

Mobile Security Solutions based on Smart Card



Requirements and application scenarios

The growing demands for mobility and security require applications that also provide financial transactions, secure internet access or access to sensitive personal or enterprise data, besides the smart card functionality.

certgate Smart Card microSD™ or MMC™ are hardware-tokens in the flash™ memory form factor of a micro Secure Digital Card (microSD™) and MultimediaCard (MMC™) industry standards with signature and encryption functions. microSD™ adapters for SD™, miniSD™ or USB™ interface are available.

The most efficient way to expand mobile data security in Banking, IT and PKI infrastructures from desktop systems to all kinds of portable devices (laptops to PDAs or smart phones). It is a perfect solution for mobile and desktop applications and highest security demands, because it is based on tamper-resistant strong encryption (RSA 2048 bit) in the smartcard and thus allows the usage of low-cost mobile devices, like PDAs and smart phones. The smart card as the heart of the security with crypto processor and private/secret key store can easily be taken out of the office PC and plugged into the laptop or PDA without the hassle and security thread of transferring/synchronizing data between these systems.

Keys can be generated within the card, never have to leave the systems and thus are not exposed to interception. It has been certified according to the current highest security levels EAL5+ (*certgate* Smart Card microSD™).

It provides like a natural and practical electronic cryptographic key highest hardware-based security along with ease of use, universal applicability and attractive price. It enables secure and profitable business process. The flash memory and the crypto-controller can be addressed independently from the terminal device.

Standards

certgate Smart Card microSD:

- microSD™ flash memory card standard
- JavaCard™ 2.2.1 (JavaCard™ 2.3 planned) and Global Platform™ 2.1.1 compliant
- on card secure random number generator FIPS PUB 140-2 and BSI AIS 31 compliant
- RSA 2048 bit on-card security algorithms

...now and everywhere

Characteristics and functions (microSD™)

- smart card usage for WindowsMobile, Symbian or PocketLinux applications via device microSD™, miniSD™, SD/MMC™ slot
- smart card usage for Windows/Linux desktop/notebook applications via a SD Slot or USB-card reader/-writer or via ActiveSync / Bluetooth / WLAN directly in the mobile device microSD™, miniSD™ or SD/MMC™ slot
- certificate, public and private key (RSA 2048 bit) upload to smart card (8 general purpose)
- on-card secure key generation (RSA 2048 bit)
- on-card secure signature generation with private key (RSA, PKCS#1.5 padding)
- on-card secure public key encryption / private key decryption (RSA, no padding)
- on-card secure random number generator; user accessible
- Speed: RSA 2048 bit signature: 0,5s.; RSA 2048 bit key generation: from 10 s up.

Your benefits

- PKI support and two-factor authentication
- fits into all of the widespread SD™ and MMC card slots used for flash memory
- perfect security for desktop and mobile applications using smart card technology
- easily plugged in and out of devices and can be carried along so that one person can always authenticate, sign and encrypt based on a universal set of keys only stored inside the card.
- protected private key store on-card (it is impossible to read out private keys from the smart card and keys never have to leave the card and thus cannot be intercepted)
- usage of low cost mobile devices (PDA, smart phone) with integrated card reader
- can additionally be used like any other flash memory to store (sensitive) data

certgate provides secure, mobile, flexible and economic solutions for your customers and employees, increasing:

- the availability of your services and applications
- your network security
- your cost efficiency
- your competitiveness

Products and components

The IICS products perfect security in all relevant scenarios by meeting the requirements of the most user-level applications: FinTS/HBCI banking clients, VPN clients, desktop or PDA software for the encryption of sensitive data, guaranteeing data integrity, access security, the certified user authentication and many more.

- **certgate** *Smart Card microSD/MMC PKI* for desktop and mobile data security within IT and PKI infrastructures
- **certgate** *Smart Card microSD/MMC FINANCE* for desktop and mobile data security within FinTS/HBCI-based banking infrastructures
- **certgate** *CSP for Windows and Windows Mobile*, (cryptographic service provider), a windows standard interface to provide security for data and communication in your Windows and WinCE-based applications
- **certgate** *Crypto API* offers an easy access to the card functionality and enables Windows mobile and desktop applications the possibility to execute cryptographic operations like encrypt, decrypt, signature and verify, through the certgate Smart Card microSD/MMC onto a mobile device
- **certgate** *Smart Card Management System* for the administration of the certgate smart card. The software is running on a Windows PC and is connected with the smart card via an USB card reader/writer or ActiveSync and a PocketPC
- **certgate** *Smart Card SDK* for the integration of all security functionalities into third-party applications