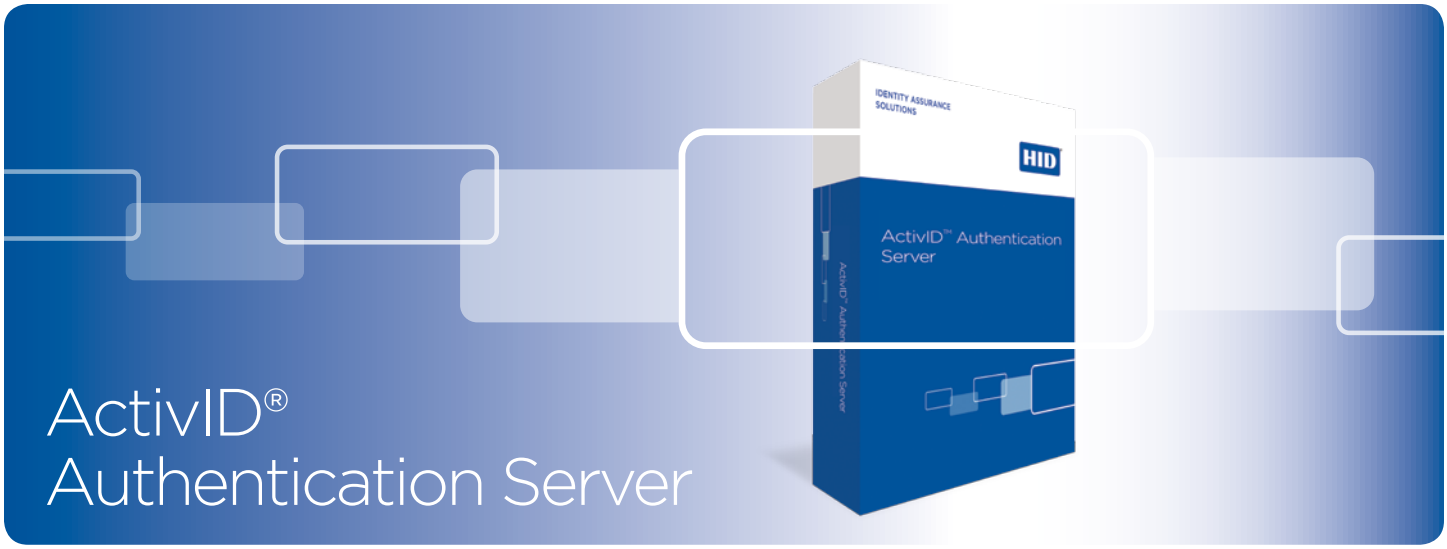
IDENTITY & ACCESS MANAGEMENT



ActivID® Authentication Server

STRONG AND VERSATILE AUTHENTICATION SERVER

- **Increase security –** Robust two-factor authentication reduces risks and mitigates breaches.
- **Enhance user convenience –** Multi-layer authentication addresses user demands for convenience and portability.
- **Increase productivity –** Connects users securely through a variety of devices and authentication methods and unobtrusive ActivID Threat Detection software for anywhere, anytime access.
- **Extended value –** Enables secure access from any smartphone, tablet, laptop or PC for login to the network, VPNs, web portals and cloud applications.

ACTIVID® AUTHENTICATION SERVER INCLUDES ADDITIONAL FEATURES THAT HELP ORGANIZATIONS IMPROVE PRODUCTIVITY:

- Secure access from laptops, browsers, tablets, and smartphones using strong authentication
- HID Approve™ provides a convenient out-of-band authentication with the user's mobile device and push notifications
- Worry-free soft tokens enable simple and affordable access to corporate data for telecommuters and heavy smartphone users
- Broad range of hardware and software authentication methods provide options and price points to best meet business needs
- Short message service (SMS) one-time passwords (OTP) ensure secure connectivity when tokens are not available or preferred
- ActivID Threat Detection Service transparently adds frictionless authentication and account take-over protection

HID Global's ActivID® Authentication Server provides corporate, financial and government organizations with risk-appropriate, cost-effective user authentication. The solution enables end users to have convenient anytime, anywhere access to sensitive data from their smartphones, tablets, computers and virtually any other device.

With ActivID Authentication Server, organizations can also tailor their authentication methods for specific groups of users, based on their business objectives and policy/regulatory compliance needs. For example, financial institutions can use HID Approve™ to enable mobile-based, out-of-band transaction verification, leveraging mobile device "push" notification capabilities. Also available is the built-in ActivID Threat Detection Service that transparently protects online transactions from a wide range of threats, including Trojan and man-in-the-browser (MitB) attacks.

It also supports the broadest range of authentication methods, from strong passwords to certificate-based authentication, including two-factor, OATH-standards-based hardware tokens; soft tokens; device forensics; and SMS Out-of-Band One-Time Password (OTP) options.

Deployment is simplified, too, through the platform's pre-integration with major cloud apps, VPN systems, application servers, banking applications and other third-party systems.

Available on-premise, the ActivID Authentication Server can help to reduce total cost of ownership with easy installation, worry-free tokens that last up to eight years, and simple integration into an organization's existing network infrastructure.

FEATURES:

- Policy driven, organization-wide authentication solution with fine-grained authentication policies.
- Easily integrates with applications to leverage strong authentication.
- Digitally signed and sequenced audit logging and policies.
- Secure, highly scalable (from 100s to millions), resilient architecture.
- Strong segregation between different user populations with enhanced security domains.
- Works optionally with FIPS 140-2 HSM to secure an organization's keys.
- Works concurrently with legacy authentication servers for graceful and efficient migration.
- Integrates with Active Directory and most standard LDAP to match the scalability and availability of the organization's network (can be deployed with internal database when there is no existing LDAP).
- Flexible solution that allows organizations to generate their own security seed files for hardware token deployments.
- Tokens auto-synchronize to improve reliability and security and reduce support calls.
- Secure real-time transaction authorization for mobile applications to provide government-strength security with consumer ease of use.
- Integrates seamlessly with full suite of credential management, middleware, smart card, single sign-on, mobility and physical access control offerings.

SPECIFICATIONS

Built-in Authentication Methods	▪ HID Approve™ for public-key based authentication and transaction signing with mobile push notification ▪ One-time password (HID Global-patented algorithm) and challenge / response ▪ One-time password: OATH HOTP Event, TOTP Time-based, & OCRA challenge / response ▪ EMV CAP algorithm ▪ OATH transaction signing (OCRA) Smart Card PKI / X.509 certificate ▪ Emergency full and partial strong static password and security questions ▪ Knowledge Based Authentication (KBA) – Out-of-Wallet Questions ▪ Out-Of-Band One-Time Password or Transaction Verification code sent via SMS or email device ID with web browser registration ▪ Optional ActivID® Threat Detection Service for device profiling and risk-based authentication and browser-based malware detection
External Authentication Methods	LDAP fallback and passthrough, RADIUS conditional routing
Authenticators	**Hardware Tokens** OTP Token, KeyChain OTP Token, Desktop OTP Token, Pocket OTP Token, Mini OTP Token, ActivID Flexi Token, Any OATH compliant event, time or challenge / response- based hardware token, Smart Card (with ActivID CMS), including Crescendo C1100
	DisplayCard Tokens DisplayCard Token and Smart DisplayCard Token
	Software Tokens PC Soft Token, Mobile Soft Token (iOS, Android), Web Soft Token
User Repositories	**Database** Oracle 11g Express, Oracle 11g R2, Oracle 12c
	LDAP Microsoft® Active Directory®, Oracle® / Sun Java™ Directory, Novell® eDirectory™
Standards Supported	**Protocols** SAML v2, RADIUS Authentication and Authorization, Web Services (SOAP v1.1), LDAP v3 SNMP V3, OpenID/OAuth2, SCIM (System for Cross-domain Identity Management)
	Cryptographic OATH event, time and challenge / response, 3DES / AES / RSA / ECC / SHA-2, FIPS 140-2 level 3 HSM, PSKC v1.0 (credential import)
Help Desk and Self Service	Web-based help desk and self -service,; localizable and U.S. Section 508 compliant
Administration	Device and Credential management, Authentication Policy management, User, User Group, Role and Permission Management
Auditing, Accounting and Reporting	Digitally signed and sequenced tamper-evident audit log, Audit log queries, Published audit schema
Secure Key Storage	▪ SafeNet® ProtectServer External ▪ Thales® netHSM™ & nCipher Connect™ 6000+ ▪ Thales nCipher™ nShield™ (PCI), ▪ Thales payShield™ (PCI & netHSM) ▪ Software cryptography

HID Global
North America: +1 512 776 9000
Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800
Latin America: +52 55 5081 1650

hidglobal.com

ASSA ABLOY
An ASSA ABLOY Group brand

2016-10-13-identity-assurance-activid-authentication-server-ds-en PLT-02543