

Technical Data Sheet

cryptovision SCinterface

Powerful and secure Smart Card 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 and SO PIN change
 - unlocking user PINs
 - offline PIN reset
 - PIN cache mode
 - PACE-PIN and -PUK
- 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
- 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™
- 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

Technical Data Sheet - SCinterface

Features	<ul style="list-style-type: none">• Support of numerous smart cards and profiles, a wide range of applications, multiple platforms• Microsoft Virtual Smart Card (MS VSC) support, including initialization and personalization• Citrix, VMware, Fat- and Thin Client (IGEL, eLUX) support• Password Authenticated Connection Establishment (PACE) support• Support of eIDAS-compliant „Siegel“ tokens• Support of D-Trust siegel & signature card• Support of biometrics (biometric edition)• Personal Identity Verification (PIV) support (PIV edition)• Advanced signature profile support• Elliptic Curve Cryptography (ECC) support• Localization via language files• Encrypted session PIN via Minidriver and PKCS#15-PACE profile• Secure PIN pad support• Secure messaging support• Java Card GlobalPlatform support up to Version 2.2.2 with SCP03• Support of ECC keys up to 521 Bit, platform dependent• Support of RSA keys up to 4096 Bit, platform dependent
Supplied modules	<ul style="list-style-type: none">• PKCS#11 Module (v2.4)• Full-featured CSP• Microsoft certifiable Smart Card Minidriver for Crypto Next Generation Key Storage Providers (Specification v7.06)• Microsoft certifiable read-only Minidriver• Crypto Token Driver for macOS• SCinterface Utility for card management functions typically needed by users• SCinterface Manager for smart card initialization, personalization and management• Register Tool for certificate registration in Windows Certificate Store• Plug-ins for validity warning and root certificate registration
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• macOS Crypto Token Driver• PC/SC• PACE (BSI TR-03110)• ISO/IEC 19794-2

Technical Data Sheet - SCinterface

<p>Supported smart cards and tokens</p>	<ul style="list-style-type: none"> • AET: AET profile • CardOS: M4.01A / V4.2 / V4.2B / V4.2C / V4.3 / V4.3B / V4.4 / V5.0 / V5.3 / V5.4 / V5.5 / V6.0 • 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 • D-Trust: D-Trust Card 3.1 / 3.4 / 4.1 / 4.4 (siegel card) / 5.1 / 5.4 • E.ON: Card V1 / V2 • ePasslet-Suite 1.1/1.2 on JCOP V2.4.1R3 and on JCOP V2.4.1R3 with PACE profile • ePasslet-Suite 2.0 on JCOP V2.4.2R3 with PACE profile • ePasslet Suite 2.1 on JCOP V2.4.2R3 with PACE profile • ePasslet Suite 3.0 on JCOP V3.0 and on G&D Sm@rtCafé Expert 7.0 and on Infineon SLJ52 (Dolphin) with PACE profile • ePasslet Suite 3.5 on JCOP V4.0 and on Infineon Secora ID X with PACE profile • Gemalto: TOP IM GX4, IDClassic 340 • G&D: Sm@rtCafé Expert 3.1 / 3.2 / 4.0 / 5.0 / 6.0 / 7.0 / 8.0 • G&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 • G&D: StarSign CUT S Token (SCE 7.0) • HID: Crescendo C700 • HID: iCLASS Px G8H • Infineon: JCLX80 jTOP / SLJ52 (Dolphin/Trusted Logic), Secora • MaskTech MTCOS Pro 2.5 with PACE (BSI TR-03110), EC and RSA, including „profile protection“ (ISO 7816/15) via PACE-CAN • Microsoft: Virtual Smart Card • 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 / V3.0 / V4.0 / V4.5 • Siemens: CardOS M4.01a / V4.3B / V4.4 • SwissSign: suisselD (CardOS M4.3B / M4.4) • TCOS: Signature Card 1.0 / 2.0 • TU Dortmund: UniCard (SECCOS) • Volkswagen: PKI Card (CardOS M4.3B / 4.4)
<p>Add-ons</p>	<ul style="list-style-type: none"> • SCinterface Cache: secure PIN caching • PKCS#11 module for iOS • SCinterface VSC: TPM-based and TPM-less virtual smart card extension

Technical Data Sheet - SCInterface

Editions	<ul style="list-style-type: none"> • SCInterface biometric: match-on-card fingerprint authentication • SCInterface PIV: supports FIPS201-2 PIV NIST standard • SCInterface eID: for electronic identity documents
Supported readers	<p>All PCSC 2.0 compliant readers (macOS, Unix/Linux needs „pcsc-lite“), recommended:</p> <ul style="list-style-type: none"> • Identiv CLOUD 2700 F (not for macOS) • Identiv CLOUD 4700 F • Cherry SmartTerminal ST-2000 (Class2) • REINER SCT cyberJack® RFID standard • REINER SCT cyberJack® RFID komfort • REINER SCT cyberJack® wave • REINER SCT cyberJack® one <p>Mobile Readers:</p> <ul style="list-style-type: none"> • Identiv @MAXX ID-1 • Identiv SCR3500 • Identiv SCL3711
Supported readers with fingerprint sensors	<ul style="list-style-type: none"> • ACS AET52 / AET63 / AET65 • Omnikey 7121 Biometric • Futronic FS 82 • All finger print readers supported by Neurotechnology
Supported biometrics	Biometric Match-on-Card for Java Card with Neurotechnology™
Cache configuration options	<ul style="list-style-type: none"> • via KeyUsage • via time limit • via process (white/black listing) <p>Options can be combined for highly selective configuration</p>
Supported platforms	<p>Microsoft:</p> <ul style="list-style-type: none"> • Windows 10, 11 • Windows Server 2016, 2019, 2022 <p>Linux:</p> <ul style="list-style-type: none"> • RHEL 8, 9 • Ubuntu 24.04 • SLED/SLES 15 <p>macOS:</p> <ul style="list-style-type: none"> • Ventura (13.7.2) • Sonoma (14.7.2) • Sequoia (15)

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



Eviden Digital Identity
 cv cryptovision GmbH
 Munscheidstr. 14
 D 45886 Gelsenkirchen
 T: +49 209 16724-50
 F: +49 209 16724-61

www.cryptovision.com