CryptoCard Graphite Pro

CryptoCard Graphite Pro is the latest version of the CryptoCard Graphite card family. It is equipped with a newer, more efficient microprocessor and an expanded functional profile. The card uses a modern hardware platform, supports longer cryptographic keys, and can store more keys and certificates. It is supported by the same middleware software as the entire CryptoCard Graphite family and continues the success of earlier CryptoCard models, Carbon and multiSIGN, which became widely adopted in the Polish market and established the de facto functionality standard for electronic PKI cards.

The card can be used simultaneously for electronic signatures, data and correspondence encryption, user identification and authentication, and access control for resources and premises. CC Graphite can be used by both individuals and large companies.

Contactless card

Card requirements increasingly combine two separate areas of electronic card use. The first is linked to the contact processor and the signature, encryption, and authentication functionality it provides. The second is the typical corporate need for time and attendance registration or building access control, which is usually handled with contactless cards. The CC Graphite Pro card can include both contact and contactless components and serve both purposes at the same time, simplifying the user experience while reducing card purchase and management costs.

There are many types and variants of contactless cards on the market. Thanks to full control over the production cycle, the CryptoCard Graphite Pro card can be supplied with virtually any type of contactless component (hybrid configuration). The most common variants are MIFARE®, Unique, Indala, and iClass.

Identifier

In corporate applications, a plastic card is often used as an employee ID badge. CC Graphite Pro can also serve this purpose. The card's appearance can be defined by the customer. In the simplest version, it may be a white card printed with user data during individual personalization using specialized plastic card printers. For customers with more demanding requirements, high-quality offset printing and all standard plastic-card production options are available, including additional security elements such as holograms or guilloches.

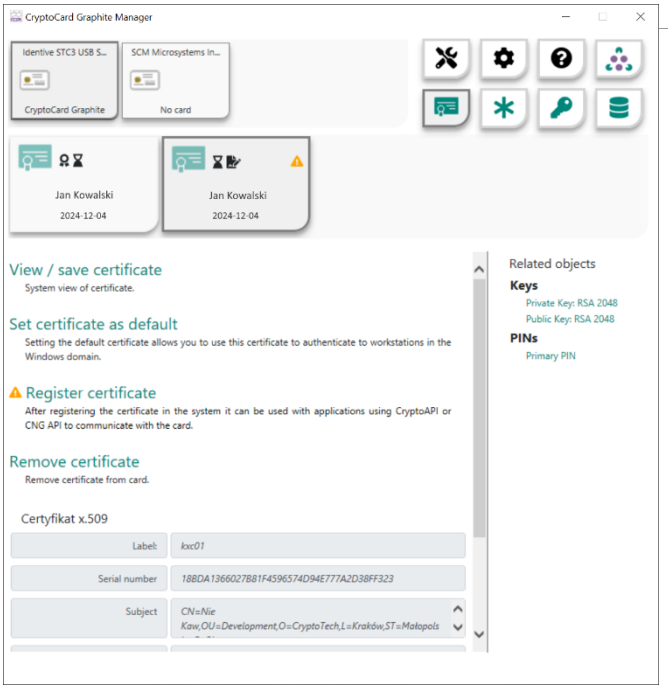
Electronic signature

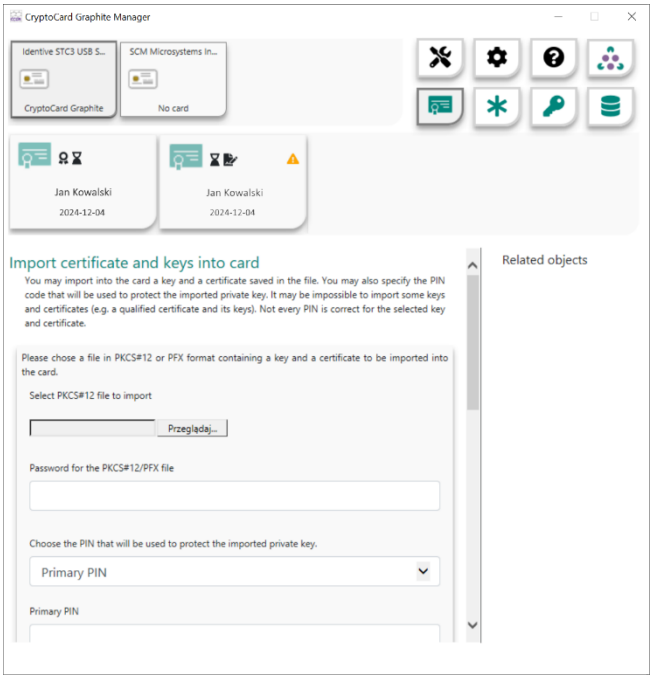
As with previous solutions from the CryptoTech portfolio, the CryptoCard Graphite Pro card can be used to create electronic signatures in all forms recognized under Polish and European

law, including those covered by the eIDAS Regulation. For secure signatures, the card constitutes a QSCD (Qualified Signature Creation Device) according to the specification defined in eIDAS and meets the requirements of Polish law for a secure signature verified by a qualified public key certificate. In accordance with technical standards and regulations, the card area responsible for handling and protecting the data used to generate such a signature is separated and subject to special controls over its use and management.

Software

The card works with a dedicated new edition of the CryptoCard Graphite Suite software, which enables management of the card contents and mediates communication between the card inserted in the reader and applications that use it, such as operating system logon, email programs, web browsers, and signing applications. CryptoCard Graphite Suite is middleware software fully compliant with industry standards PKCS#11 v2.01 and later, as well as CryptoAPI and CNG API.



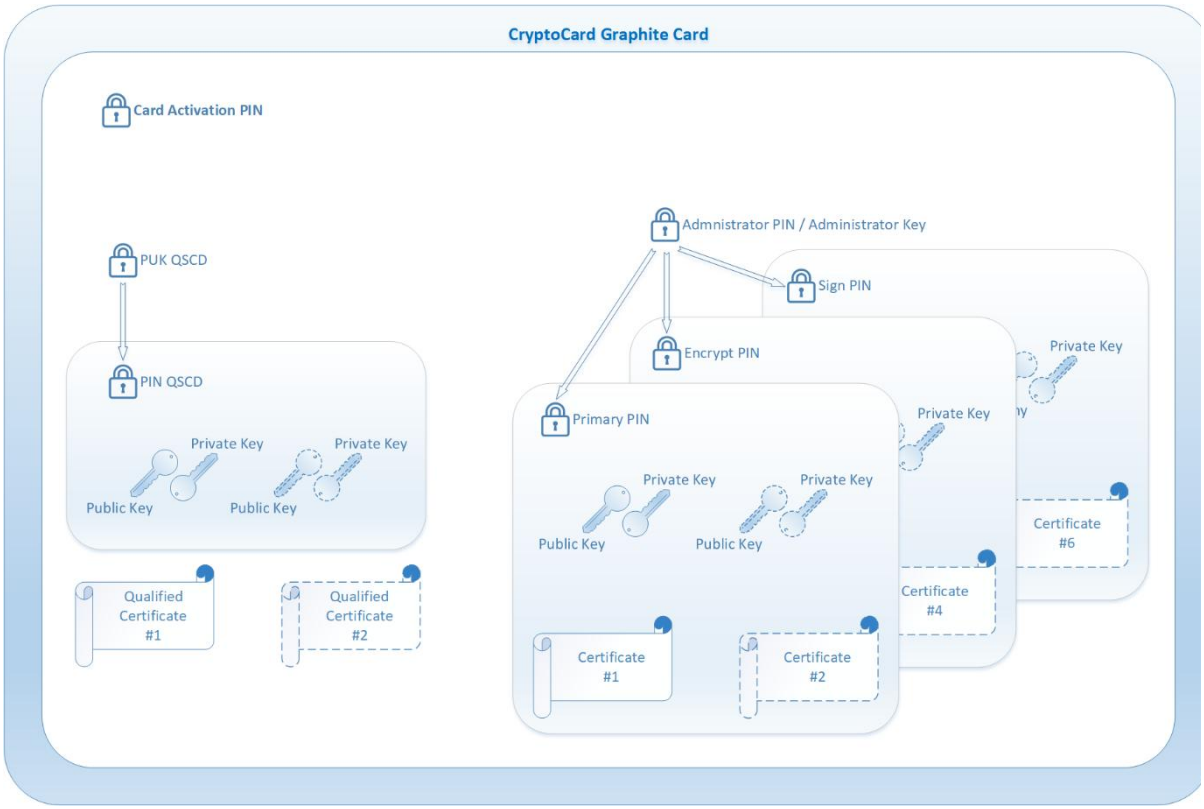


The new card is equipped with a programming interface for modern Windows operating systems and works through a module compliant with the Microsoft Smart Card miniDriver v7 API used by CSP and KSP.

Hardware

The card uses a modern processor equipped with more than 96 kB of FLASH/EEPROM memory and a cryptographic coprocessor that performs operations with RSA keys up to 4096 bits, as well as increasingly popular signatures based on elliptic curves, known as ECC (Elliptic Curve Cryptography), with a 256-bit key length. Communication between the software using the card and the card processor may be encrypted, providing additional protection against advanced attacks.

The card platform is based on the JavaCard v3.0.4 and GlobalPlatform v2.2.1 specifications. The PKI application installed on the card is certified together with the entire platform according to Common Criteria EAL4+ and is included on the official list of SSCD and QSCD devices compliant with eIDAS.



Technical specification

Memory	over 96 kB
RSA signing and encryption	keys up to 4096 bits
ECC GF(p) signing	256-bit keys (soon), 384, 512, and 521-bit keys on request
Supported algorithms	RSA, ECC, DES/3DES, AES, SHA1 (limited), SHA-256, SHA-384
Secure Messaging support	Yes
Key generation	on-card (RSA, ECC)
Protocols	T=0
Industrial standards support	PKCS#11, MS CAPI/CSP/CNG, miniDriver, PC/SC
Certified security of the qualified signature application (QSCD)	CC EAL 4+
Certified hardware platform	CC EAL 5+
OS support	Windows 8.1, 10, 11, Windows Server (32/64-bit operating system support), Linux (via PKCS#11), MacOSX (PKCS#11) and limited support for Windows 7 and 8.
Other	support for Remote Desktop and Terminal Services