Giesecke+Devrient

Sm@rtCafé® Expert

Java-based, open-platform card and token operating system

StarSign Sm@rtCafé Expert:

Interoperability, security, reliability

Commitment to open standards to sustain your investment

Giesecke+Devrient has been developing security technologies and playing a major role in their standardization since 1852. Sm@rt Café Expert cards are G+D's implementation of the current Java Card™ and GlobalPlatform standards (for details on Sm@rtCafé Expert, see overview on page 2). They are designed for all industry domains and enable services to be combined for various markets such as banking, industry, and government – on a single card. All our Sm@rtCafé Expert products ensure an accurate implementation of current GlobalPlatform specifications. G+D is represented on GlobalPlatform's Board of Directors and continues to work hard to establish and promote interoperability specifications industry-wide. Sm@rtCafé Expert faithfully implements the Java Card API and has been thoroughly tested with the official Test Suite provided by Sun®. In addition, it is fully compliant with relevant ISO® communication standards.

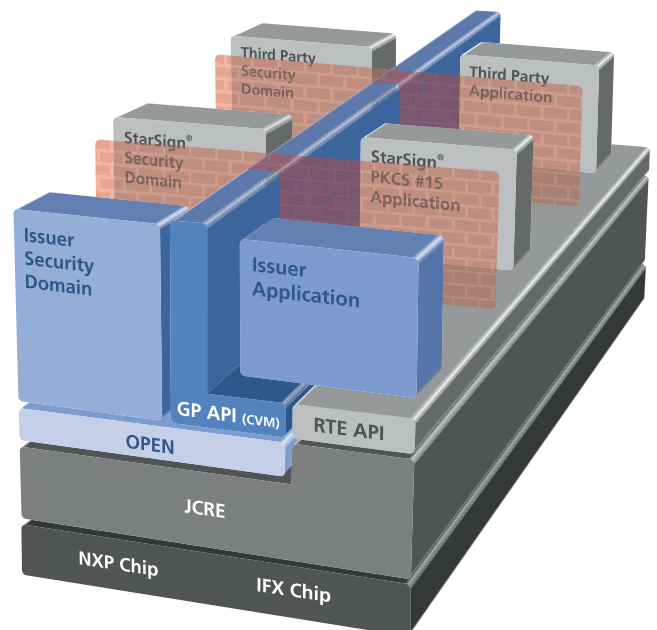### Cutting-edge security features

Sm@rtCafé Expert's extensive range of state-of-the-art security algorithms and functions provides the best protection for your valuable applications and data.

The implementation of the firewall mechanisms on Sm@rtCafé Expert cards ensures a reliable separation of the different applets with their assigned data (see figure "GlobalPlatform Security Architecture").

This prevents illicit access to the data or objects of other applications.

G+D is recognized for going the extra mile in security.

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 Packages	SLE78CLFX4000P 80 / 144 KB Dual Interface (T=CL Type A) Contact-based (T=0 / T=1) T-M8.4-8-1; P-M8.4-8-3; VQFN 32	NXP P60CDxxx 80 / 145 KB Dual Interface (T=CL Type A) Contact-based (T=0 / T=1) Mifare Desfire EV1 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

Sm@rtCafé Expert operating systems

Getting the most out of PKI

Sm@rtCafé Expert cards are integrated and tested with several global standard PKI middleware solutions (e.g. AET SafeSign, Cryptovision, Charismathics).

G+D's solution is the StarSign PIV smart card application. A Personal Identity Verification (PIV) credential is a US Federal government-wide credential used to access federally controlled facilities and information systems at the appropriate security level.

G+D can provide licenses of this supplier along with Sm@rtCafé Expert cards for immediate PKI enablement.

Meeting your needs with a choice of plat- forms

Sm@rtCafé Expert has been specially designed as a platform that supports smart card integrated circuits (ICs) from multiple manufacturers. This flexibility allows you to select the platform which meets your technical and price expectations, while giving you a wider choice of form factors (smart card or USB token), interfaces, (contact-based only, contact-based and contactless) and EEPROM capacity.

Java POWERED

Reliability and proven technology

The confidence that comes with experience

G+D has been making Java-based smart cards and tokens since 1998 and literally tens of millions of G+D's Sm@rtCafé Expert cards are used every day, around the globe. They are used in the Java card deployment of PIV cards providing around 1.5 million smart cards annually as one out of three suppliers. Tried and tested technologies, advanced security, and strict compliance with open specifications – with Sm@rtCafé Expert, reliability comes as a standard.

Optional features

Along with our robust security, you'll find a rich set of features that enable you to tailor Sm@rtCafé Expert to your exact needs. Here's a look at some of the advanced options available:
- Multiple security domains to enclose each application in its own security structure, e.g. EMV and PKI applications can coexist in the same card in their respective security domains
- Delegated management to ensure that each application is managed by its provider
- Data Authentication Pattern (DAP) verification to only accept applets digitally signed by specified vendors

Sm@rtCafé Expert: Benefits at a glance

- **EASY INTEGRATION AND INTEROPERABILITY:** Support for open standards with all GlobalPlatform specs, Sun Java Card and ISO
- **INCREASED EFFICIENCY:** Applets from different vendors run on one card (Write Once Run Anywhere)
- **EASY UPDATES, LOW ISSUANCE COSTS:** Extend/Upgrade functionality on cards in the field with applets
- **TIME SAVINGS:** Efficient and flexible architecture for application administration
- **RISK MINIMIZATION:** State-of-the-art security features prohibit unauthorized access
- **FLEXIBILITY:** Applets can easily be added to the card – whether customer developed or from a third party