vSEC:CMS S-Series

Advanced credential 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 credential 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*

Credential Management

Credentials such as 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 credential use, the cards must be managed across the entirety of the credential 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 credential lifecycle, but it is also the point when the credential can be personalized again. All of these tasks and many more are handled by the vSEC:CMS credential management system.

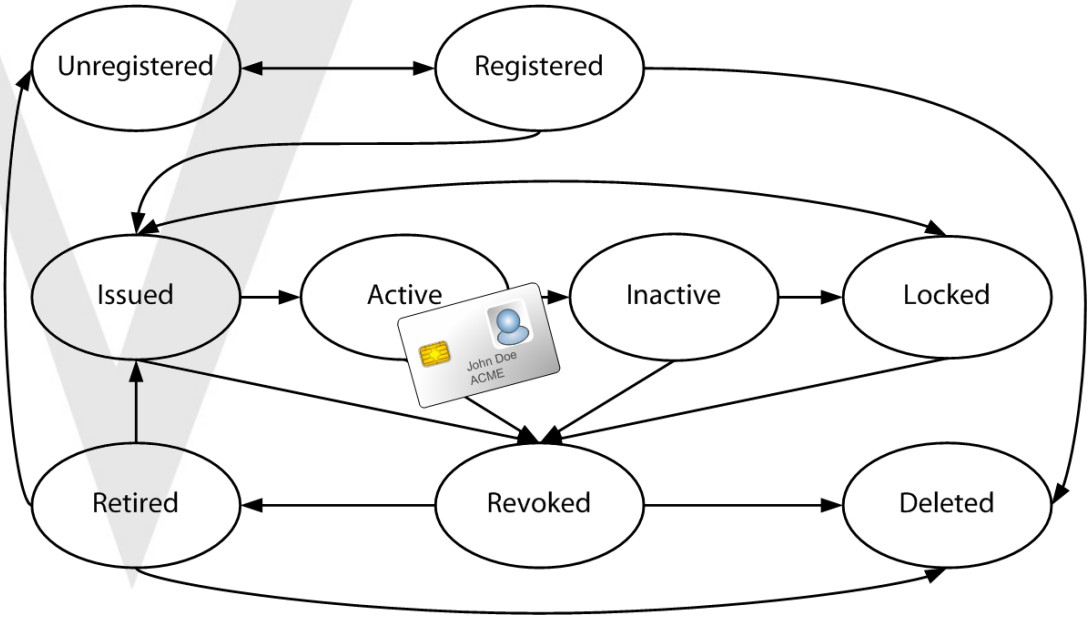

Figure 1: vSEC:CMS S-Series Graphical Interface

Credential Lifecycle

All credential operations within vSEC:CMS focus on the credential lifecycle. We use a state diagram to graphically visualize the lifecycle; the diagram clearly shows the operator each credential, it type, 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.

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

The vSEC:CMS S-Series is an innovative, easily integrated and cost-effective credential management system that helps organizations deploy and manage credentials 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.

Figure 2: Connections

Technical Specifications

Operating Systems

Client/Operator/User Self-service:

- MS Windows 7, 8, 10, 2008, 2012, 2016

Server:

- MS Windows 2008, 2012, 2016

Credentials Supported

- ACS CryptoMate64
- Athena CNS/IDProtect
- Avtor CryptoCard 337
- CardOS 4.4/5.3
- Cryptovision ePKI Applet
- Feitian ePass2003 Token
- Gemalto IDPrime MD, PIV, .NET
- Gemalto Safenet eToken
- HID C200/C1150
- Identiv uTrust MD
- Longmai mToken CryptoID
- Microsoft minidriver enabled devices
- Mifare DESFIRE EV1
- Morpho ypsID S2/S3
- Oberthur Authentic/IAS ECC/PIV 8.1
- Open FIPS 201 Applet
- SafeTrust-PIV on Placard
- Taglio C2/PIVKey
- TCOS TeleSec IDKey
- Virtual Smart Cards
- Yubico YubiKey 5/4/NEO

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, Evolis Primacy & Matica 8300
- Upgrade path from vSEC:CMS K/T-Series, Gemalto DAS and Microsoft FIM/MIM CM
- APIs: Plugin, SOAP, COM, SQL, Script, 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