vSEC:CMS - Smart Card Management Software Evaluation Kit

**Brand:** Versasec  
**Product Code:** SMAV100DEM  
**Weight:** 0.30kg  
**Dimensions:** 0.00cm x 0.00cm x 0.00cm  

**Price:** €300.00  
Ex Tax: €300.00

**Short Description**  
**The vSEC:CMS Try 'n' Buy package**  

The vSEC:CMS S-Series is fully functional with minidriver enabled smart cards and it streamlines all aspects of a smart card management system by connecting to enterprise directories, certificate authorities, physical access control systems, email servers, log servers, biometric fingerprint readers, PIN mailers... the list goes on. With vSEC:CMS organizations can issue smart cards to employees, personalize the smart card with authentication credentials and manage the lifecycle of the smart card - directly from the off-the-shelf product.

**Description**  
**The vSEC:CMS Try 'n' Buy package** is for the evaluation of the software.

**The Kit contains:**  

2 x Minidriver/PKI enabled Smart Cards  
1 x USB Smart Card Reader
1 x Minidriver Key, USB Token incl PKI/Minidriver enabled 2FF Smart Card

1 x Operator Token

1 x Support and Maintence for PoC

Specifications:

Operating Systems:

- Client/Operator/User Self-service:

Server:


Smart Cards:

- Gemalto .NET, .NET BIO, IDPrime PIV & MD

- Raak Technologies C2

- Morpho ypsID S2/S3

- Athena CNS & IDProtect

- Safenet eToken PRO

- ACS ACOS5-64 & Cryptomate64

- Oberthur Authentic, IAS ECC & PIV, PIV 8.1

- Feitian ePass2003 Token
- Avtor CryptoCard337

- HID C200, C1150

- Taglio C2, PIVKey

- T-Systems TCOS

- Yubico YubiKey PIV

- SafeTrust-PIV on Placard

- Virtual smart cards (MS, vSEC & Charismatics)

- Mifare DESFIRE EV1

- Java Card with Cryptovision eID Applet v2.8

- Java Card with Open FIPS 201 Applet v2.8

- MS Minidriver enabled cards

**Card Features:**

- Printer support for graphical personalization
- PIN mailers (both email and regular mail)
- Contactless RFID interface
- Batch processing
- Card stock management
Compatibility:

- User directory: MS Active Directory, IBM-LDAP, OpenLDAP and LDAP v2/v3
- Card DB: SQL comp or local file
- Certificate Authority: MS CA, Entrust, Symantec MPKI, EJBCA, neXus PKI, Opentrust PKI and Verizon UniCERT CA, DigiCert CA
- HSM: Gemalto SafeNet Luna, Utimaco HSM and Engage BlackVault
- Card Printers: Fargo HDP5000, Datacard SR300, Magicard Prima 4 and Evolis Primacy
- Migration path to and from MS FIM/CLM
- Upgrade path from vSEC:CMS K and T-Series
- Upgrade path from Gemalto IDAdmin 100/DAS vSEC:CMS Plugin API, Scripting, WebStart

Security Features:

- Secure key storage
- Secure backup and synchronization of databases
- Disaster recovery for stolen/lost tokens
- Encrypted audit log
- Granular access control
- Approval work flows
- Connects logical and physical access control
- Key archival and key restore processes
- Fingerprint template management
- Failover clustering for high availability

Performance:

- The system is tested and is functional with 300 000 registered user smart cards and 100 parallel operators interacting with the system
- Load balancing for high scalability

Version 5.5 of vSEC:CMS S-Series is now available. The new version includes a long list of smart new features. The new features will help smart card administrators better manage user smart cards.

vSEC:CMS 5.5 adds support for the following:
- Fingerprint enrollment using Oberthur PIV 8.1 smart cards
- Gemalto IDPrime MD 3940 smart cards
- Gemalto PIV 3.0 smart cards
- Identiv uTrust MD smart cards
- R-END/R-MAC in the GlobalPlatform secure messaging for Oberthur PIV 8.1 (2.4.1-SPE)
- PUC-based challenge/response PIN unblock for all vSEC:CMS supported PIV smart cards

**New features** within vSEC:CMS include the following:

- Subscription-based licensing
- Ability to export certificate data when performing life cycle / certificate operations.
- Option to server-side import PKCS#12/PFX files for smart card issuance
- HSM protected GlobalPlatform keys for Oberthur PIV 8.1 cards
- Smart card delete function is added to the SOAP API
- New configuration option to set if Operator Console shall do certificate requests to Microsoft CA directly or via vSEC:CMS server (proxy)
- Added functionality to allow for the reconfiguration of MS SQL connection when the local internal database is empty
- Ability to rebuild local cached database from MS SQL
- Versasec-Activator SO Session: Once a System Owner card has been used to authenticate, the System Owner PIN is not asked for again for 10 minutes, enabling issuance of multiple operator cards
- A feature has been added to allow manual creation of System Owner cards
- Manual deletion of operator accounts
- The error returned on life cycle card issuance is now configurable
- Ability to store only overview data for RSDM device info

**Scalability**

The vSEC:CMS S-Series scales with your project. With the new load balancing capability, there is no upper limit!