

StarSign® Crypto USB Token

High security – seamless integration



Whenever you are looking for a highly secure and cost-effective token solution, you need the StarSign® Crypto USB Token.

Whether you are looking for strong user authentication, password management, secure digital signatures, or data security solutions for your organization, you need a smart card based USB token. The token provides easy integration into Public Key Infrastructure (PKI) architectures, enabling secure portable storage of keys and guaranteed non-repudiation for sensitive applications such as online banking, stock trading, and e-commerce.

The StarSign® Crypto USB Token contains G&D's Java Card based operating system Sm@rtCafé® Expert 6.0, which is listed for FIPS certification. Due to its rich variety of crypto features, the token is applicable across all market segments and can be used for a wide variety of security applications, e.g. secure login, single sign on, digital signature, disk & file encryption, secure banking, boot protection, PKI, e-mail protection, VPN remote access, web & web-based remote access, and many more.

With its compact and lightweight design, the StarSign® Crypto USB Token is your key to strong two-factor authentication, password management, and secure PKI implementation for your organization. The design of the StarSign® Crypto USB Token allows individual customer branding with logo and/or company name on the token cap.

FIPS 140-2 level 3 certification is pending from NIST (National (US) Institute for Standards and Technology) for the crypto module and the entire token.

The StarSign® Crypto USB Token implements and utilizes the standard USB device class CCID (USB smart card reader functionality) and – optionally – the human interface device class (HID). The host driver for all Microsoft Windows platforms is distributed via the Windows update service. Support for Mac OS X and Linux distributions is available on request. The communication interface between the host PC and the token is USB 2.0 full speed. Optional middleware can handle the communication between token and host application. The token offers users and issuers maximum security and cost efficiency.



Giesecke & Devrient
Creating Confidence.

StarSign® Crypto USB
Token benefits at a glance

• **Easy, efficient & flexible**

The StarSign® Crypto USB Token offers a plug & play solution that uses a CCID interface. Optionally, the token can be operated in HID mode.

No additional drivers need to be installed to run the token on Windows XP, Vista, and Windows 7, 32 and 64 bit, which means flexibility for users at its best. On request the token will be supported by Linux and MAC OS.

An individual token serial number located at the rear may help to increase (user) help desk efficiency.

• **Innovative design**

Boasting a new design, yet fully integrated into the family design concept, its small size guarantees that additional USB devices can be used in adjacent USB ports.

• **Customizable housing**

The modern design leaves maximum space for individual issuer branding on the housing cap.

• **Applicable across all market segments**

Since the token is based on the new Java Card operating system Sm@rtCafé® Expert 6.0, it is possible to integrate further applications at any time.

• **User interface**

A LED indicates the token's power status.

• **Top-level security**

The token's smart card operating system, with its wide range of crypto features such as RSA and elliptic curves as well as the SHA 512, secures almost all applications conceivable for the new USB token.

• **FIPS certification**

The token has been submitted for FIPS 140-2 level 3 certification. Certification is expected in Q3 2011 as the token is made of certified materials and features G&D's established smart card security.

Technical data of StarSign® Crypto USB Token

Smart Card Operating System
 SmartCafé® Expert 6.0

Hardware
 Security controller – NXP P5CC081
 EEPROM – 80 KB
 Interface – Contact-based T=1

Cryptography
 - RSA 2048 bit, AES 256 bit
 - DSA up to 1024 bit
 - Triple-key triple-DES
 - 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: Common Criteria EAL 5+
 - Operating system: FIPS 140-2 level 3*
 - Token: CE, FCC, WEEE, RoHS



* Under certification

Standards
 - Java Card™ 3.0.1 Classic
 - GlobalPlatform 2.1.1 + Amendment D (SCP03)
 - ISO® 7816
 - USB 2.0 full speed
 - CCID Device Class Specification (2005)

Available applets / applications
 - StarSign®
 - PKCS#11
 - Further applets on request
 - HID device class specification (optional)

Additional features
 - Multiple security domains
 - Multiple DAP (DES and RSA)
 - Delegated management
 - RMI

Operating conditions
 0°C to 40°C at 90% RH

Approx. dimensions
 56 x 16 x 9.5 mm

Weight
 5 g

Storage conditions
 -40°C to 70°C

Supported host operating systems
 - Windows XP
 - Vista
 - Windows 7 – 32 and 64 bit
 - Linux and MAC OS 10.5 on request

System interface
 - PKCS#11
 - Microsoft CSP
 - USB 2.0
 - PC/SC (CCID)

Maximum power consumption
 < 80 mW

Giesecke & Devrient GmbH
 Prinzregentenstrasse 159
 P.O. Box 80 07 29
 81677 Munich
 GERMANY
 Phone: +49 (0) 89 41 19-23 84
 Fax: +49 (0) 89 41 19-90 93
 www.gi-de.com
 starsign@gi-de.com

© Giesecke & Devrient GmbH, 2011
 StarSign® and SmartCafé® Expert are registered trademarks of Giesecke & Devrient. Other company product and service names may be trademarks of these or other companies. All technical data subject to change without notice. G&D patents.