

# SCinterface

12/2019

## Powerful and secure Smart Credential Middleware

SCinterface connects a smart card or token to virtually any PKI-enabled application. It is a user-friendly and convenient universal middleware supporting dozens of smart cards, virtual smart cards, security tokens in different form factors and all major desktop operating systems.

### Functions

- Higher security level with smart cards or tokens
- Convenient lifecycle management for PINs, keys and certificates
- PIN management includes:
  - 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:
  - 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 2008 / 2012 / 2016
- Initialization & rollout functions:
  - Generation of smart card profiles (PKCS#15, PKCS#15 with PACE, PKCS#15 biometric profile, third party profiles)
  - Biometric Match-on-Card for Java Card with Neurotechnology™, Precise BioMatch™ Flex\*
- Other token management functions:
  - Configuration of default smart card container for MS-CAPI
  - Creation, storage and administration of data on smart card
  - Support of multiple keys per card with separate PINs

\* Legacy support only

## Technical Data Sheet - SCinterface

Features	<ul style="list-style-type: none"><li>• Support of numerous smart cards and profiles, a wide range of applications, multiple platforms</li><li>• Microsoft Virtual Smart Card (MS VSC) support, including initialization and personalization</li><li>• Citrix, VMware, Fat- and Thin Client (IGEL, eLUX) support</li><li>• Password Authenticated Connection Establishment (PACE) support</li><li>• Support of eIDAS-compliant „Siegel“ tokens</li><li>• Support of D-Trust siegel &amp; signature card</li><li>• Support of biometrics (biometric edition)</li><li>• Personal Identity Verification (PIV) support (PIV edition)</li><li>• Advanced signature profile support</li><li>• Elliptic Curve Cryptography (ECC) support</li><li>• Localization via language files</li><li>• Encrypted session PIN via Minidriver and PKCS#15-PACE profile</li><li>• Secure PIN pad support</li><li>• Secure messaging support</li><li>• Java Card GlobalPlatform support up to Version 2.2.2 with SCP03</li><li>• Support of ECC keys up to 521 Bit, platform dependent</li><li>• Support of RSA keys up to 4096 Bit, platform dependent</li></ul>
Supplied modules	<ul style="list-style-type: none"><li>• PKCS#11 Module (v2.20)</li><li>• Full-featured CSP</li><li>• Microsoft certifiable Smart Card Minidriver for Crypto Next Generation Key Storage Providers (Specification v7.06)</li><li>• Microsoft certifiable read-only Minidriver</li><li>• Crypto Token Driver for macOS</li><li>• SCinterface utility</li><li>• SCinterface manager for smart card initialization, personalization and management</li><li>• Register tool for certificate registration in Windows Certificate Store</li><li>• Plug-ins for validity warning and root certificate registration</li></ul>
Supported standards	<ul style="list-style-type: none"><li>• PKCS#10 for certificate requests</li><li>• PKCS#11</li><li>• PKCS#12 for key and certificate import</li><li>• PKCS#15</li><li>• ISO/IEC 7816</li><li>• Microsoft CryptoAPI, CNG</li><li>• macOS Crypto Token Driver</li><li>• PC/SC</li><li>• PACE (BSI TR-03110)</li><li>• ISO/IEC 19794-2</li></ul>

## Technical Data Sheet - SCinterface

<p>Supported smart cards and tokens</p>	<ul style="list-style-type: none"> <li>• AET: AET profile</li> <li>• ATOS CardOS: M4.01A / V4.2 / V4.2B / V4.2C / V4.3 / V4.3B / V4.4 / V5.0 / V5.3</li> <li>• AustriaCard JCOP: 21 V2.2 / 21 V2.3.1 / 31 V2.2 / 31 V2.3.1 / 31/72 V2.3.1 / 31 / 72 V2.3.1 contactless / 41 V2.2.1 / 41 V2.3.1 / 41 V2.4</li> <li>• D-Trust: D-Trust Card 3.1 / 3.2 / 3.4 (siegel card)</li> <li>• E.ON: Card V1 / V2</li> <li>• ePasslet-Suite 1.1/1.2 on JCOP V2.4.1R3 and on JCOP V2.4.1R3 with PACE Profile</li> <li>• ePasslet-Suite 2.0 on JCOP V2.4.2R3 with PACE Profile</li> <li>• ePasslet Suite 2.1 on JCOP V2.4.2R3 with PACE Profile</li> <li>• ePasslet Suite 3.0 on JCOP V3.0 and on G&amp;D Sm@rtCafé Expert 7.0 and on Infineon SLJ52 (Dolphin) with PACE Profile</li> <li>• Gemalto: TOP IM GX4, IDClassic 340</li> <li>• G&amp;D: Sm@rtCafé Expert 3.1 / 3.2 / 4.0 / 5.0 / 6.0 / 7.0</li> <li>• G&amp;D: STARCOS 3.0 / 3.1 / 3.2 / 3.4 / 3.4 (Swiss Health Card eGK) / 3.4 (Swiss Health Card VKplus G2) / 3.5 / 3.52</li> <li>• G&amp;D: StarSign CUT S Token (SCE 7.0)</li> <li>• HID: Crescendo C700</li> <li>• HID: iCLASS Px G8H</li> <li>• Infineon: JCLX80 jTOP / SLJ52 (Dolphin) / SLJ52 (Trusted Logic)</li> <li>• MaskTech MTCOS Pro 2.5 with PACE (BSI TR-03110), EC and RSA, including „profile protection“ (ISO 7816/15) via PACE-CAN</li> <li>• Microsoft: Virtual Smart Card</li> <li>• NXP: JCOP V 2.1 / V2.2 / V2.2.1 IDptoken 200 / V2.3.1 / V2.4 / V2.4.1 / V2.4.2 R1+R2+R3 / V2.4.2 R3 SCP 03 / 3.0</li> <li>• Infineon Secora Pay Java Card</li> <li>• Siemens: CardOS M4.01a / V4.3B / V4.4</li> <li>• SwissSign: suisseID (CardOS M4.3B / M4.4)</li> <li>• TCOS: Signature Card 1.0 / 2.0</li> <li>• TU Dortmund: UniCard (SECCOS)</li> <li>• Volkswagen: PKI Card (CardOS M4.3B /4.4)</li> </ul>
<p>Add-ons</p>	<ul style="list-style-type: none"> <li>• SCinterface Cache: secure PIN caching</li> <li>• PKCS#11 module for iOS</li> </ul>

## Technical Data Sheet - SCInterface

Editions	<ul style="list-style-type: none"> <li>• SCInterface biometric: match-on-card fingerprint authentication</li> <li>• SCInterface PIV: supports FIPS201-2 PIV NIST standard</li> <li>• SCInterface eID: for electronic identity documents</li> </ul>
Supported readers	<p>All PCSC 2.0 compliant readers (macOS, Unix/Linux needs „pcsc-lite“), recommended:</p> <ul style="list-style-type: none"> <li>• Identiv CLOUD 2700 F (not for macOS)</li> <li>• Identiv CLOUD 4700 F</li> <li>• Cherry SmartTerminal ST-2000 (Class2)</li> <li>• REINER SCT cyberJack® RFID standard</li> <li>• REINER SCT cyberJack® wave</li> </ul> <p>Mobile Readers:</p> <ul style="list-style-type: none"> <li>• Identiv @MAXX ID-1</li> <li>• Identiv SCR3500</li> <li>• Identiv SCL3711</li> </ul>
Supported readers with fingerprint sensors	<ul style="list-style-type: none"> <li>• ACS AET52 / AET63 / AET65</li> <li>• Omnikey 7121 Biometric</li> <li>• Precise Biometrics 250 MC</li> <li>• Precise Sense™ MC / MC-S</li> <li>• Precise Biometrics Tactivo™ for iPhone / iPad</li> <li>• All finger print readers supported by Neurotechnology</li> </ul>
Supported biometrics	<p>Biometric Match-on-Card for Java Card with Neurotechnology™, Precise BioMatch™ Flex*</p>
Cache configuration options	<ul style="list-style-type: none"> <li>• via KeyUsage</li> <li>• via time limit</li> <li>• via process (white/black listing)</li> </ul> <p>Options can be combined as desired</p>
Supported platforms	<p>Microsoft:</p> <ul style="list-style-type: none"> <li>• Windows 7 SP1**, 8.1, 10</li> <li>• Windows Server 2008 SP2 / R2 SP1**, 2012 R2, 2016, 2019</li> </ul> <p>Linux:</p> <ul style="list-style-type: none"> <li>• RHEL 6, 7</li> <li>• Ubuntu 16.04 LTS / 18.04 LTS</li> <li>• SLES 15</li> </ul> <p>macOS:</p> <ul style="list-style-type: none"> <li>• High Sierra (10.13)</li> <li>• Mojave (10.14)</li> <li>• Catalina (10.15)</li> </ul>

\* Legacy support only

\*\* Windows 7 and Windows Server 2008 R2 reach end of support on January 14, 2020

## Technical Data Sheet - SCinterface

Supported applications	<ul style="list-style-type: none"><li>• Compatible with several Smart Card Management Systems (e.g. Versa-sec, Intercede, IDnomic, OpenTrust CMS, Noreg, Nexus Prime)</li><li>• Smart card login to Linux, macOS, Microsoft Windows, Micro Focus eDirectory, IBM Notes</li><li>• Single Sign-on with NetIQ SecureLogin, ActivIdentity Secure Login, IBM Security Access Manager for Enterprise Single SignOn, and Control Sphere</li><li>• TLS authentication with smart card (Internet Explorer, Edge, Chrome, Firefox, Safari, etc.)</li><li>• Microsoft Terminal Services, Citrix, XenDesktop and XenApp</li><li>• SAP Secure Login Client</li><li>• Digital signature and encryption via smart card for e-mails (GreenShield, Mozilla Thunderbird, Microsoft Outlook, IBM Notes, Secude Secure Mail)</li><li>• Kobil mIDentity</li><li>• Qualified signatures with SuisseID, SwissSigner, all D-TRUST signature and siegel cards</li><li>• VPN (Checkpoint, Windows, Cisco, NCP, OpenVPN)</li><li>• Support of PKIs (CAmelot, PKIntegrated, RSA, Keon® PKI, VeriSign® PKI, GlobalSign PKI, Microsoft® PKI, Nexus)</li><li>• Smart card login for disk encryption with Pre-Boot Authentication (Cryptware Secure Disk, CPSD, etc)</li><li>• Microsoft Office, Libre Office, Apache OpenOffice, NeoOffice</li><li>• Adobe Acrobat, Adobe Reader</li><li>• Encrypted and signed data according to S/MIME, PKCS#7, XML Encryption</li><li>• XML Digital Signature, and other formats</li></ul>
System requirements	<ul style="list-style-type: none"><li>• Supported platform</li><li>• Supported card reader with installed driver</li><li>• Free USB or microSD slot for card reader</li><li>• Supported security token or MS VSC on TPM 2.0</li><li>• Additional application-specific requirements may occur</li></ul>



cv cryptovision GmbH  
Munscheidstr. 14  
D 45886 Gelsenkirchen

T: +49 209 16724-50  
F: +49 209 16724-61

[www.cryptovision.com](http://www.cryptovision.com)  
[info@cryptovision.com](mailto:info@cryptovision.com)