



StarSign® PKI Cards

High security for organizations

The StarSign PKI Card is a well-established member of G+D's StarSign family. It is seamlessly integrated in different middleware solutions, compliant to established global industrial standards.

In conjunction with the middleware, StarSign PKI Cards are the classic solution in corporate environments for secure log-in, single sign-on, remote access over VPN, preboot authentication, digital signature, and document, disk, file, and e-mail encryption.

An embedded contact, contactless only or dual interface chip is used to ensure secure logical access.

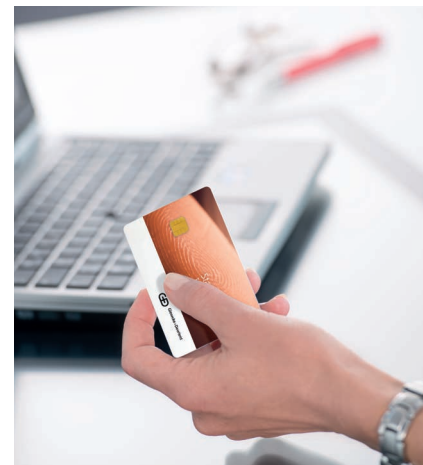
The optional middleware is available for Windows up from Version 7, Mac OS X, and Linux and can handle the communication between the PKI Cards and host applications.

When combined with a contactless interface, the StarSign PKI Card can also be used for physical access control, making it the all-in-one security element for

any enterprise: it enables time recording or proprietary payment functionalities, logical and physical access control, also serving as an employee ID badge. To meet the requirements of physical access, the card can be customized with Mifare application from NXP and the Secure UHF Solution from G+D Mobile Security.

StarSign PKI Cards are a leading product group in the market and are integrated in smart card readers and smart card management systems (CMS) of major vendors for the mentioned use cases. StarSign cards are mainly based on the dual interface technology to serve the all-in-one-approach, but it is of course also possible to customize them as a contact only version exclusively for logical access. On demand, hybrid versions are possible.

The advantage of smart card technology is that it can serve various needs with just one card using different applets (EMV and PKI), thus allowing multiple applications on a single card. This has been successfully implemented in use cases where the financial functions of debit and credit of a payment card have been combined with logical PKI applications for digital signature.



G+D's smart card and middleware security bundle:

- StarSign PKI Cards with 80 KB or 144 KB EEPROM, powered by Sm@rtCafé Expert 7.0 – G+D's newest Java-based card operating system.
- G+D Middleware bundle with StarSign PKI Cards.

Since StarSign PKI Cards are based on G+D's most modern Java Card-based Smart Card operating system Sm@rtCafé Expert 7.0, they support a wide range of crypto features such as AES, RSA, elliptic curves, and up to SHA-512. The StarSign PKI Card modules have been granted FIPS 140-2 Level 3 certification by NIST (National Institute of Standards and Technology).



Card personalization and individualization services are available:

- Optical personalization such as card body printing.
- Electronic personalization such as pre-installation and configuration e.g. of PKI applications.

G+D has broad-based expertise in smart card production. Depending on customerspecific requirements, we can offer additional integrated security features to combat counterfeits (e. g. guilloches).

G+D card bodies provide enhanced card durability, as well as alternatives to standard PVC materials.

Our smart cards can be supplied in various materials for the card bodies such as:

- Polyvinyl chloride (PVC)
- Polyethylene terephthalate (PET)
- Glycol-modified polyethylene terephthalate (PETG)
- Polycarbonate (PC)
- High Flexible Foil (HFF)

StarSign PKI Cards: Benefits at a glance

• EASY, EFFICIENT & FLEXIBLE

StarSign PKI Cards offer a plug-and-play solution in any platform supporting smart cards (Windows up from Version 7, 32 and 64 bit, as well as Mac OS and Linux Redhat and Ubuntu).

• MAXIMUM SECURITY AND COST EFFICIENCY

StarSign PKI Cards reduce card management costs and increase user convenience by combining logical and physical access control in a single card. They offer a convenient and portable authentication device that can be extended/upgraded in the field.

• COMMITMENT TO SUSTAIN YOUR INVESTMENT

As Java-based smart cards, StarSign PKI Cards are designed to provide a multi-application platform to meet current requirements and future needs during the card life cycle. The card's open architecture enables post-issuance loading of applets, maximizing the return on investment for issued cards.

• APPLICABLE ACROSS ALL MARKET SEGMENTS

Since StarSign PKI Cards are based on standard Java Card and Global Platform specifications, it is possible to integrate further applications in this multi-application card at any time.

• TOP-LEVEL SECURITY

The StarSign PKI Card smart card operating system, with its state-of-the-art crypto features such as RSA and elliptic curves as well as the SHA-512, prohibits unauthorized usage.

• FIPS CERTIFICATION

The StarSign PKI Card security module with its Java Card-based Sm@rtCafé Expert 7.0 operating system has been granted FIPS140-2 Level 3 certification.

• WIDE RANGE OF CARD BODIES

A choice of card bodies addresses different needs regarding service life and personalization modes. Furthermore, a FIPS 201 compliant card body that meets the strong requirements of the U.S. Federal Government, for example, is available.

• G+D IS YOUR PARTNER OF CHOICE

G+D excels with its competence gained from many years of experience in printing banknotes and security documents. As a global group, Giesecke+Devrient (G+D) has a 160-year history of developing security technologies and has played a major role in their standardization.

With outstanding levels of customer satisfaction, G+D is a global leader and premier brand in security technologies. A brand that creates confidence.



Technical data of StarSign PKI Cards

	Sm@rtCafé Expert 7.0	Sm@rtCafé Expert 7.1
Hardware Chip EEPROM Interfaces	SLE78CLFX4000P 80 / 144 KB Dual Interface (T=CL Type A) Contact-based (T=0 / T=1)	NXP P60CDxxx 80 / 145 KB Dual Interface (T=CL Type A) Contact-based (T=0 / T=1) Mifare Desfire EV1
Packages	T-M8.4-8-1; P-M8.4-8-3; VQFN 32	PDM 1.1
Cryptography	4096 bit RSA, AES 512 bit, DSA up to 1024 bit, Triple-DES 3-key, ECDSA up to 256 bit, ECDH up to 256 bit, SHA-224, SHA-256, SHA-384, SHA-512, RNG: according to NIST SP 800-90	2048 bit RSA, AES 512 bit, DSA up to 1024 bit, Triple-DES 3-key, ECDSA up to 256 bit, ECDH up to 256 bit, SHA-224, SHA-256, SHA-384, SHA-512, RNG: according to NIST SP 800-90
Certifications Chip Operating System	Common Criteria EAL 5+ FIPS 140-2 Level 3	Common Criteria EAL 5+
Standards	- Java Card 3.0.4 Classic - GlobalPlatform 2.2.1 + Amendment D (SCP03) - ISO 7816, ISO 14443A	- Java Card 3.0.4 Classic - GlobalPlatform 2.2.1 + Amendment D (SCP03) - ISO 7816, ISO 14443A
Available Applets / applications	- PIV and different PKI applet and middleware - StarSign Security Domain Applet	- PIV and different PKI applet and middleware - StarSign Security Domain Applet
Feature Overview	- Multiple security domains - Multiple DAP (DES, AES and RSA) - Delegated management - RMI	- Multiple security domains - Multiple DAP (DES and RSA) - Delegated management - RMI
Standards Support	PKCS11, Base CSP, X.509 certificates	PKCS11, Base CSP, X.509 certificates

**Giesecke+Devrient
Mobile Security GmbH**
Prinzregentenstrasse 159
81677 Munich
Germany

P +49 89 41 19-0
mobilesecurity@gi-de.com
www.gi-de.com/mobile-security

StarSign® and Sm@rtCafé® are registered trademarks of Giesecke+Devrient Mobile Security GmbH. SafeSign® is a registered trademark of A.E.T. Europe B.V. Windows is a registered trademark of Microsoft Corporation in the United States and other countries. Mac and Mac OS are trademarks of Apple Inc., registered in the U.S. and other countries. Linux® is an OSTG trademark or registered trademark in the United States and in other countries. Java™ and Java Card™ are registered trademarks of Sun Microsystems, Inc. ISO® and the ISO logo are registered trademarks of ISO Properties, Inc. The EMV™ mark is a trademark exclusively owned by EMVCo LLC. RSA owns the trademark "RSA®" for use in connection with its software products, services, and data security conference.

© G+D Mobile Security GmbH, 2020.

All technical data subject to change without notice. G+D Mobile Security patents.

December 2020

