IDENTITY AND ACCESS MANAGEMENT SOLUTIONS

ActivID® Authentication Server

ACTIVID® AUTHENTICATION SERVER HELPS ORGANIZATIONS IMPROVE PRODUCTIVITY:

- Secure access from laptops, browsers, tablets, and smartphones using strong authentication.
- Broad range of hardware and software authentication methods provide options and price points to best meet business needs
- Convenient and secure push notification based authentication with HID Approve.
- Out-of-band authentication via SMS One-Time Passcodes or email ensures secure connectivity when other methods are not available
- Seamless integration with HID Risk Management Solution enables adaptive step-up authentication and account take-over protection

STRONG AND VERSATILE AUTHENTICATION SERVER

- **Increase security –** Reduces risks and mitigates breaches with robust two-factor authentication.
- **Enhance user convenience –** Addresses user demands for convenience and portability with multi-layer authentication.
- **Increase productivity –** Connects users securely through a variety of devices and authentication methods for anywhere, anytime access.
- **Extend value –** Enables secure access from any smartphone, tablet, laptop or PC for login to networks, VPNs, web portals and cloud applications.

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 access to sensitive data from their smartphones, tablets, computers and virtually any other device.

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 out-of-band transaction verification, leveraging mobile device "push" notifications.

The HID Risk Management Solution uses machine learning and artificial intelligence to protect online transactions from a wide range of threats, including fraudulent transactions, account take over, financial malware and Man-in-the-browser (MitB attacks). HID Risk Management also supports risk-based advanced authentication, allowing organizations to deploy a highly secure authentication workflow that is transparent to the end user.

The ActivID Authentication Server 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 also simplified through the platform's pre-integration with major cloud apps, VPN systems, application servers, banking applications and other third-party systems.

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:

- Natively integrated with HID Risk Management Solution for threat and fraud detection, and risk-based advanced authentication.
- Interoperable with HID Approve for push-based authentication with mobile notifications.
- 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 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 allowing organizations to leverage their existing user repository (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 as well as 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 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 ▪ Out-of-Band One-Time Password or transaction verification code sent via SMS or email ▪ Adaptive authentication with HID Risk Management Solution ▪ Optional threat and fraud detection with HID Risk Management Solution
External Authentication	LDAP fallback and passthrough, RADIUS conditional routing
Authenticators	**Hardware Tokens** BlueTrust Token, 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, FIDO U2F and FIDO 2.0 devices, Smart Card (with ActivID CMS), including Crescendo C1100
	Software Tokens Mobile and PC software token with HID Approve on iOS®, Android™, Windows 10
User Repositories	**Database** Oracle 12c
	LDAP Support for Microsoft® Active Directory®, Oracle / Sun Java™ Directory, Novell® eDirectory™
Standards Supported	**Protocols** SAML v2, RADIUS Authentication and Authorization, FIDO, Web Services (SOAP), RESTful API over HTTP, LDAP v3 SNMP V3, OpenID/OAuth2, SCIM (System for Cross-domain Identity Management), Open Banking Security Profile
	Cryptographic OATH event, time and challenge / response, 3DES / AES / RSA / ECC / SHA-2, FIPS 140-2 level 3 HSM, PSKC v1.0 (credential import)
	Compliance Enablement DFS 23 NYCRR 500, FFIEC, GDPR, OpenBanking, PCI DSS, PSD2
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) ▪ nShield XC (Base, Mid, High) ▪ Software cryptography

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

2019-07-10-identity-assurance-activid-authentication-server-ds-en PLT-02543