IDENTITY ASSURANCE SOLUTIONS

ActivClient

ADVANCED SECURITY CLIENT PROTECTS WORKSTATIONS AND NETWORKS WITH SMART CARDS AND USB TOKENS

The insider threat to enterprise information assets is rising in the wake of increased layoffs, consolidation and a weak economy. In this environment, the opportunity for insiders to exploit static passwords for business disruption or personal gain is high. HID Global’s ActivClient ensures strong authentication of employees, contractors and suppliers when they access enterprise resources to help IT managers, security professionals and auditors manage the risk of unauthorized access to workstations and networks.

As a market-leading middleware for smart cards and USB tokens, 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, network, and productivity applications, enables organizations to use strong authentication, encryption, and digital signatures to protect high-value resources and interactions.

ActivClient features include:

- 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 USB tokens
- Compatibility with major certificate authorities and encryption utilities
- Simple automated deployment, updates and diagnostics
- 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 (PIV) cards

AT-A-GLANCE: ACTIVCLIENT BENEFITS INCLUDE:

- Increases security with proven technology that is widely adopted because of its user-friendly, familiar ATM-like authentication experience
- Optimizes productivity with 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 existing enterprise infrastructure
- Enforces corporate policies and security best practices for workstations and network access
- Scales to tens of thousands of desktops using Windows management tools
- Provides flexibility, with an option of a standalone mode and an initialization tool

hidglobal.com
Increased Security

HID Global’s ActivClient allows organizations to protect Windows® workstations and internal networks from unauthorized access. Using 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.

ActivClient can be deployed with HID Global’s 4TRESS™ AAA Server for Remote Access or HID Global’s 4TRESS Authentication Appliance for OTP validation. This enables organizations to authenticate, using the same smart card, to legacy authentication systems that are not PKI-enabled yet.

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.

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 Deployment Costs

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 the end users. For example, Microsoft Outlook is automatically configured for secure email with the 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 the administrative costs normally associated with endpoint security.
4TRESS AUTHENTICATION

APPLIANCE BENEFITS:

- Broad range of authentication methods and devices based on open standards (e.g., OATH, EMV, and PKI)
- Comprehensive management tools providing complete life cycle management for user credentials, soft tokens, and devices
- Centralized and tamper-evident audit logs for tracking transactions across channels, improving security, and simplifying compliance
- Highly scalable deployment architecture that supports multiple application servers and platforms
- Extensible framework to easily add third-party authentication methods

Flexible Deployment Models

The ActivID™ Card Management System (CMS) is a reliable, proven, and extensible solution that enables organizations to securely issue and manage digital credentials on devices. For organizations that need secure PIN management and smart card issuance quickly and easily, HID Global's ActivID CMS Appliance provides a new level of ease of ownership and accelerated time-to-benefit. When deployed with these ActivID CMS products, ActivClient offers a smart card auto-update service, enabling credentials to be centrally updated after card issuance, with minimal cardholder disruption.

For customers without a card management system, ActivClient offers a standalone mode, with an initialization tool for easy issuance and reset of smart cards and USB tokens.

Security Clients

ActivClient is the enterprise smart card middleware in the HID Global Identity Assurance portfolio. In addition to Windows, it is available for Unix-based platforms.

The ActivClient Software Development Kit (SDK) enables systems integrators and independent software vendors to smart card-enable their applications. Software developers do not need specific knowledge of smart card technology to integrate ActivClient services into their applications.

When users lose a smart card or forget a password, ActivClient provides an emergency Windows login using knowledge-based (i.e., question and answer) authentication.

ActivClient User Console
**System Requirements**

- Linux, Mac, Solaris: contact ActivIdentity for the latest information

**Government Standards**

- FIPS 201 certified / NIST Special Publications 800-73-3 compliant
- U.S. Government Smart Card Interoperability Specifications GSC-is 2.1
- ActivIdentity Applets - FIPS 140-2 Level 2 and Level 3 certified
- FDOCC / SCAP 11 compliant
- Section 508 compliant

**Technology**

- Smart Card Mini Driver (ActivClient 7.0), Smart Card CSP (ActivClient 6.2), PKCS#11

**Security Services**

- Secure workstation and network login: Windows Smart Card Login, Novell Login
- Secure VPN with Check Point®, Cisco®, Juniper®, Microsoft® and many other remote access solutions
- Secure Web Login with Google Chrome, Microsoft Internet Explorer® 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) and BitLocker To Go
- Entrust Ready: Support for Entrust Entelligence Security Provider and Entrust Entelligence Desktop Solutions*
- Pre-boot authentication, disk and file encryption with Check Point, McAfee, Safenet, Symantec, Sophos, Trend Micro, WinMagic and more

**Smart Card Support**

- Smart cards and USB tokens from ActivIdentity, Athena, Atmel, CardLogix, Gemalto, Giesecke & Devrient, HID Global, Keycorp, NXP, Oberthur, Safenet, Sagem Orga and Sharp

---

* ActivClient 6.2 only