



sc/interface

Flexible and secure smart card and token middleware

sc/interface connects the smart card or token to virtually any PKI enabled application. It is a sophisticated universal middleware with support for dozens of smart cards, security tokens of several different form factors, and all major desktop operating systems.

Functions	
	<ul style="list-style-type: none"> • Increasing the level of security with smart cards or tokens • Comfortable functionality for managing the lifecycle of PINs, keys and certificates • PIN management: <ul style="list-style-type: none"> • PIN change • unlocking User-PINs • offline PIN reset • PIN Cache Mode • PACE-PIN and -PUK • Session-PIN according to Minidriver Spec. version 7.06 • Key & certificate management: <ul style="list-style-type: none"> • Generation of key pairs and secret keys, secure storage of secret keys • Import of keys and certificates (PKCS#12) • Generation of certificate requests (PKCS#10) • Registration of certificates in Microsoft Windows Certificate Store • Certificate update for Windows 2003 / 2008 / 2012 • Initialization & rollout functions: <ul style="list-style-type: none"> • Generation of smart card profiles (PKCS#15, PKCS#15 with PACE, PKCS#15 biometric profile, cv profile, third party profiles) • Biometric Match-on-Card for Java Card with Precise BioMatch™ Flex and Digital Persona™ • Other Token management functions: <ul style="list-style-type: none"> • Configuration of default smart card container for MS-CAPI • Creation, storage, and administration of data on smart card • PKCS#11 Virtual slots enable multiple keys per card with unique PINs used per key

Features	<ul style="list-style-type: none"> • Support of <ul style="list-style-type: none"> • numerous tokens and profiles • a wide range of applications • multiple platforms • Secure messaging • Encrypted session PIN support via Minidriver and PKCS#15-PACE profile • Secure PIN pad support • Multi-language support (language files) • Microsoft HCK certifiable (on customer request) • Java Card GlobalPlatform supported up to Version 2.2.2 with SCP03 • ECC keys up to 521 Bit, platform dependent • RSA keys up to 4096 Bit, platform dependent
Supplied Modules	<ul style="list-style-type: none"> • PKCS#11 Module (v2.20) • Full-featured CSP • Microsoft certifiable Smart Card Minidriver for Crypto Next Generation Key Storage Providers (Specification v7.06) • Microsoft certifiable Read Only Minidriver • Token for OS X (10.9, 10.10.4, 10.11) • User Tool for simple administration tasks (sc/interface utility) • Admin Tool for complete configuration and administration (sc/interface manager) • Register Tool for certificate registration in Windows Certificate Store for all supported smart cards and USB tokens (sc/interface register tool)
Supported Standards	<ul style="list-style-type: none"> • PKCS#10 for Certificate Requests • PKCS#11 • PKCS#12 for Key and Certificate Import • PKCS#15 • ISO/IEC 7816 • Microsoft CryptoAPI, CNG • OS X Token • PC/SC • PACE as defined in BSI TR-03110 • ISO/IEC 19794-2

Supported Smart Cards	<p>ATOS: ATOS CardOS: M4.01a / V4.2 / V4.2B / V4.2C / V4.3 / V4.3B / V4.4 / V5.0 / V5.3</p> <p>AustriaCard JCOP: 21 V2.2 / 21 V2.3.1 / 31 V2.2 / 31 V2.2 contactless / 31 V2.3.1 / 31 V2.3.1 contactless / 31/72 V2.3.1 / 31/72 V2.3.1 contactless / 41 V2.2.1 / 41 V2.2.1 contactless / 41 V2.3.1 / 41 V2.3.1 contactless / 41 V2.4 / 41 V2.4 contactless</p> <p>Bundesdruckerei Gold card v1</p> <p>D-Trust: D-Trust Card 3.0, 3.1, 3.2</p> <p>ePasslet-Suite 1.1/1.2: on JCOP V2.4.1R3, on JCOP V2.4.1R3 w or w/o PACE Profile</p> <p>ePasslet-Suite 2.0/2.1: on JCOP V2.4.2R3, on JCOP V2.4.2R3 w or w/o PACE Profile</p> <p>Gemalto: TOP IM GX4</p> <p>G&D Sm@rtCafé: Expert: 3.1 / 3.1 contactless / 3.2 / 4.0 / 5.0 / 6.0 / 7.0</p> <p>G&D STARCOS: 3.0 / 3.2 / 3.4 / 3.5</p> <p>HID Crescendo: C700 / C700 contactless</p> <p>Infineon: JCLX80 jTOP / JCLX80 jTOP contactless / SLJ52 (Trusted Logic)</p> <p>Microsoft: Virtual Smart Card</p> <p>NXP JCOP: V2.1 / V2.2 / V2.2 contactless / V2.2 / V2.3.1 / V2.4 / V2.4.1 / V2.4.2 / V2.4.2 R3</p> <p>SwissSign: suisseID (CardOS M4.3B / M4.4)</p> <p>TCOS: 3.0 R1 Signature Card/ 3.0 R4 Signature Card 2.0</p> <p>And many more</p>
Supported Tokens	<ul style="list-style-type: none"> • Certgate microSD (NXP JCOP) • G&D Sm@rtCafé Expert 3.2 USB token • IDENTIV @MAXX (SCT3512) • NXP JCOP: V2.2.1 IDptoken 200 • SwissSign SwissID (CardOS M4.3B) • Swissbit <p>And many more</p>

Supported Readers and Terminals	<ul style="list-style-type: none"> • All PCSC 2.0 compliant readers (OS X, Unix/Linux needs „pcsc-lite“) • Recommended: <ul style="list-style-type: none"> • Identive CLOUD 2700 F (not for OS X) • Identive CLOUD 4700 F • Cherry SmartTerminal ST-2000 (Class2) • REINER SCT cyberJack® RFID standard • REINER SCT cyberJack® wave
Supported Profiles, Applets, and Data Structures	<ul style="list-style-type: none"> • A.E.T. SafeSign • ATOS • Charismathics • cryptovision ePKI applet 2.8 • cryptovision ePKI applet v2.126 w or w/o PACE extension • D-Trust • UniCard • G&D StarSign • Nexus • Siemens HiPath • SwissSign • Swiss Health Card eGK • TCOS • other PKCS#15 data structures, including PACE <p>And many more</p> <p>Not all card operating systems are supported for all solutions</p>

Supported Applications

- Fully compatible with Microsoft Forefront Identity Manager (FIM)
- Compatible with several Smart Card Management Systems (e.g. IDnomic OpenTrust CMS, Nexus Prime)
- Smart card login to a NetIQ eDirectory
- Smart card login to Linux and OS X
- Smart card login to Microsoft Active Directory
- Single Sign-on with NetIQ SecureLogin, ActivIdentity Secure Login, IBM Security Access Manager for Enterprise Single Sign-On, and Control Sphere
- TLS authentication with smart card (Internet Explorer, Edge, Chrome, Firefox, Safari, etc.)
- Microsoft Terminal Services, Citrix Xen Desktop 5.x and XenApp 6.x and XenDesktop 7.x
- Smart card login to Lotus Notes
- SAP Secure Login Client
- Digital signature and encryption via smart card for e-mails (Mozilla Thunderbird, Outlook, Outlook Express, Lotus Notes, PGP, Secude Secure Mail)
- Kobil mIDentity
- Qualified signatures with SuisseID, SwissSigner, D-TRUST card, D-TRUST multcard, TCOS
- Smart card support for VPNs (Checkpoint, Windows, Cisco, NCP, OpenVPN)
- Support of PKIs (CAmelot, PKIntegrated, RSA, Keon® PKI, VeriSign® PKI, GlobalSign PKI, Microsoft® PKI)
- Smart card login for disk encryption with Pre-Boot Authentication (Cryptware Secure Disk)
- MS Office 2010 / 2013 / 2016, Libre Office, Adobe Acrobat, Adobe Reader
- Support of applications using Sun-Java 1.7 (or higher) or IAIK-Library
- Encrypted and signed data according to S/MIME, PKCS#7, XML Encryption
- XML Digital Signature, and other formats

Supported Biometry	Use of Precise BioMatch™ Flex package for use with JavaCard based operating systems including NXP JCOP, Giesecke & Devrient Sm@rtCafé® Expert, Infineon JTOP, Neurotechnology MoC
Supported Platforms	<ul style="list-style-type: none"> • Windows 7 / 8.1 / 10 • Windows Server 2008 (R2) / Windows Server 2012 (R2) • Centos 7.1, Debian 8, Fedora 23, Mint 17.3, Red Hat Enterprise Linux 6.x (not Kerberos) / 7.x, OpenSuse 42.1 Leap, Ubuntu 14.04 LTS • OS X Mavericks (10.9), Yosemite (10.10.5), El Capitan (10.11.1) • Citrix XenDesktop 5.x / XenApp 6.x and XenDesktop 7 • VMware Horizon
System Requirements	<ul style="list-style-type: none"> • A supported operating system • A supported card reader with installed driver • A free USB or microSD slot for card reader • A supported security token • Additional application-specific requirements may occur