ActivID® ActivClient®

Advanced security client protects workstations and networks with smart cards and security keys

HID's ActivID® ActivClient® ensures strong authentication of employees, contractors and suppliers when they access enterprise resources, helping IT managers, security professionals and auditors to manage the risk of unauthorized access to workstations and networks by enabling the deployment of Zero Trust security framework.

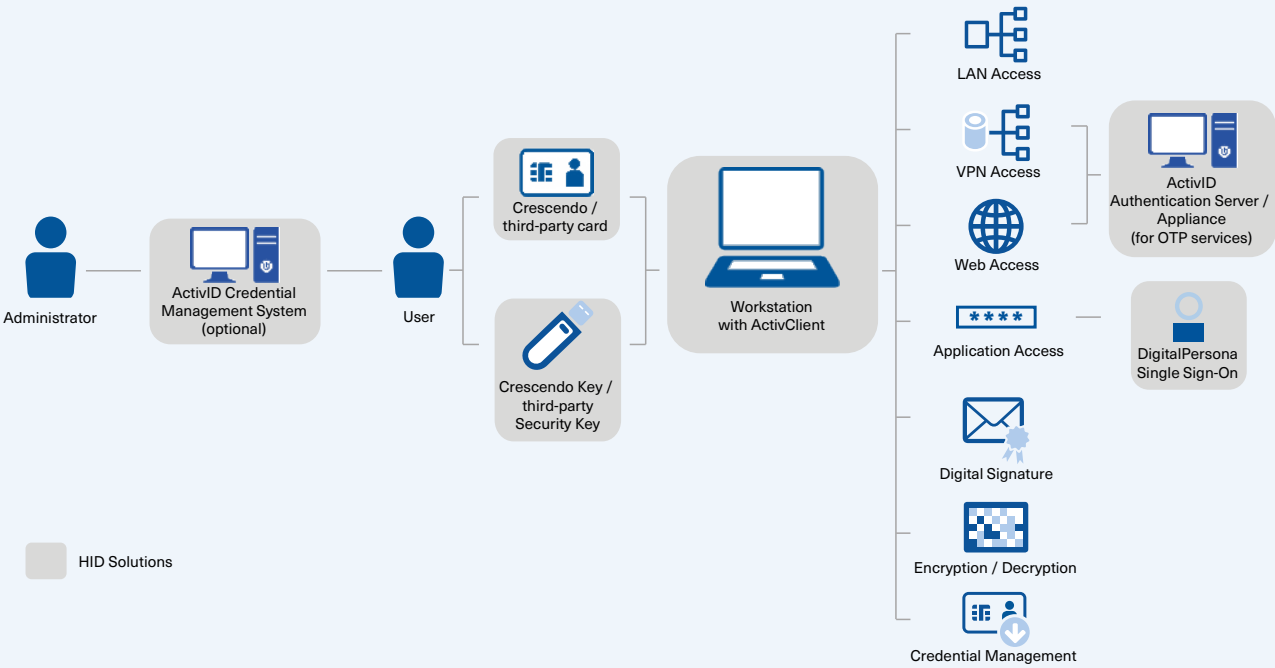
As a market-leading middleware for smart cards and security keys, ActivID ActivClient consolidates identity credentials (private keys for public key infrastructure [PKI] certificates and symmetric keys for one-time password [OTP] generation) on a single, secure, portable device. This capability, combined with support for a wide range of desktop and network applications, enables organizations to use strong authentication, encryption and digital signatures to protect high value resources and interactions.

ACTIVCLIENT OFFERS:

- Interoperability with a wide range of remote access solutions, thin clients, applications (e.g., Microsoft® Outlook®, Adobe Acrobat® and popular web browsers), smart cards, smart card readers and security keys
- Compatibility with major certificate authorities and encryption utilities
- Simple automated deployment, updates and diagnostics
- An open, standards-based architecture, which is easily extensible using the companion software development kit
- Support for standard U.S. Government- issued Common Access Cards and Federal Information Processing Standards (FIPS) 201- certified Personal Identity Verification certified (PIV) cards

AT-A-GLANCE ACTIVCLIENT BENEFITS:

- Increases security with proven technology that is widely adopted because of its user-friendly, familiar, ATM-like authentication experience
- Optimizes productivity with a single, versatile strong authentication tool for both Windows Login and Remote Access (e.g., PIN-protected PKI certificates or OTPs for VPN)
- Improves compliance with government and industry regulations
- Reduces costs with easy integration into an existing enterprise infrastructure
- Enforces corporate policies and security best practices for workstations and network access
- Reduces the risk of phishing with email digital signature
- Protect corporate data with encryption capabilities
- Scales to millions of endpoint devices
- Provides flexibility with an option of a stand-alone mode and an initialization tool



INCREASED SECURITY

ActivID® ActivClient® allows organizations to protect Windows® workstations and internal networks from unauthorized access. Using ActivID ActivClient, IT managers can easily enforce strong authentication policies when users login to their Windows desktop or access the organization's network using a virtual private network (VPN) or remote desktop session.

ActivID ActivClient can be deployed with ActivID AAA Server for Remote Access or ActivID Appliance for OTP validation. This enables organizations to authenticate to legacy authentication systems that are not PKI-enabled yet—using the same smart card.

ActivClient includes a Windows compliant smart card mini-driver and a PKCS #11 compliant library, enabling email and document digital signature and encryption services with a large number of applications.

When using the HID DigitalPersona single sign-on solution, use ActivClient to add digital certificates as an additional DigitalPersona authentication factor for increased security.

These security services help organizations improve compliance with government regulations (e.g., Sarbanes-Oxley Act Section 302: Internal Controls) and industry standards (e.g., PCI DSS Section 8).

LOWER SMART CARD & SMART USB KEY DEPLOYMENT COSTS

ActivID ActivClient can easily be deployed and managed via standard software such as Microsoft Active Directory and Microsoft Group Policy Objects, reducing the cost of smart card deployment.

ActivClient makes PKI easy for end users. For example, Microsoft Outlook is automatically configured for secure email with smart card certificates, and the Exchange Global Address List (GAL) is automatically updated with the same certificates. These capabilities provide increased security to end users, without the burden of learning new software capabilities. This significantly reduces help desk costs and other administrative costs normally associated with endpoint security.

FLEXIBLE DEPLOYMENT MODELS

ActivID® Credential Management System (CMS) enables organizations to securely issue and manage digital credentials on devices. When deployed with ActivID CMS, ActivID ActivClient® offers a smart card auto-update service, enabling credentials to be centrally updated after card issuance, with minimal cardholder disruption.

For increased security in contactless mode, ActivClient encrypts the communication between the computer and the card, when the devices are issued with VCI (Virtual Contact interface) enabled, in compliance with the NIST SP 800-73 standard.

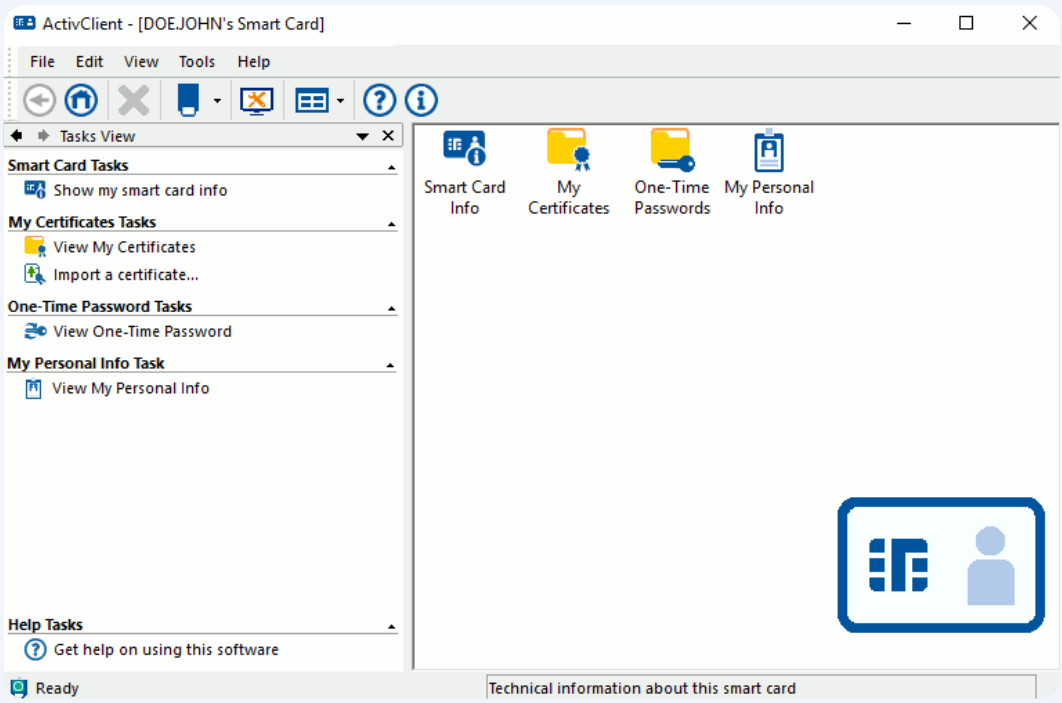
For customers without a Credential Management system, ActivID ActivClient offers a stand-alone mode, with an initialization tool for easy issuance and reset of smart cards and security keys.

SECURITY CLIENTS

ActivID ActivClient is the enterprise smart card middleware in the HID Credential Management portfolio. In addition to Windows®, it is available for Apple® OS X and Linux®-based platforms.

ActivID ActivClient comes with a Software Development Kit (SDK) that enables systems integrators and independent software vendors to link smart cards to their applications. Software developers do not need specific knowledge of smart card technology to integrate ActivID ActivClient services into their applications.

ACTIVCLIENT USER CONSOLE



	ActivID® ActivClient® 8.0 for Windows®	ActivID ActivClient 4.0.1 for Mac®	ActivID ActivClient 4.0 for Linux®
Government Standards	• NIST Special Publications 800-73-4 compliant • NIST Personal Identity Verification Program (NPIVP) certified • GSA FIPS 201 Approved Product • U.S. Government Smart Card Interoperability Specifications GSC-IS 2.1 • U.S. DoD Common Access Card Middleware Requirements v4.0 compliant • HID Applets – FIPS 140-2 Level 2 and Level 3 certified • FDCC / SCAP 1.1 compliant • Section 508 compliant		
Smart Card and Security Key Support	• All generations of the U.S. Department of Defense (DoD) Common Access Cards (CAC) • Personal Identity Verification (PIV), PIV-Interoperable (PIV-I) and Commercial Identity Verification (CIV) cards • HID Crescendo smart cards, Crescendo Security keys (NFC, USB-A, USB-C) • Select smart cards and security keys from Gemalto, Giesecke & Devrient, Idemia and Yubico		
System Requirements	Windows 10, Windows 11, Windows Server 2016, Windows Server 2019 (32- and 64-bit), Windows Server 2022	Mac OS 10.8, 10.9, 10.10 and 10.11	• Red Hat® Enterprise Linux 6.5 • CentOS 6.5, Debian 7.3, Ubuntu 12 (32- and 64-bit)
Technology (APIs)	Smart Card Mini Driver, PKCS#11, PIV and BSI	Apple® TokenD and PKCS #11	PKCS #11 and BSI
Security Services	• Windows Smart Card Login, Novell Login, Windows 802.1x Login • Secure VPN with Check Point®, Cisco®, Juniper®, Microsoft® and many other remote access solutions • Secure Web Login with Google Chrome, Microsoft Edge™, and Mozilla® Firefox® • Secure remote sessions with Citrix® XenApp and Windows Remote Desktop Services • Secure email (signature and encryption) with Microsoft Outlook®, Microsoft Exchange / Outlook Web App and Mozilla Thunderbird®. Automatic configuration of the Outlook security profile and publication of certificates to the Global Address List • Secure documents through digital signature with Adobe Acrobat and Microsoft Office • Secure files through Microsoft Encrypting File System (EFS), BitLocker	• Secure Web Login with Apple Safari® and Mozilla Firefox • Secure email (signature and encryption) with Apple Mail, Microsoft Outlook for Mac, and Mozilla Thunderbird.	Secure Web Login with Mozilla Firefox
Management Services	• User console for end-users to view and manage their smart card and credentials • Smart card presence and activity icon in the Windows notification area • Change PIN / unlock card • Initialize / reset card • Digital Certificates: Certificate viewer, import / export user and CA certificates • Generate OTP in synchronous or challenge / response mode, resynchronize event counter • View personal information for US DoD Common Access Cards and PIV cards • Automatic and secure card update, post issuance, via ActivID Credential Management System • Advanced Diagnostics utilities • MSI-based installer compatible with Microsoft Active Directory and many other software deployment solutions • Policy management via administrative templates, compatible with Windows Group Policies	Initialize card, generate and load key pairs, change PIN, unlock card – using PKCS #11	Initialize card, generate and load key pairs, change PIN, unlock card – using PKCS #11

HID
hidglobal.com

North America: +1 512 776 9000 | Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +353 91 506 900
Asia Pacific: +852 3160 9800 | Latin America: +52 55 9171 1108
For more global phone numbers click here

2023-10-09-iams-activid-activclient-security-software-ds-en PLT-01263
Part of ASSA ABLOY