vSEC:CMS S-Series

Advanced smart card management made easy. Versasec's vSEC:CMS S-Series introduces a new approach to lifecycle management of physical and virtual smart cards. Now, enterprises can implement an advanced and feature-rich smart card management system offering a variety of important benefits:

- *Fast implementation that takes minutes, rather than weeks or months*
- *Intuitive user interface that improves operational efficiency*
- *No hidden costs and low total cost of ownership*
- *Consistently high security level without exception*
- *Large scale capabilities, available from day one*

Smart Card Management

Smart cards are secure devices that are used for many purposes, with perhaps the most important being as combined identification badges for enterprises. With all professional smart card use, the cards must be managed across the entirety of the smart card lifecycle. At the base level, personalization tasks include setting PIN codes, setting policies, loading certificates, provisioning and setting management keys. At the management level, tasks include unblocking PIN codes, setting new PIN codes, and renewing and issuing new certificates. Revocation typically ends the smart card lifecycle, but it is also the point when the card can be personalized again. All of these tasks and many more are handled by the vSEC:CMS smart card management system.
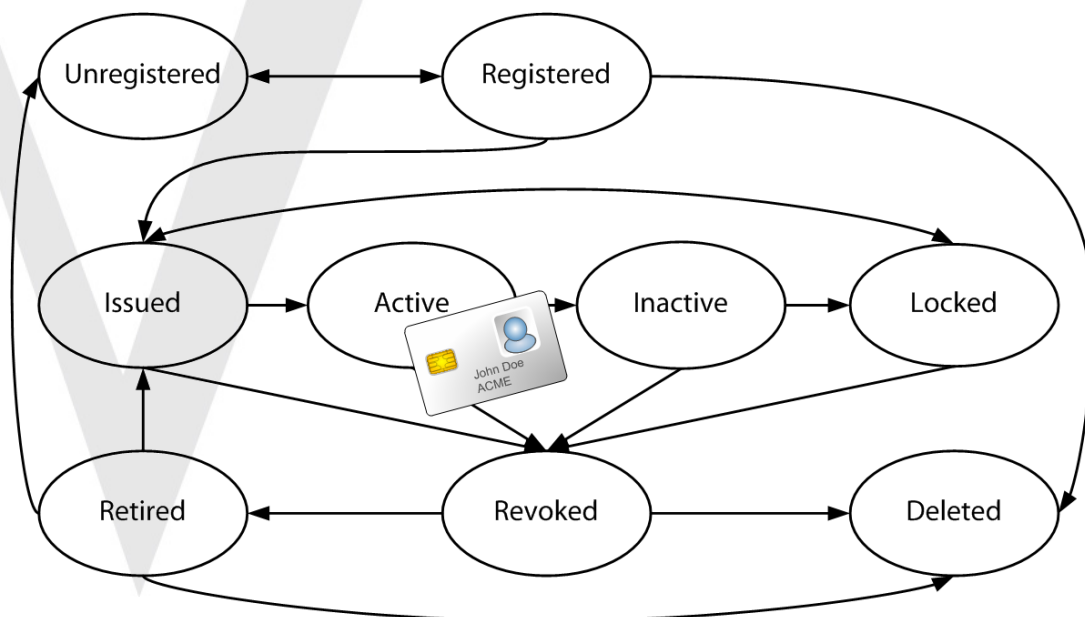

Figure 1: vSEC:CMS S-Series Graphical Interface

Smart Card Lifecycle

All smart card operations within vSEC:CMS focus on the smart card lifecycle. We use a state diagram to graphically visualize the lifecycle; the diagram clearly shows the operator each card, its location in the lifecycle and available actions/processes from this state. The same diagram is also used by the administrator when configuring the processes.

Figure 2: Connections

Fast Installation, High Security, No Dedicated Servers, Low TCO

The vSEC:CMS S-Series is an innovative, easily integrated and cost-effective smart card management system that helps organizations deploy and manage smart cards quickly and efficiently. The vSEC:CMS S-Series is client-server based. It streamlines all aspects of smartcard management by easily connecting to enterprise directories, certificate authorities, smart card printers, external databases, physical access control systems, and more. The S-Series is designed for several operators and users working in parallel without a need for synchronization; each operator requires access to the operator application and the operator's operator smart card only.

Technical Specifications

Operating Systems
Client/Operator/User Self-service:
- MS Windows 7, 8, 10, 2008, 2012, 2016

Server:
- MS Windows 2008, 2012, 2016

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
- Longmai mToken CryptoID
- 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 ePKI Applet
- Java Card with Open FIPS 201 Applet
- 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: GlobalSign PKI, MS CA, Entrust, Symantec MPKI, EJBCA, neXus PKI, Opentrust PKI, Verizon UniCERT CA, DigiCert CA
- HSM: Gemalto SafeNet Luna & ProtectServer, Thales nShield, 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
- Tested with 300 000 registered user smart cards and 100 operators interacting with the system
- Load balancing for high scalability