and decision analysis.

GAINS
• Managing energy market data centrally,
• Online applications and data notifications from e-Government Gateway,
• Establishing data analysis infrastructure for detecting petroleum smuggling
MODEL DEVELOPMENT AND COMPETENCE BUILDING

* Due to ongoing research and development, specifications in this catalogue and its content may change without prior notice.
TÜBİTAK BİLGEM Software Technologies Research Institute provides gained knowledge and experiences within the scope of the Institute, develops guidelines and reference techniques and models for the purpose of developing needed skills in the IT ecosystem, and renders services in the field of Model Development (Technique, standard, guidelines) and acquiring competency to provide guidance through various mechanisms.

In this service area, Software Technologies Research Institute provides following services to governmental institutions and establishments:

- Project Management
- Acquisition
- Institutional Architecture
- Performance Management
- Interoperability
- Usability and Accessibility
- Social Media and Mobile
- IT Assurance and Guidance
- Monitoring and Evaluation
GOAL
It is aimed to develop guidelines in which presented theoretical and practical implications are supported by eye-tracking researches in the User Experience Laboratory, and to acquire competency and to create awareness in governmental institutions by means of dissemination practices via related guidelines. For these purposes, the objective is to provide more usable and accessible governmental websites which are compatible with governmental institutions' and e-services' usability and accessibility standards.

SCOPE
Web Portal

GAINS
- To identify a standard approach on the user interface problems such as usability and accessibility of public websites
- To build a national awareness on the web usability and accessibility
- To provide consultancy and guidance about web usability and accessibility for the governmental institutions
- To implement research projects about the usability of governmental websites

www.kamis.gov.tr
GOAL
The objectives of the project are; classifying government investment projects, updating Government ICT Projects Preparation Guide on preparing public ICT project proposals for submitting to the Ministry of Development, evaluation of the project proposals by the Ministry of Development and improving the monitoring process of the projects in the investment program.

SCOPE

- Current Situation Analysis Report
- Government ICT Investment Types
- Survey Report for Evaluation of the Government ICT Funding Proposal Process
- Government Information and Communication Technologies Projects Preparation Guide

GAINS
- To help government agencies and institutions on preparing ICT project proposals easily clearly and in accordance with the Turkey’s realities
- Evaluation of ICT projects’ proposals more efficiently by Ministry of Development and consequently, contribution to using of public funds efficiently
During our country’s digital transformation, it is aimed to build national and enterprise scale enterprise architecture methods and technical abilities for the establishment of the digital government structure that can offer high quality and integrated reliable digital government services linked together with all its institutions and, also aimed to develop native reference enterprise architecture models and methods with R&D studies and collaborations with the world’s leading standard and methodology developing organizations in the field such as The Open Group Consortium.

Development and advances of native enterprise architecture models and methods will provide government institutions and agencies to gain the required capabilities and abilities of analyzing, planning and managing change in enterprise digital transformation with the help architectural views of critical corporate assets that are services and business processes, business processes data and supporting applications systems, system infrastructure and technologies, uncovering relationships among them, and unveiling their connections and effects on enterprise business strategies and objectives as well.

GAINS
The expected benefits and achievements provided by the national reference models and services developed in Enterprise Architecture R & D activities using TOGAF (The Open Group Architecture Framework) methodology and approaches are:

• Development of national enterprise architecture reference models and methods in national and enterprise-scale
• Development of interoperability and data architecture for government digital service delivery objectives
• Creation of as-is and to-be enterprise architecture, establish transformation roadmap
• Alignment of Business objectives and IT investments, planning and enhancement of investment efficiency
• Quick adaptability of IT to transformation objectives, increasing the flexibility of against change
• To address and describe modernization needs and requirements properly, increase in operational efficiency
• Ensuring business continuity and risk management feasibility
With the Digital Maturity Model and Guidance Project; it is aimed to make an assessment about the digital maturity of the public institutions and the services they offer, to detect the related levels and to ensure the continuity of this evaluation purposes. Other aim is to improve the capability of the e-government ecosystem stakeholders in Operation and Maintenance domains.

**SCOPE**
- To create the institutional and national digital maturity model.
- To develop guidelines specific to operation and maintenance project types in order to guide and improve capability in this field.
- To conduct pilot applications for the development of the digital maturity model and guidelines.

**GAINS**
- Development of a systematic and holistic view in e-Government studies will be supported.
- By the guidelines to be prepared in Operation and Maintenance perspective, execution of the public institutions’ projects in time, in budget and in planned scope will be provided by increasing the success rate of projects.
- Capability and competence of the public IT staff will be improved related to the operation and maintenance processes.
- Efficiency, effectiveness and information security of the related projects will be increased and the quality and performance of these services will be improved.
YTE provides the services in the area, Governance Planning.

- to plan the assets, processes and the services within the IT projects and activities compatible with the target maturity and capability levels considering the related standards and the best practices covered in the framework models,
- to implement them by developing the decision and reporting mechanisms,
- to monitor, evaluate and improve them.

In this field of service YTE provides public agencies and institutions with the following services:

- Maturity Assessment
- IT Capacity Analysis
- IT Service Management System Implementation
- Software Life Cycle System Implementation
The capacity usage of physical, system, and network components of data centers which hosts IT services of organizations are examined, subsequently improvement suggestions and planning for the future (1-5 years) capacity, hardware needs and business continuity of IT services are determined. In accordance with the findings and improvement suggestions, guidance services such as composing technical specifications documents from a competitive perspective, purchase planning, monitoring and evaluation of modernization proposals are provided.

The projects that have been conducted within the scope of Data Center Modernization are as follows:

- Republic of Turkey Presidency of the Council of State Data Center Modernization Project (DANISTAYSOM)
- The Turkish Language Association Data Center Modernization Project (TDKSOM)
- Turkish State Railways Data Center Modernization Project (TCDDSOM)
- Republic of Turkey Ministry of Transport, Maritime Affairs and Communications Data Center Modernization and Supervision Project (UDHBSOM)
- Prime Ministry of Republic of Turkey Presidency for Turks Abroad and Related Communities Data Center Modernization Project (YTBSOM)
- Republic of Turkey General Directorate of Highways and 18 Regional Directorates
GOAL
For organizations developing software solutions, it is aimed to support process improvement activities based on best practices from international models and standards and to craft solutions composed of necessary process implementations, quantified management, monitoring and education, to make it a sustainable and long lasting effort.

SCOPE
Within this context, will be working on:

- methodological as-is analysis to find out the strengths and weaknesses of the organization,
- defining improvement goals and planning the activities to achieve them,
- defining processes and improvements to the processes,
- monitoring the processes,
- analyzing and evaluating the overall processes,
- providing education and process implementation support for dissemination of the processes

GAINS
- Organizations in the software industry producing high quality solutions, which meets customer needs, by continuous process improvement according to the international standards will be assured.
POLICY AND STRATEGY MONITORING AND EVALUATION

* Due to ongoing research and development, specifications in this catalogue and its content may change without prior notice.
YTE, makes policy researches and plans the related actions accordingly to improve the performance and quality of the digital transformation activities in the public and private sector.

To guarantee and improve the digital government performance and quality, the following Policy and Strategy Monitoring and Evaluation services are provided:

- Trend and Problem Analysis
- Performance Management, Evaluation and Assessment
- e-Government Measurement Activities in the International Scope
This study aims at catalyzing national and international actors’ access to the accurate, actual and comparable information on digital transformation activities in Turkey by conducting policy researches, trend and problem analyses.

**SCOPE**
Primary topics to be researched on digital transformation domain as below:
- Policy and Legislation
- Institutionalization and Management
- Performance and Quality
- Domestic Content
- Shared Infrastructures
- Standards and Guides
- Online Services
- e-Participation
- Open Government / Open Data

**GAINS**
First results of the research is reported as “TÜBİTAK BİLGEM YTE, 2016, ‘e-Government in Turkey: Outlook Report’, Digital Transformation Research Series, No.1, Ankara, Turkey”. The report will be updated periodically in Turkish and English.

It will be assured to extend and keep institutional knowledge up-to-date by the means of in house working groups and presentations.

Hardcopies and online versions of the reports will be shared with national and international actors in digital transformation ecosystem.
The aim is to achieve the vision stated by 2016-2019 National e-Government Strategy and Action Plan, to follow the progress of the actions and to evaluate their performance via the performance indicators. In addition, to ensure the timeliness of the action plan during implementation, it is targeted to model the change management processes and methodology in order to manage the change requirements.

SCOPE

▪ “e-Government Action Plan Monitoring and Evaluation Model”
▪ “Guide of Action Execution and Performance Indicators Definition”
▪ ” e-Government Action Plan Change Management Model”

GAINS

▪ Efficient implementation of the 2016-2019 National e-Government Strategy and Action Plan as a whole with a program management discipline for will be provided.
▪ The actions will be monitored and evaluated in a systematic way.
▪ Sustainable coordination with the responsible and relevant institutions / organizations will be provided.
▪ The strategic goals and objectives will be achieved more effectively with the change oriented management approach.
▪ The Action Plan will be compatible with the dynamic conditions.
▪ In the context of e-Government, the transparency and accountability principles will be supported by the periodic monitoring and evaluation activities related with the Action Plan.
▪ The dynamics of the e-Government ecosystem will be monitored in detail via the periodic evaluation of the Action Plan.
DEVELOPMENT OF R&D PROJECT ON NEW TECHNOLOGY AND TRENDS

* Due to ongoing research and development, specifications in this catalogue and its content may change without prior notice.
TUBITAK BİLGEM Software Technology Research Institute is carrying out projects and activities in related fields in order to develop capacity and to provide to get into use in ecosystem by following international digital trends and technological developments in its working area.

The Institute is conducting R&D activities in prioritized scopes that is identified by analyzing technology/trends ecosystem maps and performing cost/benefit analysis in R&D areas in the high level strategy and policy documents related to area of development in the fields in the sector serviced by the Institute.

- National Database R&D
GOAL
In YTE, it is aim to develop open-source database system, tools and expertise in order to create a strong alternative for the commercial database management systems which are the largest and top item in IT infrastructure budget of government agencies/organizations, and to be used in strategic and critical application systems.

SCOPE
As part of the development studies of national database R&D project, development of PostgreSQL expertise, enhancement of awareness about open source databases in public institutions and encouraging them to use in application development projects, and development of migration strategy and methods from commercial databases are being performed.

GAINS
Heightened awareness of open source database in the public sector with the leverage of national database research and development activities will make open source databases alternative to commercial ones, reduce license and maintenance costs remarkably, increase in service quality, and develop comprehensively both employment and skills in the ecosystem.
DISASTER AND EMERGENCY MANAGEMENT SOLUTIONS

* Due to ongoing research and development, specifications in this catalogue and its content may change without prior notice.
The objective is to establish:

- Message Distribution System (HAY),
- Warning and Alarm System (İAS),
- Warning with Message System (MUS)

aimed to caution nation and organizations that will be assigned in case of emergency, about:

- Enemy attacks,
- KBRN dangers,
- Disasters.

**Warning with Message System (MUS)**
News will be published from mobile phones and social media in order to inform nation before, during and after the disasters.

AVEA, TURKCELL and VODAFONE cellular message and SMS services will be used. Also system delivers warning messages via iOS and Android smart phones application.

**Warning and Alarm System (İAS)**
In case of disasters or emergency accidents, the sirens that have the ability for announcement and alarm will be used and the sections inhabited by people will be covered in optimal range.

Communication between command center and sirens will be with VHF-UHF walkie talkies. Furthermore system will support cabled and satellite communication.

**Receive and Deliver News System (HAY)**
Secure and rapid communication will be ensured between units. News can be delivered, end points’ states can be watched and 7/24 communication news flow will be ensured over system.

A Main Command Center for watch and manage the system, Data Suppliers for delivering news to system, Local Command Center for receiving news from system will connect to the HAY system. All end points’ connection status can be watched and be managed from Main Command Center.
Within the scope of Turkey-Ready for Disaster Project, what is intended to achieve is a disaster plan control system that could (apart from ensuring a distance education and allowing for indoor risk analysis) ensure that Disaster and Emergency Management Plans at schools within the Republic of Turkey Ministry of National Education can be

- prepared and updated by those who are in charge at schools,
- audited by MEB (Ministry Of National Education),
- analyzed by AFAD (Prime Ministry Disaster & Emergency Management Authority).

PLANSIS is designed as a useful, easy to use and a responsive control system.
**Objective;**

Before, during, and after a disaster and/or emergency case, at pilot areas, develop a continuous and secure communication infrastructure in order to:
- Coordinate institutions which will take charge during disasters and/or emergency cases to fulfill their duties
- Communicate message collection and dissemination system, warning and alarm system, early warning system, and so forth.

**FEATURES**

- The prototype includes 15 terminals connected and communicated:
  - Ankara (10)
  - Eskişehir (2)
  - Diyarbakır (2)
  - Zonguldak (1)
- Among terminals, cable, 3G, satellite, and HF communication options are switched according to their availability, respectively.
- Network layer is encrypted by a crypto device.
ADVANCED TECHNOLOGIES RESEARCH INFRASTRUCTURE

- ANTENNA TEST & RESEARCH LABORATORY
- COMMUNICATIONS SECURITY LABORATORY
- SPEECH & LANGUAGE TECHNOLOGIES LABORATORY
- ELECTRO-OPTICS & LASER SYSTEMS LABORATORY
- CATHODE & MICROWAVE VACUUM TUBE RESEARCH LABORATORY
- CRYPTOANALYSIS LABORATORY
- SPHERICAL NEAR FIELD MEASUREMENT SYSTEM LABORATORY
- COMMON CRITERIA TEST LABORATORY
- RADAR RESEARCH & DEVELOPMENT LABORATORY
- RADAR PERFORMANCE AND SIGNATURE ANALYSIS LABORATORY
- RF RESEARCH & DEVELOPMENT LABORATORY
- TEMPEST TEST LABORATORY
- SEMICONDUCTOR TECHNOLOGY RESEARCH LABORATORY
- SOFTWARE TEST & QUALITY ASSESSMENT LABORATORY
- WIRELESS COMMUNICATION TECHNOLOGIES RESEARCH LABORATORY
- VLSI DESIGN AND EDUCATION LABORATORY
ATAM is a research center where R&D, design and production activities are carried out regarding electromagnetics, microwaves and antennas. In parallel to these activities, the center provides consultancy to public administrations and agencies, Turkish Armed Forces, universities and the private sector.

<table>
<thead>
<tr>
<th>Spherical Near Field Measurement System</th>
<th>Moderate and Low Gain Antenna Measurements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Room Dimensions</td>
<td>7.5 x 4.7 x 3.30 m (LxWxH)</td>
</tr>
<tr>
<td>Maximum Dimension of Test Antenna</td>
<td>1.5 m</td>
</tr>
<tr>
<td>Maximum Weight of Test Antenna</td>
<td>75 kg</td>
</tr>
<tr>
<td>Scanning Plane</td>
<td>Full Spherical</td>
</tr>
<tr>
<td>Frequency Range</td>
<td>0.75 GHz - 40 GHz</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Planar and Cylindrical Near Field Measurement System</th>
<th>High Gain Antenna Measurements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Room Dimensions</td>
<td>17 x 18 x 14 m (LxWxH)</td>
</tr>
<tr>
<td>Maximum Dimension of Test Antenna</td>
<td>6 x 6 x 6 m</td>
</tr>
<tr>
<td>Maximum Weight of Test Antenna</td>
<td>4000 Kg</td>
</tr>
<tr>
<td>Scanning Plane</td>
<td>9 x 9 meters</td>
</tr>
<tr>
<td>Frequency Range</td>
<td>0.5 GHz - 40 GHz</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Near Field Radar Cross Section (RCS) Measurement System</th>
<th>Radar Cross Section Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Room Dimensions</td>
<td>29 x 15 x 15 m (LxWxH)</td>
</tr>
<tr>
<td>Maximum Dimension of Target</td>
<td>10 meter</td>
</tr>
<tr>
<td>Maximum Weight of Target</td>
<td>2500 Kg</td>
</tr>
<tr>
<td>Frequency Range</td>
<td>0.2 GHz - 40 GHz</td>
</tr>
<tr>
<td>Range and Cross Range Resolution</td>
<td>5 cm</td>
</tr>
</tbody>
</table>
Communications Security (COMSEC) Laboratory conducts tests to assess whether information security products processing classified cryptographic information are compatible with the COMSEC criteria. Services provided by the COMSEC laboratory, including consultancy and training, are of utmost importance especially for the information security products to be used by the military.

**ACTIVITIES**

- **COMSEC TEST**
  Within the scope of the COMSEC product tests, it is aimed to test whether product’s design and implementation method is in conformance with the COMSEC criteria. As a result of the COMSEC testing, how information security products will respond to and show protection against threats, such as “tampering, fault attack, side-channel analysis and protocol attacks”, is assessed.

- **COMSEC CONSULTANCY**
  Consultancy given for COMSEC information security products mainly focuses on specific details about the design and implementation of a product in accordance with its confidentiality level. Main objective of this consultancy is to ensure that COMSEC criteria are taken into account during the design and implementation phase.

- **COMSEC TRAINING**
  Within the scope of the COMSEC training, information is given about COMSEC criteria and against what sort of attacks these criteria maintain protection.

⚠️ Subject to Approval of Turkey Ministry of National Defence for Selling.
ISO and NATO certified semi-anechoic acoustic recording and test rooms are Turkey’s first and only “Voice and Speech Technology Evaluation” infrastructure.

This infrastructure comprises two specially insulated semi-anechoic acoustic recording rooms (20 and 18 m² area) and a specially insulated listener test room (91 m² area). In the test room, 16 subjects can actively participate in the assessment simultaneously.

Various audio technologies developed for military and civilian purposes can be evaluated in this infrastructure with the help of simulations of various acoustic environments. The listener room can be used as a “Human Factors Laboratory” thanks to its silent terminals and touch screen monitors.

APPLICATIONS
- Intelligibility tests
- Communications efficiency and quality of service tests
- Evaluation of civilian and military voice encoder equipment and systems
- Acoustic and digital embedding (cockpit, tank, aircraft, helicopter, restaurant, concert, outdoors etc.)
- Acoustic database construction and recording for language-dependent and language-independent technologies
Electro-optics and Laser Systems Laboratory is established in line with the mission of TÜBİTAK BİLGEM to perform R&D activities in laser and laser systems involving critical technologies for the nation, to develop systems and to ensure the continuity, to improve the quality of laser-optic products, and to become one of world’s leading nations in this field.

CAPABILITIES

- Development of new laser technologies
- Development of high power laser systems
- R&D studies in free space optical communication systems
- R&D studies in fiber-optic communication systems
- Quantum cryptology and related R&D studies
- R&D studies in optical systems based on radiation sources other than laser
- Activities related to adaptive optical systems
Cathode and Microwave Vacuum Tube Research Labs aim is to design and develop cathodes for microwave vacuum tubes (Magnetrons, TWTs, etc.) for various applications like satellite communications, electronic warfare systems, high power radar systems and medical systems.

**RESEARCH INFRASTRUCTURE AND TECHNICAL CAPABILITIES**

- Hydrogen, Argon and Nitrogen sintering technology up to 2500 °C
- Brazing technology in high temperature and vacuum environment
- Cathode coating technology with metal thin films
- Material characterization technology
- Pneumatic and Isostatic pressing technology
- Cathode and e-Gun test and characterization technology in vacuum tube environment
- Microwave vacuum tube (Magnetron, TWT) infrastructure development technology
- Thermionic Cathode, Magnetron and TWT prototype infrastructure development technology

**FACILITIES**

- 4500 m² indoor area
- 2500 m² laboratory area
- 500 m² cleanroom area
- Electromechanics Laboratory
- Chemistry Laboratory
- Microwave Vacuum Tube Sources Assembly, Prototype Production and Test/Measurement Laboratory
- Cathode Prototype Production and Test Laboratory and Test Laboratory
- Sintering and Brazing (in Hydrogen Atmosphere) Laboratory

Subject to Approval of Turkey Ministry of National Defence for Selling.
Cryptanalysis Laboratory carries out the cryptanalysis activities under Vice Presidency of Testing and Evaluation (TDBY). In Cryptanalysis Laboratory, cryptographic security of information security solutions for military, public and private institutions/organizations are being studied by expert cryptographers since 1995.

Cryptanalysis Laboratory performs its activities in two major fields: "cryptographic algorithm analysis" and "cryptographic architecture analysis". During these activities, the cryptographic security of a cryptographic algorithm or an architecture against open literature attacks or original attacks is determined.

Cryptanalysis of cryptographic algorithms comprises following activities:

- Cryptanalysis and evaluation of cryptographic primitives, such as cryptographic encryption/decryption algorithms, cryptographic hash algorithms, message authentication codes, etc. in cryptographic systems. Security conditions of these cryptographic primitives are also determined.

Cryptanalysis of cryptographic architectures comprises following activities:

- Analysis of cryptographic aspects of key management plan, synchronization of cryptographic parameters, authentication, access control, authorization, confidentiality, integrity, signature, source verification mechanisms, etc. in cryptographic systems and their mutual interactions.

- Determination of cryptographic management rules that are vital for the security and maintenance of cryptographic systems.
Parametric measurements of antennas (up to 1.5 m) up to 40 GHz frequency band are performed in the Spherical Near Field Measurement System Lab. Also, their 3D radiation patterns are obtained.

<table>
<thead>
<tr>
<th>Spherical Near Field Measurement System</th>
<th>Moderate and Low Gain Antenna Measurements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Room Dimensions</td>
<td>7.5 x 4.7 x 3.3 m (L x W x H)</td>
</tr>
<tr>
<td>Maximum Dimension of Test Antenna</td>
<td>1.5 meter</td>
</tr>
<tr>
<td>Maximum Weight of Test Antenna</td>
<td>75 kg</td>
</tr>
<tr>
<td>Frequency Range</td>
<td>0.75 GHz - 40 GHz</td>
</tr>
<tr>
<td>Scanning Plane</td>
<td>Full Spherical</td>
</tr>
</tbody>
</table>
PURPOSE
OKTEM (Common Criteria Test Laboratory), established in 2001, conducts tests of and provides consultancy and training for Information Technology (IT) products. OKTEM guarantees the security of an IT product by evaluating it according to an international standard known as Common Criteria (CC) or ISO/IEC 15408. This standard not only determines the security requirements of the IT product users, but also guides the vendors to implement these requirements on the products/systems. It is a principal method for security evaluation of the products/systems.

Product vendors choose having Common Criteria evaluations in order to increase the security quality of their products and to get assurance that the claimed security features are valid and have been independently tested against recognised criteria. Additionally, security evaluations of some IT products, which are of critical importance for national security and which are widely used both at public and military domains, are all carried out within the Center.

OKTEM conducts Common Criteria security evaluations for a wide range of products including firewalls, smart card integrated circuits, software security applications and secure flash disks. The evaluation results are reported in an Evaluation Technical Report (ETR) to the Turkish Standards Institute (TSE), which is the CC Certification Body of Turkey. The final step of the evaluation process is the certification of the product by TSE. The CC Certificate issued by the TSE are recognised and valid in countries, including USA, Canada, Australia, Japan and many European countries, who have signed the Common Criteria Recognition Agreement.

Apart from the Common Criteria evaluations of IT products, OKTEM offers consultancy to specify the security requirements of critical products and develops Protection Profiles that are compatible with the international standards. Additionally, crypto module conformity tests in accordance with the Security Requirements for Cryptographic Modules (ISO/IEC 19790) and Basic level Security Evaluations (TSE K 505) are also being conducted.

Quality of the evaluations conducted by OKTEM is accredited by the Turkish Accreditation Agency (TÜRKAK) within the scope of the ISO 17025.

ACTIVITIES
- Common Criteria Product Evaluation
- Common Criteria Protection Profile Evaluation
- Common Criteria Consultancy
- Common Criteria Training
- Crypto Module Conformity Test
- TSE K 505 Basic Level Security Evaluation
CAPABILITIES

▪ Radar Systems Engineering
  Coverage area analysis
  Analysis and design
▪ Algorithms and Software Development
  Target detection
  Doppler processing
  Micro-doppler processing
  Clutter reduction
  Baseband signal processing
  Multi-target tracking
  Data association
  Target classification
  Communications layer for distributed and embedded systems
  Multilayered software architecture
  Multi operating systems support (Linux & Windows)
  Radar database management
  EUROCONTROL ASTERIX coding
  Built-in test (BIT) management
  Radar PPI, PPI Map etc. interface development
  Web statistical analysis with web access
▪ Signal Processing Hardware
  FPGA-based signal processing
  Analog-digital card design
  VME/VPX multi-core high speed digital system design
  High speed baseband signal generation and processing
  SFP+ (Enhanced small form-factor pluggable) data transmission
▪ Radar Verification and Validation
  Target signal & environment simulation
  Performance evaluations
  Laboratory testing
  Field tests

Advanced radar signal processing research and development, radar systems integration and validation/verification studies are carried out in the Radar Research and Development Laboratory. Current research areas are basically pulse-Doppler, FMCW, mm-Wave and phased-array radars.
RAPSİM, having its name from the acronym of the Turkish title corresponding to ‘Radar Performance and Signature Analysis Centre’ was founded within BİLGEM (Informatics and Information Security Research Center) in TÜBİTAK (The Scientific and Technological Research Council of Turkey) with the aim of assessing the wind turbine effects on military and civilian electronic systems on March 1 of 2011.

By the virtue of its researchers that are specialized on electromagnetic theory, digital signal processing, communications and software designs, RAPSİM is able to model and simulate radar, navigation and communications (RNC) systems by considering real terrain characteristics and operating parameters. The modeling and simulation processes that have been administered in a high-fidelity engineering sense aim to produce insightful and inspiring outcomes that are propped up by high-level graphical user interface and automatic report generating tools.

Some of the extensive consultation and services provided by RAPSİM are:

- **Impact Assessment Analysis**
  Technical interaction analysis performed to investigate and determine the possible effects of wind farms on the performance of RNC systems,

- **Radar Cross Section (RCS) Computation/Reduction Studies**
  The monostatic and bistatic RCS characteristics of platforms, and further studies on reduction and enhancement of the RCS values for specific conditions with the help of the simulation tool RASES (i.e., the former product of RAPSİM),

- **Additional researches on the performance metrics of point-to-point communications, radar/RF coverage investigation, and signature analysis from the perspective of pattern recognition and classification.**
RF R&D Laboratory consists of personnel and infrastructure capable of research and development up to 110 GHz frequency band. There exists a realization and test/measurement RF/microwave infrastructure up to 40 GHz. Millimeter wave band designs can be implemented in “Chip On Board” technology-based MCMs (Multichip Modules) using the facilities of Gebze Campus.

RF DESIGN PRODUCTS
- S-band very high power (16 kW) solid-state power amplifiers
- X-band medium power (< 1 kW) solid-state power amplifiers
- Frequency up-down converters (X-, Ku-, K-band)
- Passive RF Components (filters, diplexers, combiners, couplers, etc.)
- Very low phase noise DDS-based frequency synthesizers
- Very low noise amplifiers
- Radio link systems in ITU-R frequency bands up to 25 GHz
• TEMPEST Test Laboratory conducts tests of equipment, systems and platforms processing classified data in accordance with the NATO standard SDIP 27/1 "NATO TEMPEST Requirements and Evaluation Procedures".
• Equipment and system tests are carried out using Fully Anechoic Chambers while platform tests are conducted on site.

The activities conducted at TEMPEST Test Laboratory are:
• Equipment/System TEMPEST Tests
  - All types of cryptographic communication devices
  - TEMPEST-protected devices, such as PCs, scanners, fax, printers
• Platform TEMPEST Tests
  - Satellite cryptographic communication equipment (e.g. GOKTURK-1)
• TEMPEST Consultancy and TEMPEST risk analysis
• Facility TEMPEST installation inspection
• TEMPEST trainings

Subject to Approval of Turkey Ministry of National Defence for Selling.
YİTAL was established for conducting research in the fields of semiconductor technology in 1983.

YİTAL currently uses the 0.7 μm CMOS technology and has been developing the 0.25 μm 5 metal CMOS and SiGeC HBT BiCMOS processes. YİTAL, which develops original production processes, has reached present position by developing BIPOLAR technology, 3 μm and 1.5 μm CMOS technologies and producing low-volume military standard integrated circuits (IC).

YİTAL has the infrastructure which enables to implement IC design, mask production, water processing, water probing, packaging, circuit test and aging processes. Having 800 m2 of clean room space YİTAL is the unique laboratory in Turkey which produces ICs in semiconductor technologies.

For the first time in 1999, the ICs containing national crypto algorithms developed at TÜBİTAK UEKADE's cryptographic devices were designed and manufactured with YİTAL CMOS processes. From this date, the institute's crypto ICs are designed and manufactured at YİTAL.

YİTAL team has designed Turkey's first National Smart Card IC with the use of combined power coming from extensive experience in IC design and the knowledge of secure circuit design captured through 6th Framework Programme. These ICs are currently in use.

Parallel PCI NTDS (Naval Tactical Data System) Interface Communication Card is implemented with the use of YİTAL ICs. These ICs are manufactured with high voltage 24 V CMOS process which is specially developed for this work.

Additionally, radon gas and photodetector production processes are developed. Detectors produced with these processes are widely used with success in applications oriented towards Turkey’s needs.

YİTAL, parallel to Turkey’s objectives in the field of space, is conducting research space-grade IC manufacturing technology. Within this scope, there is an ongoing effort to develop SOI CMOS process.

YİTAL is in collaboration with various universities providing support to master’s and doctoral programs which will enhance Turkey’s semiconductor technology and electronic design capability.

Developing advanced semiconductor manufacturing processes and having military-standard products used in Turkey’s critical applications manufactured with this processes, YİTAL has the capability of converting a design on paper to a packaged and tested IC with national resources.
Software Test and Quality Assessment Laboratory (YTKDL) was established in January of 2010 with the objective of conducting test and quality assessment activities of software projects. The center aspires to meet test and quality assessment needs of software projects in both national and international scale by checking conformity to international software standards. Software test and quality assessment activities carried out in YTKDL aim at contributing to the software quality by detecting possible defects in the early phases of the projects.

SOFTWARE TEST SERVICES
The services are focused on both functional and non-functional testing by well-experienced teams using advanced test methodologies and test automation tools. Details of the services provided are as follows:

- Preparation of test plans
- Participation in reviews (documents, requirements, design, codes)
- Preparation of tests and maintenance of traceability
- Setting up the test environment in cooperation with the project team
- Development of testing software
- Execution of test cases (software, system and acceptance tests) for integrated products
- Execution of regression tests

STATIC CODE ANALYSIS
In the scope of static code analysis assessment of software source code is carried out by software static code analysis tools. Measuring software quality metrics such as maintainability, reliability, portability, efficiency and testability is also a part of the assessment. After measurements corresponding software quality analysis reports are prepared. These reports include analysis about the potential problems in the software quality as well as recommendations on where to start improving the code.

USABILITY ASSESSMENTS
Within the scope of the usability assessments, the following activities are conducted: Evaluation of web applications in compliance with the rules of “TS ISO 9241-151 Web User Interface rules (Human System Interaction Ergonomics Standards)”, preparation of the related reports, compatibility evaluation of the internet websites of public institutions with KAKIS (Websites for Public Institutions).

LOAD TESTS
Conduct of load tests of websites and preparation of evaluation reports.

TS ISO/IEC 25051 COTS PRODUCT EVALUATION
Evaluation of the commercial off-the-shelf software products (COTS) in compliance with a series of documents such as “TS ISO/IEC 25051 Software engineering—Software product Quality Requirements and Evaluation (SQuaRE)” and preparation of the corresponding reports.

TS 13298 EDMS SOFTWARE EVALUATION
Compatibility evaluation of Electronic Document Management System Software within the national standards of TS 13298 Electronic Document Management System (EDMS) and preparation of the corresponding report.

TRAINING AND CONSULTANCY
YTKDL also provides training and consultancy services using its knowledge and experience in software V&V activities.
Wireless Communication Technologies Research Laboratory (KİTAL), which was established at TÜBİTAK BİLGEM under the sponsorship of Ministry of Development, aims at providing an infrastructure that will support industry-leading efforts in this critical area. KİTAL, which will significantly increase the R&D capabilities of Turkey in the area of wireless communication technologies, provides a laboratory infrastructure for experimenting different aspects of heterogeneous networks. It will include equipments for R&D activities of both 3rd and 4th generation technologies (3G, LTE, etc.) and 5th generation technologies (LTE-A, 802.11ad, etc.) whose standardization has been going on. KİTAL will also provide infrastructure for R&D of next generation tactical wireless communication technologies towards enabling “Network Centric Warfare”. KİTAL infrastructure will be made open to universities and companies to support wireless communication R&D activities in Turkey.

Several ongoing projects within KİTAL framework concentrate on different aspects of wireless communications research.

- OFDM based 4G-5G mobile broadband wireless system project
- Outdoor wireless mobile mesh network project
- Detailed real-time emulation of heterogenous wireless systems project
TÜTEL, collaborating with YİTAL (Semiconductor Technologies Research Laboratory) which has the biggest infrastructure about microelectronic in our country, is opening into service as a considerable infrastructure and it will create equality of opportunity around the country.

With TÜTEL, it is aimed to attain worthwhile know-how to our country on VLSI (Very Large Scale Integration) technology, and to establish an ecosystem which all parties (researchers, firms, universities and regular citizens) can exploit. In this ecosystem, besides the educational activities; design, development, test and fabrication capability services will be provided on a prototype and ‘proof of concept’ level. TÜTEL will carry out advertisements and expositional activities to improve of awareness on microelectronic for everybody from all ages throughout the country.

Goals
- Establishing an organization across the country to support VLSI designs for universities and companies
- Establishing and actuating the center laboratory for VLSI education, design, prototype development and verification
- Providing necessary software and licenses for CAD tools used in VLSI design
- Organizing training programs for VLSI design
- Constructing national and international cooperation for VLSI improvements
- Supporting VLSI fabrications in certain scales and sizes

Core Functions
- Working as a VLSI education center
- Operating as a VLSI design center by providing CAD tools
- Functioning as a VLSI test center with necessary laboratory infrastructure support
- Providing VLSI prototype fabrication support
- Coordinating national VLSI design programs to develop 1.5μm, 0.7μm CMOS ve 0.25μm SiGe BiCMOS technology prototypes
- Organizing international cooperations in order to develop VLSI prototypes for a couple of 10-nm technologies,

Services
- VLSI Design Education
- VLSI Design Environment Support
- VLSI Fabrication Support
- VLSI Test and Verification Environment Support
- VLSI Research Support
- VLSI Cooperation Support