



vSEC:CMS T-Series

Advanced smart card management made easy. vSEC:CMS T-Series brings a totally new approach to smart card lifecycle management. It is an advanced and feature-rich smart card management system offering important benefits:

- *Implementation takes minutes, rather than months*
- *Requires no dedicated hardware or servers*
- *Provides an intuitive user interface that improves operational efficiency*
- *Offers a low total cost of ownership with no hidden costs*
- *Delivers consistently high security level, without exception*

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.

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

vSEC:CMS is an innovative, easily integrated and cost effective smart card management system that makes it easy to deploy and manage smart cards within the enterprise. The T-Series is delivered pre-installed on a secure USB token with the application; configuration settings and credentials residing securely on the USB token, thereby removing the requirement to invest in expensive server hardware. vSEC:CMS streamlines all aspects of smartcard management by connecting to enterprise directories, certificate authorities, physical access control systems, and more.



Figure 1: Smart card management Plug and Play

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.

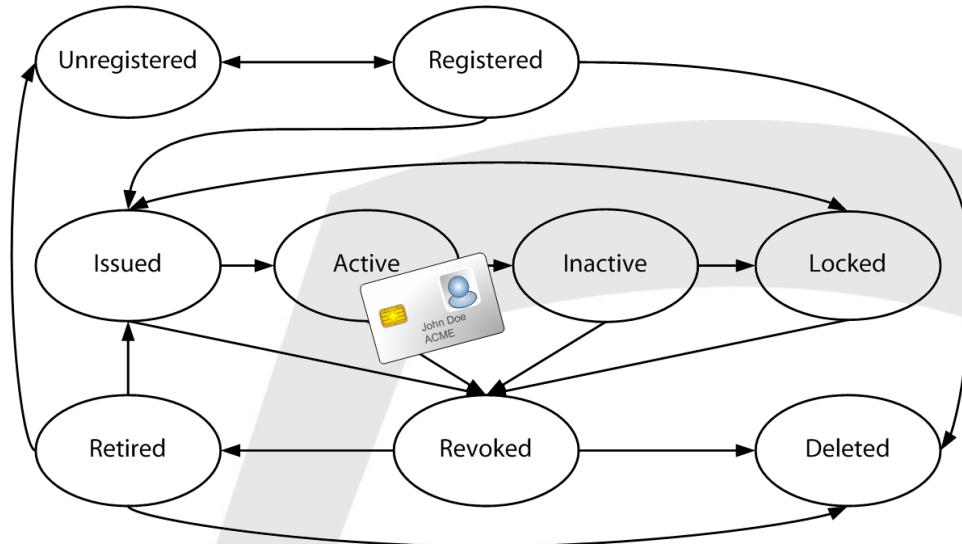


Figure 2: Smart Card Lifecycle

Technical Specifications

Operating Systems (Operator)

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

Smart Cards

- Gemalto .NET, .NET BIO, IDPrime PIV & MD
- Raak Technologies C2
- Morpho ypsID S2
- Athena CNS & IDProtect
- Safenet eToken PRO
- ACS ACOS5-64 & Cryptomate64
- Oberthur Authentic, IAS ECC & PIV
- Feitian ePass2003 Token
- Avtor CryptoCard337
- HID C200, C1150
- Taglio C2, PIVKey
- MS Win8+ Virtual smart cards
- Mifare DESFIRE EV1
- MS Minidriver enabled cards

Smart Card Readers

- PC/SC reader
- Contactless

Compatibility

- User directory: MS AD and LDAP v2/v3
- Certificate Authority: MS CA
- MS event handler
- Migration path to and from MS FIM/CLM
- Upgrade path from vSEC:CMS K-Series
- Upgrade path from Gemalto IDAdmin 100/DAS

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
- Support for fingerprint template management