



StarSign® Crypto USB Token M

Delivers the key to digital identity and secure online services

The Challenge

The more everything becomes digital, the more dependent medium and large enterprises, governments, and banks become on information systems and the greater their concerns about data integrity and loss.

As a result, all will have to make trade-offs between the value inherent in a hyperconnected world and the associated risks (e.g. operational disruption, intellectual property loss, public embarrassment).

Privacy and security have turned into key issues for potential service providers serving users or companies for their mobile workforce. Likewise, machine authentication is essential for remote updates or monitoring in the IoT space.

It still is a major challenge to authenticate users to grant them access to sensitive data or authorization for certain applications. Similarly, remote maintenance services such as secure software updates are the next hurdle to take.

The Solution

G+D provides the StarSign Crypto USB Token in response to these growing security needs.

The StarSign Crypto USB Token with its compact and lightweight design is the convenient key to strong two-factor authentication, password and credential management, encryption, and secure digital signing applications.

FIPS 140-2 level 3 and Common Criteria EAL 5+ certification of the token enables compliance with country-specific regulations.

Did you know ...

G+D has already delivered over 40 million crypto USB keys.



Technical key features

SMARTCARD OS

- G+D Sm@rtCafé® Expert 7.0 Java Card OS
- Running on a smartcard security controller

SMARTCARD SECURE ELEMENT MEMORY

- 215 KB free EEPROM, e.g. PKI applet and 15 key pairs and certificates

STANDARDS AND SPECIFICATIONS

- Java Card 3.0.4 Classic
- GlobalPlatform 2.2.1 + Amendment D (SCP03)
- Multiple security domains
- Multiple DAP (3DES, AES, RSA, ECDSA)
- Authorized and delegated management
- RMI
- USB 2.0 full-speed
- CCID Class specifications (2005)

CERTIFICATIONS

- Chip: Common Criteria EAL 5+ And FIPS 140-2 level 3
- Token: CE, FCC, WEEE, RoHS

SECURITY AND CRYPTOGRAPHY

- Enhanced high-security memory management
- Secured OS against DPA/SPA and physical attacks RNG according to NIST
- Trusted Channel Booster® for accelerated ICAO secure messaging functionality and support for various privacy protocols
- Symmetric encryption: 3-DES up to 768 bit, AES up to 256 bit, SEED up to 128 bit
- Asymmetric encryption: RSA up to 4096 bit DSA up to 1024 bit ECDSA up to 521 bit ECDH up to 521 bit
- Digital signatures with symmetric or asymmetric encryption
- Hash algorithms: SHA-224, SHA-256, SHA-384, SHA-512

AVAILABLE APPLETS / APPLICATIONS

- AET SafeSign
- PKCS#11
- Further applets on request

SUPPORTED PLATFORMS

- Windows OS
- Linux and MAC OS

SYSTEM INTERFACE

- PKCS#11
- Microsoft CSP
- PC/SC (CCID)

AVAILABLE SMARTCARD TOOLS (OPTIONAL)

- G+D JLoad

APPROX. DIMENSIONS AND WEIGHT

- L40mm x W12.3mm x H4.7mm
- 5.9 g

INGRESS PROTECTION CLASS

- IP67 for the token body

OPERATING CONDITIONS

- 0°C to 40°C at 90% RH

STORAGE CONDITIONS

- -40°C to 70°C

MAXIMUM POWER CONSUMPTION

- < 125 mW



Benefits

- Delivers top-level security with its wide range of crypto features.
- Provides compliance with local regulations (FIPS 140-2 level 3 and Common Criteria EAL 5+ certified).
- Allows easy and flexible integration into smartcard applications.
- JavaCard 3.0 compliance benefits applet developer community.
- Helps to increase help desk and administration efficiency with unique lasered serial number.
- Offers a plug & play solution using a CCID interface. No additional drivers needed to run the token on Windows XP, Vista, and Windows 7, which means flexibility for users at its best. Other OS on request.
- Availability also as an embedded secure element.
- Combines the advantages of a smartcard on a USB device, without the burden of deploying readers to end users.
- Permits individual issuer branding on body of token.
- Provides highest level of robustness due to metal token housing.
- Small size guarantees that additional USB devices can be used in adjacent USB ports.
- Very fast processing due to single chip solution.
- G+D is your partner of choice with its 160-year history developing security technologies and playing a major role in their standardization.

Did you know...

G+D was the first supplier of USB keys for online banking.

Giesecke+Devrient
Mobile Security GmbH
Prinzregentenstrasse 159
81677 Munich
Germany

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

November 2020