sc/interface

Powerful and Secure Smart Credential 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, virtual smart cards, security tokens of several different form factors, and all major desktop operating systems.

Functions	• Increasing the level of security with smart cards or tokens
	• Comfortable functionality for managing the lifecycle of PINs, keys and certificates
	• PIN management:
	  • 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
	• Initialization & rollout functions:
	  • 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:
	  • 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	• 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 processes • Citrix, VMware, Microsoft fat- and thin clients (IGEL, eLUX) support • Password Authenticated Connection Establishment (PACE) • eIDAS-compliant „Siegel“ tokens • Biometry (sc/interface biometric) • PIV support (PIV edition) • Advanced signature profile • Elliptic Curve Cryptography (ECC) • Localization support via language files • User-friendly and convenient operation • Encrypted session PIN support via Minidriver and PKCS#15-PACE profile • Secure PIN pad support • Secure messaging • 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	• **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** • **Crypto Token Driver** for macOS • **sc/interface utility** for simple administration tasks • **sc/interface manager** for smart card initialization, personalization and management • **Register Tool** for certificate registration in Windows Certificate Store for all supported smart cards and USB tokens (sc/interface register tool) • **Plug-Ins** for validity warning and root certificate registration
Supported Standards	• 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 as defined in BSI TR-03110 • ISO/IEC 19794-2

Supported Smart Cards and Tokens	• AET: AET profile • ATOS CardOS: M4.01A / V4.2 / V4.2B / V4.2C / V4.3 / V4.3B / V4.4 / V5.0 / V5.3 • 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 • Bundesdruckerei: GoID card V1 / V2 • D-Trust: D-Trust Card 3.1 / 3.2 / 3.4 (Siegel card) • 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 • Gemalto: TOP IM GX4, IDClassic 340 • G&D: Sm@rtCafé Expert 3.1 / 3.2 / 4.0 / 5.0 / 6.0 / 7.0 • 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) / SLJ52 (Trusted Logic) • 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 / 3.0 • Siemens: CardOS M4.01a / V4.3B / V4.4 • SwissSign: suisseID (CardOS M4.3B / M4.4) • TCOS: Signature Card 1.0 / 2.0 • TU Dortmund: UniCard (SECCOS) • Volkswagen: PKI Card (CardOS M4.3B /4.4)
Add-ons	• sc/interface biometric: match-on-card fingerprint authentication • sc/interface cache: secure PIN caching • sc/interface PIV: supports FIPS201-2 PIV NIST standard • PKCS#11 module for iOS

Supported Readers	• All PCSC 2.0 compliant readers (macOS, Unix/Linux needs „pcsc-lite“), recommended:
	  • Identiv CLOUD 2700 F (not for macOS)
	  • Identiv CLOUD 4700 F
	  • Cherry SmartTerminal ST-2000 (Class2)
	  • REINER SCT cyberJack® RFID standard
	  • REINER SCT cyberJack® wave
	• Mobile Readers
	  • Identiv @MAXX ID-1
	  • Identiv SCR3500
	  • Identiv SCL3711

Supported Readers with Fingerprint Sensors	• ACS AET52 / AET63 / AET65 • Omnikey 7121 Biometric • Precise Biometrics 250 MC • Precise Sense™ MC / MC-S • Precise Biometrics Tactivo™ for iPhone / iPad
Supported Biometry	sc/interface supports the Neurotechnology fingerprint recognition solution. The Neurotechnology Biometric Credential Provider and the cryptovision biometric extension for sc/interface need to be installed.
Supported Platforms	Microsoft: • Windows 7 SP1, 8.1, 10 • Windows Server 2008 SP2 / R2 SP1, 2012 R2, 2016 Linux: • RHEL 6, 7 • Ubuntu 16.04 LTS / 18.04 LTS • SLES 15 macOS: • El Capitan (10.11.1) • Sierra (10.12) • High Sierra (10.13)

Supported Applications	• Fully compatible with Microsoft Identity Manager (MIM) • Compatible with several Smart Card Management Systems (e.g. IDnomic OpenTrust CMS, Nexus Prime, Versasec, Intercede, Noreg) • Smart card login to a Micro Focus eDirectory • Smart card login to Linux • Smart card login to macOS • 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 7, XenDesktop 5.x and XenApp 6.x • Smart card login to Lotus Notes • SAP Secure Login Client • Digital signature and encryption via smart card for e-mails (Mozilla Thunderbird, Outlook, Notes, Secude Secure Mail) • Kobil mIDentity • Qualified signatures with SuisseID, SwissSigner, D-TRUST card, D-TRUST multicard, TCOS. • 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) • MS Office 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
System Requirements	• A supported operating system • A supported card reader with installed driver • A free USB or microSD slot for card reader • A supported security token or MS VSC on TPM 1.2 / 2.0 • Additional application-specific requirements may occur

cv cryptovision GmbH | T: +49 (0) 209.167-24 50 | F: +49 (0) 209.167-24 61 | info(at)cryptovision.com

81029062