

KEC

Smartcard Access Device



TÜBİTAK

UEKAE

**NATIONAL RESEARCH
INSTITUTE OF ELECTRONICS
AND CRYPTOLOGY**



KEC, Smartcard Access Device

KEC- Smartcard Access Device is one of the main terminal devices of EKDS-Electronic Authentication System, designed for electronic identity verification operations in the applications of an electronic service provider society or cooperations on internet media. (Other types of KEC Devices are Personal KEC, Mobile KEC, Emergency Service KEC, Kiosk KEC, Turnstile KEC, Card Issuance KEC). The purpose of EKDS is to enhance security for the operations executed between service participants. It reads the identity and signature cards used for providing security in electronic way, for the operations and services realized by users on internet environment and verifies the information in the cards. The expression enhancing electronic security means the topics listed below:

- 1) Being sure from the related service participant identities of the application operations executed on internet environment,
- 2) Assuring the origin of the data sent to service participant is really from who sent it by using electronic signature for the application operations executed on internet environment, providing integrity and denial free operations.
- 3) Recording the date and realized by whom information of the operations executed and taking the precautions like digital signing for the non-reputation.

Related with the variety of applications, KEC carries out authentication functions communicating in secure way with automation systems (ethernet) in LAN architecture over GSP- Security services Platform software using SSL or with web based applications and desktop applications in PC platforms over USB interfaces.

There are three smartcard slots on the device for the electronic identity cards of service participants to be used in authentication operations and the electronic signature card of service participant, to be used in electronic signing for the executed operation. Inside of the device, SAM module which has the certificates of the device, provides the security of the operations achieved by the device.

In KEC devices, biometrics methods are used besides using PIN for increasing the security of identity verification of service participant; there are fingerprint sensor on the device and externally connected veinprint sensor for reading fingerprint / veinprint of service participant.

For easy and user friendly usage, KEC Device can be used with KECHUB- KEC Mobile Terminal Device which is used for service participant's operations. KEC, being a commercial, portable, office type device which operates in commercial temperature range, is also compatible to commercial EMI/EMC, CE,CC standards.

For providing the needs of large scaled cooperations, there exists the extra operation mode of the KEC devices operating together in a master-slave network configuration.

COMMUNICATION AND INFORMATION ASSURANCE

TECHNICAL SPECIFICATIONS

Security Levels	Four levels of security depending on policy (Card[1], Card[2], PIN, PIN + Biometrics)
Applications	<ul style="list-style-type: none"> - Identity verification- authentication for different security levels - Local and general identity verification- authentication for each security level - XML based document signing using an electronic signature card - Adaptation to different authentication policies (representative usage, authentication levels, generic policy, having the approval of serviced person in case of problem met during biometric identity verification. - Fingerprint and/or veinprint verification depending on the security level
Language Support	Turkish, English (Other languages can be supported upon demand)
Access Security	User password required for device configuration, AKIS (The Smartcard Operating System designed by TUBITAK - UEKAE) based electronic identity smartcards for authentication operations
Algorithms	2048-bit RSA, SHA-256, 3DES, AES256, SSL v3
User Interface	3.5" 320x240 256K colors TFT LCD display, 20-keys keypad
Smartcard Slots	IEC/ISO 7816 compatible 3 smartcard slots: Service participant electronic signature card slot, two service participants' electronic identity card slots, IEC/ISO 7816 compatible 1 SAM (Security Access Module) card slot
Biometric Sensors	Fingerprint sensor (on-device), veinprint sensor (externally connected optional module)
Alarm mechanisms	Auditory and visual alarms via buzzer, LCD and LEDs
Communication Interfaces	<ul style="list-style-type: none"> - USB 2.0 Full Speed host port (for connections of KEC mobile terminal device or veinprint sensor device) - USB 2.0 Full Speed slave port (for PC connection) - 10/100 Mbits Ethernet port (for GSP- Sec. Serv.Platform - connection) - VGA monitor interface
Power Consumption	<5W
Dimensions and Weight	12cm / 21cm / 6,5 cm (W/L/H) , 472 g
Operating Temp.	0°C ... +45°C
Storage Temp.	-20°C ... +65°C
Relative Humidity	%90 at +40°C
Supported Standards	<ul style="list-style-type: none"> - IEC/ISO 15408 (Common Criteria) Ortak Kriteri - EAL4 - EN 55022 EMI/EMC - CE

Due to continuing product improvements, these specifications are subject to change without notice.

TUBITAK UEKAE

T: +90262 648 1000 • F: +90262 648 1100 • E: uekae@uekae.tubitak.gov.tr

W: <http://www.uekae.tubitak.gov.tr> • A: PO.BOX.: 74, 41470, Gebze, Kocaeli, TURKEY