



certgate
mobile security now!



certgate Smartphone Protector
**ULTIMATE SECURITY
FOR YOUR
SMARTPHONE**



Your Advantage

certgate Smartphone Protector

- Highest security level for your smartphone
- Pre-boot authentication and kernel protection
- Smartcard protected memory encryption
- Operating system protected by proprietary certificates and keys
- Tamper-proof interface configuration and control along your organization's security policy
- Smartcard based email encryption and internet security

certgate Smartphone Protector

Network security is one of the key issues to be addressed in every IT strategy. Behind the firewall there are strict rules in place to block out potential intruders, maintain data integrity, and prevent critical information from falling into the wrong hands. In view of the growing risk associated with theft and misuse of sensitive data, a corporate network without precisely defined access policies has almost become an impossibility. At the same time, the increasing use of mobile applications on PDAs and smart phones, in particular when linked to corporate applications, leads to the emergence of a whole new set of risks. Ensuring toplevel network security without sacrificing the advantages of mobile communications is one of the key challenges to IT administrators today. But how can data communication of smartphones be reliably protected against spying and abuse?

The **certgate Smartphone Protector** - based on the **certgate SmartCard microSD** - offers comprehensive hardware-based security for all mobile devices with a microSD card slot. The **certgate SmartCard** - in the shape of a microSD flash memory card - reliably prevents unauthorized access to, and tampering with, the data and applications on your mobile device.

The **certgate Smartphone Protector** combines top-level security with the advantages of miniaturization and the use of universal standards. It enables you to implement your organization's security policy on the mobile devices that your executives and field staff have in daily use.

The combination of a flash memory with a highperformance, common-criteria-evaluated cryptographic processor makes it possible to generate and store digital key pairs (RSA 2048 Bit) and certificates.

Proven encryption mechanisms, the separation between knowledge (PIN) and possession (smart card) and the tamperproof device configuration together offer a maximum security potential. ■

Your Benefits

- Fast and economical integration of mobile devices in your organization's security infrastructure
- Identical or even higher security level for usage of mobile applications and for mobile network access
- Security level individually scalable – up to the level needed for top-security zones
- Use of any security applications compatible with conventional smartcards also for mobile devices
- Insertion into normal card slot (SD, miniSD, microSD) of mobile devices under Windows Mobile – no additional drivers needed
- No replacement of terminal devices (smartphones, PDAs, laptops, etc.) required
- No additional cost for card readers or any special mobile devices
- Certificates stored on certgate card also usable on desktop PCs, directly or via adapter
- Limited administrative effort required for one-time configuration of certgate application to comply with internal security policies
- Maximum possible security for user, application, and corporate data
- Safe initial authentication of user
- Single sign-on to check user's authorization.

Characteristics and Functions

- Windows Mobile™-devices supported
- Supported operating systems: Windows™ Mobile, Windows™ PC
- Interfaces: certgate API, CSP, PKCS#11, PC/SC
- Available adapters: microSD™ to miniSD™, microSD™ to SD™, microSD™ to USB
- Mobile device usable as a smartcard reader with Windows™ -PC und -Notebook
- Mass storage capacity: 1 GB
- Storage protection: All user data are encrypted by a hybrid method of RSA 2048 and AES 256. All used keys are generated at the smartcard.

Standards

- SD specification: 1.1 and microSD™ Addendum 1.1
- Smartcard chip: NXP P5CC072 smartcard controller; Common Criteria EAL5+ certificated
- On-card secure random number generator; FIPS PUB 140-2 and BSI AIS 31 compliant
- On-card RSA 2048 bit security algorithms
- Enhanced 80C51 microcontroller (Secure_MX51/NXP)
- ISO7816 interface for APDU transfer between smartcard and SD controller
- Smartcard operating system: JCOP™ 2.3.1 (Common Criteria EAL4+ certificated), JavaCard™ 2.2.1 and GlobalPlatform™ 2.1.1 compliant
- high resistance against SPA/DPA counter measure attacks; BSI DSZ CC 0227 compliant

certgate GmbH
Merianstrasse 26
90409 Nuremberg
Germany

Fon +49 (911) 93523-0
Fax +49 (911) 93523-52
E-Mail info@certgate.com
www.certgate.com