

ActivID® Credential Management System



ACTIVID CREDENTIAL MANAGEMENT SYSTEM BENEFITS

- Increase security and reduce fraud with a single platform capable of issuing and managing HID Global devices and credentials
- Better user experience on mobile environments (tablets and mobile phones): strong security without the need to carry a smart card or card reader
- Unique, patented post-issuance update capabilities that allow organizations to extend the lifetime of authentication devices, offering substantial cost-savings and productivity enhancements
- Proven technology that numerous security-minded organizations have leveraged to issue hundreds of millions of credentials
- Compliance with stringent U.S. Federal government Personal Identity Verification (PIV) standards including derived PIV credentials
- Easy integration with a wide variety of operating systems, directories, front or backend identity management and provisioning systems, certificate authorities, and physical access control systems

PROVEN CREDENTIAL MANAGEMENT SYSTEM TO SECURELY DEPLOY AND UPDATE HIGH ASSURANCE USER CREDENTIALS

HID Global's ActivID® Credential Management System (CMS) provides organizations comprehensive, highly configurable solutions to meet their unique needs. With HID Global, organizations can establish trust in the identity of users to securely manage access to all their networks, PCs, in-house, public and private cloud applications, building facilities, and other resources.

Organizations evolving towards industry standard (X.509) digital certificate-based smart cards or smart USB tokens can trust the HID Global portfolio to support their changing requirements. HID Global delivers the technology expertise organizations need, from the readers, smart cards and card printers to the authentication software and PACS integration to conveniently and cost-effectively deploy a complete smart ID card solution for both physical and IT access.

The ActivID CMS enables organizations to easily replace traditional user names and passwords with digital identities. Organizations can quickly and securely issue and manage smart cards and smart USB tokens containing a variety of credentials, including public key infrastructure (PKI) certificates, one-time passwords (OTPs), biometrics and demographic data. The ActivID CMS also enables organizations to deploy software digital certificates on Windows and mobile devices, to provide flexible form factor and assurance level deployment options. Organizations can also securely

manage a large number of end users, in heterogeneous, dispersed locations, and update their credentials at any point in their life cycle.

The ActivID CMS includes the following features and capabilities:

- Customizable workflows and policies that readily adapt to a variety of environments and deployment scenarios
- Tamper-evident audit features that log all event activities for reporting
- Extensibility to support batch and service bureau issuance models
- Unique, patented post-issuance update capabilities
- Web-based self service
- Web-based help desk administration
- Extensible plug-in capability, which allows organizations to extend and customize the product feature set
- Integration with physical access control systems to seamlessly manage credentials for physical and logical access



The ActivID® CMS consists of HID Global's ActivID Credential Management System (CMS), as well as an add-on module -- HID Global's ActivID® Batch Management System (BMS), which is bundled into the Advanced Edition of ActivID CMS.

ActivID CMS

ActivID CMS provides a comprehensive, flexible and highly configurable solution to manage the issuance and administration requirements of successful smart chip deployments. With ActivID CMS, organizations can manage their authentication devices, data, applets and digital credentials (including PKI certificates) through their entire lifecycle. They can also update user access in real-time, without additional costs or resources.

Together with the ActivID ActivClient® security software, ActivID strong authentication platform, and ActivID authentication device offerings, the HID Global portfolio offers a complete credential lifecycle management solution.

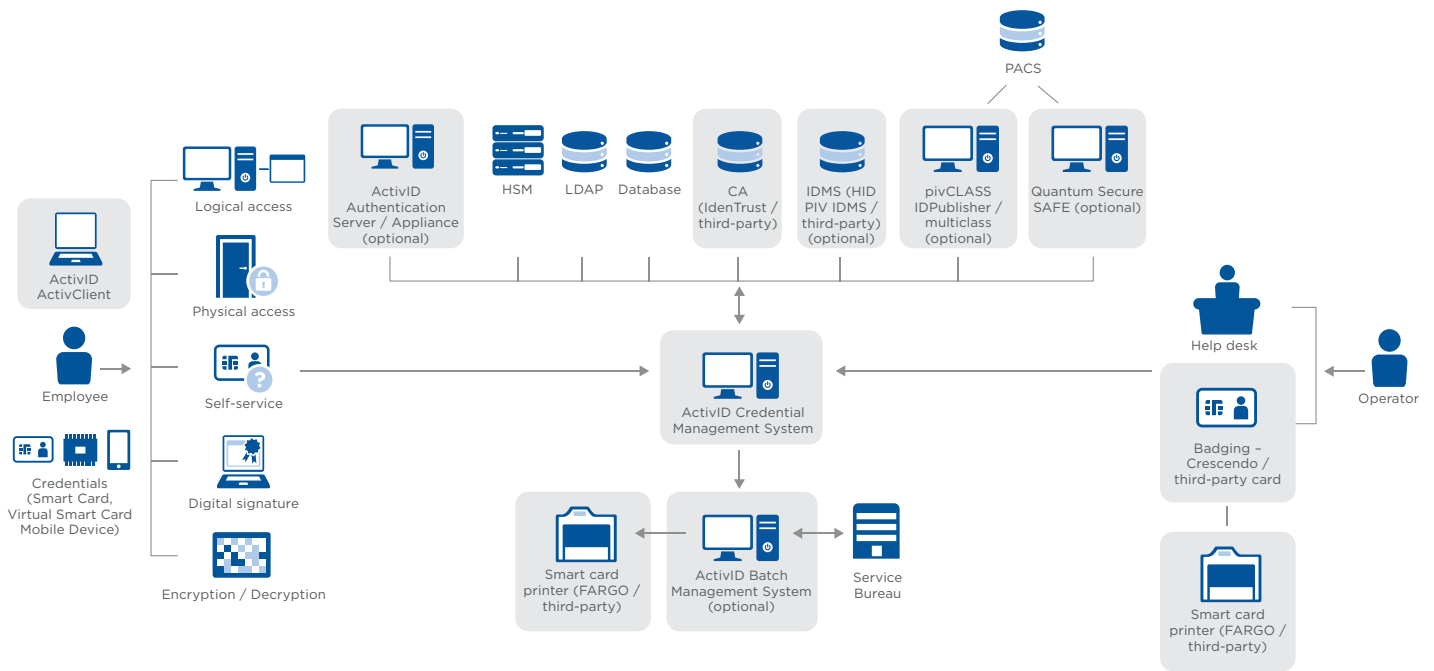
When ActivID CMS is deployed with ActivClient security software, organizations can use smart cards for both strong authentication to the corporate network and physical access to corporate facilities. For example, organizations can use HID Global's Crescendo® smart cards, which are a series of highly secure multi-technology smart cards built to provide standards-compliant support for existing access control and strong authentication applications.

Additionally, United States Government agencies and contractors can leverage ActivID CMS to issue and manage Personal Identity Verification (PIV) cards and PIV-Interoperable (PIV-I) cards in compliance with FIPS 201. ActivID CMS makes it easy for enterprise customers to issue Commercial Identity Verification (CIV) compliant smart cards that follow the same standard but for the commercial market. Once issued, CIV cards are compatible with a large number of systems and applications compatible with the PIV standard.

In addition to issuing and managing smart cards and USB tokens, ActivID CMS also manages virtual smart cards and software credentials, better suited for mobile computing devices such as tablets and smart phones. Users then have access to strong authentication, digital signature and encryption services on all their computing devices: desktop, laptop, tablet and phone. ActivID CMS offers simple and central management of multiple credential types in an heterogeneous environment.

The ActivID CMS also includes a software development kit for systems integrators and independent software vendors.

Combined with HID Global Crescendo smart cards, OMNIKEY® smart card readers, FARGO® card printers, Asure ID® card personalization software and pivCLASS® software solution for PACS in PIV environments, HID is the only vendor offering a complete solution to create, manage and use PKI smart cards for both IT resource and physical access.



HID Global ActivID BMS

ActivID BMS extends the functionality of the ActivID CMS to enable organizations to communicate securely with service bureaus for personalization and encoding of their employee smart cards. At the same time, the ActivID BMS communicates with the ActivID CMS to enable secure post-issuance activation and life cycle management of the smart cards after production is completed.

ActivID BMS provides a lower cost, standard-based solution for batch requests and also offers the flexibility of a local issuance model by allowing card issuers to produce cards using their own printers.

Why HID Global Identity Management Solutions?

HID Global has a proven history of helping enterprise, government and financial service organizations meet their information security and compliance requirements. That's why more than 2,500 of the most security conscious businesses and organizations around the globe trust HID Global for their secure identity needs. HID Global is committed to continually enhancing customer value through identity and access management solutions that drive down costs, are easy to use and increase end user and administrative convenience.

ACTIVID CREDENTIAL MANAGEMENT SYSTEM THIRD-PARTY INTEROPERABILITY

ActivID Credential Management System is interoperable with many third-party systems including those from:

- Apple®
- Entrust
- Gemalto®
- IBM®
- IdenTrust™
- IDnomic™
- Lenel®
- Microsoft®
- NetIQ®
- Oracle®
- Safenet® Assured Technologies
- Symantec®
- Thales®
- Red Hat®
- Verizon® Business

	ActivID® Credential Management System	ActivID Batch Management System
Server Platform Support	Operating Systems: Microsoft® Windows® Server 2012 / 2012 R2 / 2016	Operating Systems: Microsoft Windows Server 2012 / 2012 R2
	Databases: Microsoft SQL Server 2012 SP1 / 2014 / 2016, Oracle® 11g / 12c	Databases: Oracle® 11g R2 and 12c
Client Platform Support	Operating Systems: Windows 7 / 8.1 Update / 10, Windows Server 2012 / 2012 R2 / 2016 (32- and 64-bit)	Operating Systems: Windows 7 and 8.1 Update 1
	Browsers: Internet Explorer 11	Browsers: Internet Explorer 6.0 and higher
Main Feature Set	Administrative Services: Issuance, device life cycle management, PIN management, certificate management, One-Time Password (OTP) management, user management, configuration	Administrative Services: Allocation of batch orders, information exchange with ActivID Credential Management System, generation and encryption of data exchange with service bureau, synchronization of smart card status, local batch issuance
	End User Services: Issuance, device life cycle management, PIN management, OTP management, authentication, post-issuance	
Credentials	Smart cards and USB tokens: Java Card-based devices from vendors such as Atmel®, Gemalto™, Giesecke & Devrient, HID Global and Oberthur Technologies; PKCS#11 devices that comply with ActivID Credential Management System requirements	
	Smart Card Readers: PC / SC compliant readers	
	Virtual Smart Cards: compliant with Microsoft Windows 10, Trusted Platform Modules (TPM) 2.0	
	Mobile credentials: Apple iOS	
Additional Devices	Biometric Service Providers: Precise Biometrics and Secugen	
	Datacard® printers (using Datacard ID Works) and FARGO® printers (using HID Asure ID® Developers Edition)	Smart Card Printers: Datacard printers (using Datacard ID Works) and FARGO printers (using HID Asure ID)
	Hardware Security Modules: AEP KeyPer® Enterprise / Plus, Gemalto SafeNet Network HSM / PCIe HSM, SafeNet Assured Technologies Luna SA for Government, Thales nShield™ Connect / Connect+ / Solo / Solo+	Hardware Security Modules: Gemalto SafeNet Network HSM / PCIe HSM, Thales nShield Connect / Connect + / Solo / Solo+
Compliance and Standards	U.S. Government: FIPS 201-2 (PIV cards – NIST SP 800-73-4, derived PIV credentials – NIST SP 800-157), Smart Card Interoperability Specifications GSC-IS v2.0, GSA Basic Services Interface (BSI), GSC-IS v2.1, Section 508-compliant, U.S. Department of Defense Pre-Issuance Requirements v4.2.1, FIPS 140-2 certified cards and applications support, FIPS 140-2 certified HSM support	
	Data Access: LDAP v3, JDBC	
	General: Secure communication (SSL/TLS), GlobalPlatform / OpenPlatform, Java Card™	
Third-party Interoperability	Directories: Atos DirX® Directory, IBM® Tivoli® Directory Server, Microsoft Active Directory, Microsoft Active Directory Lightweight Directory Services, NetIQ eDirectory, Oracle Directory Server, Red Hat Directory Server	
	Certificate Authorities: Entrust® Authority Security Manager™, IdentTrust®, Microsoft Windows Certificate Authority, OpenTrust by IDnomic, Symantec® Managed PKI, Verizon® UniCERT®	
	Service Bureaus: Oberthur Card Systems; any services bureau supporting the U.S. Department of Defense Pre-Issuance Requirements v4.2.	
Compatibility with other HID Global Software Products	HID PIV IDMS, ActivID ActivClient, ActivID AAA Server for Remote Access, ActivID Appliance, pivCLASS® IDPublisher, pivCLASS MultiCLASS, Quantum Secure SAFE™	