

Supported cryptographic tokens

Native smart card platforms

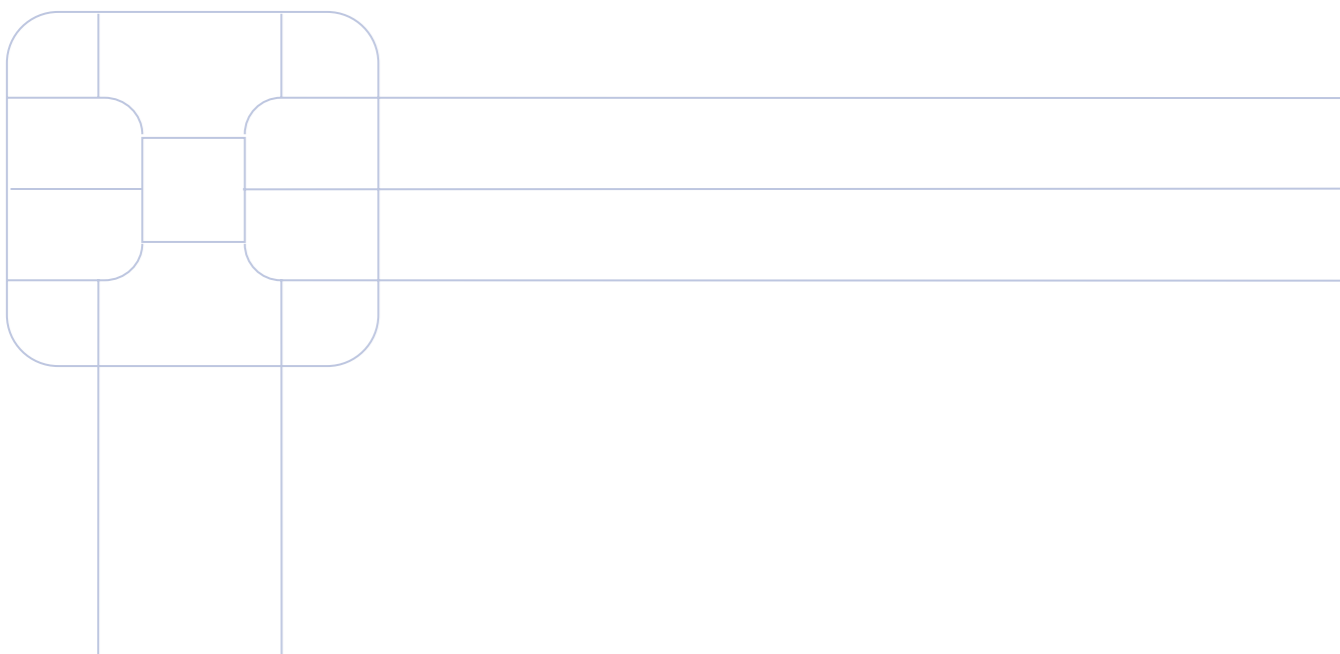
Java Card platforms

- G&D StarCOS 2.3
- G&D StarCOS 2.4
- G&D StarCOS 2.5 DI
- G&D StarCOS 3.0
- G&D StarCOS 3.2
- SIEMENS CardOS 4.3B

Java Card platforms

- G&D SmartCafe Expert 2.0
- G&D SmartCafe FIPS 64
- G&D SmartCafe 3.0

- Gemalto GemSafe 2.0
- Oberthur ID-One ClassIC v7.0
- NXP JCOP 2.4.1 R2/R3 with ID&Trust IDentity applet
- NXP JCOP 2.4.2 R2/R3 with ID&Trust IDentity applet
- NXP JCOP 3 P60 with ID&Trust IDentity applet
- NXP JCOP 4 P71 with ID&Trust IDentity applet



Our SmartID middleware connects smart cards to applications through standard interfaces.

It ensures that e-ID document functions such as e-signature and e-ID can be accessed by third-party applications, online and offline.



SmartID enables PKI applications to use any type of cryptographic tokens through standard APIs. Highly customizable and easy to integrate, the middleware can be used with a variety of secure signature creation devices in trusted and untrusted signature environments.







The SmartID Token Management Utility allows users to manage all objects on their cards, including PINs, PUKs, certificates and personal data.

The e-ID Client module and corresponding e-ID Server subsystem make access to ID cards' eIDAS token functions possible, such

as age verification, restricted identification and ID attribute sharing, via OpenID Connect. It ensures fast and easy integration of the e-ID card functions with third-party systems, making the e-ID card the centre of the digital identity ecosystem.

The Mobile SDK module also works with the e-ID server subsystem in order to make e-signature and e-ID functions accessible to Android and iOS smartphones with an NFC interface.

BENEFITS

-  Maximum efficiency by using existing cards and equipment
-  Flexible, customizable software that minimizes costs
-  Card management through a single interface for better control
-  Increased security even in untrusted environments
-  Supports all ID cards functions
-  Can be used for online and offline uses cases

DISCOVER FEATURES

- QSCD USAGE IN TRUSTED AND UN-TRUSTED ENVIRONMENT**
 SmartID middleware can be used in both trusted and un-trusted environment, depending on the user's needs. Secure Messaging based on symmetric or asymmetric device authentication are supported.
- SUPPORT OF DIFFERENT TYPE OF PKI TOKENS AND SMART CARD READERS**
 With the help of Card Abstraction Layer and Reader Abstraction Layer it is possible to involve new smart card and/or smart card reader products in the system. TeleTrust and most common proprietary PINPAD readers are supported.
- PLUGIN ARCHITECTURE**
 It is implemented in order to support 3rd party software modules for the management of proprietary on-card data from the Card Manager.
- INDUSTRY STANDARD TOKEN MANAGEMENT MODULES**
 PKCS#11, Microsoft CSP, Microsoft Minidriver based on PKCS#15 file structure.
- CUSTOMIZED CARD PROFILES**
 Based on specific customer requirements. E.g. different kind and number of security objects (i.e. keys, Transport PIN, Signature PIN).
- OPERATING SYSTEMS SUPPORTED**
 Supports the most popular PC operating systems (Windows, Mac OS, Linux) as well as mobile operating systems (iOS, Android).

DISCOVER COMPONENTS

SmartID consists of the following main components to integrate cryptographic hardware tokens into PKI applications. All SmartID components are built in a modular way to support a wide range of smart cards and can be customized for proprietary cards.

SmartID PKCS#11

PKCS#11 standard developed by RSA Laboratories is the industry standard platform independent API to cryptographic tokens. SmartID implementation of the PKCS#11 library has Smart Card and Smart Card Reader Abstraction layers in order to support different type of tokens and smart card readers.

SmartID CSP

SmartID CSP provides integration between Microsoft Crypto API compliant applications with SmartID supported cryptographic tokens with the help of SmartID PKCS#11.

SmartID Minidriver

SmartID Minidriver is a common interface to Microsoft Smart Card Base Cryptographic Provider (CSP) or Crypto Next Generation (CNG) software modules.

SmartID PAM

SmartID Pluggable Authentication Module is a security component to be integrated into (Qualified) Signature Creation Applications (SCA) if Secure Message is needed between the SCA and QSCD for integrity and confidentiality. Helper HSM is supported optionally.

SmartID Card Manager

SmartID Card Manager utility provides various management functions for the card holder of his/her security objects stored on the cryptographic token such as: initialization/personalization, change/unblock PIN/PUK, import/view/delete digital IDs, verify certificate validity, etc.

Certificate registration utility

SmartID certification registration utility provides automatic registration and de-registration of X.509 certificates stored on cryptographic tokens on token insertion and removal. It is typically convenient in multi-user environments.