

AEP SMARTGATE®

A SECURE INFORMATION SHARING SOLUTION FOR IP-BASED NETWORK ENVIRONMENTS

AEP SmartGate is an identity-based application layer security product designed for large-scale, distributed, information-sharing environments. SmartGate, a FIPS-certified solution, enables organizations to securely exchange information with employees, customers and business partners over any IP-based infrastructure. Advanced features enable federated identity and access privileges across trusted organizations.



Key Capabilities

SmartGate software allows organizations to rapidly deploy an application layer VPN solution capable of supporting thousands of simultaneous users, while meeting stringent security standards.

- Delivers a framework for data encryption, access control, strong user authentication, and audit logging
- Fine-grained access controls allow secure access to specific TCP/IP based applications and internal resources
- All traffic routed to a single port proxy that hides network topology and prevents direct connection to target resources
- Software architecture allows separation of proxy server, identity and encryption modules for maximum flexibility and performance
- Scalability to more than 100,000 users, proven in real-world implementations
- Geographical separation and redundancy for high availability and continuity of operations
- Works over any IP networking infrastructure – terrestrial, wireless, Internet, IPsec VPN, Frame Relay and satellite
- Allows PKI-enabling of TCP/IP applications without modification
- Patented on-line registration establishes user identity and activates credentials
- Integrates easily within enterprise-wide security framework

Government Grade Security

- FIPS-validated solution: All cryptographic elements of the server software, not just subcomponents, are FIPS 140-2 validated
- Integrated FIPS 140 validated software token for strong, 2-factor user authentication
- End-to-end 256-bit AES encryption using dynamic session keys

Compliance Features

- Fine-grained access controls provide user-to-application protection, with audit logging capabilities, to secure internal and external network access
- Supports HIPAA and Sarbanes Oxley requirements
- End-to-end encryption assures data privacy
- End Point Security protection can be configured for compliance-based policy enforcement and interoperates with third party applications
- Users and applications can be activated or revoked in seconds

- SmartAdmin™ delivers centralized or distributed management with four administrator levels and powerful group management options

Strong Authentication

- Integrated government approved FIPS-validated software token for digital identity and multi-factor authentication
- Token stored on user's machine or on variety of token storage devices
- Supports third-party authentication mechanisms, including LDAP, RSA SecurID, X.509 PKI, RADIUS and biometric devices
- Advanced capabilities allow separation of authentication and encryption servers, portable identity entitlement across domains for federated authentication, and single sign-on to multiple resources

Flexible End User Access Options

- Clientless Java™ agent available for all leading browsers
- AEP SmartPass® lightweight intelligent client does not require a browser; runs as a non-intrusive application on the end user device
- Broad platform support includes Java, Windows 98/2000/XP/NT/Me, CE/PocketPC, Sun Solaris, Linux, and Macintosh

Mobile Wireless/Satellite Security

- Delivers high performance, end-to-end secure communications over hybrid networks
- SmartSat™ engineered to overcome high-latency delays associated with satellite connections, allowing virtually same as "in-the-clear" performance
- Secures PDAs and wireless LAN/WAN connections to support the mobile workforce

Specifications

General

- Software based secure access solution built on application layer and SSL VPN technology
- Hardware turnkey solutions available
- All secure traffic directed to SmartGate single port proxy server
- SmartPass client employs shim technology to eliminate need for end user device configuration

Application Access

- Natively supports IP-based protocols and applications including HTTP, HTTPS, FTP, Telnet, rlogin, POP, SMTP, IMAP, TN3270, SSH, VNC, RDP, Citrix, Oracle, etc.
- Access to virtually any application in data center
- Drive mapping (CIFS)

Authentication

- AEP FIPS 140 validated software token
- RSA SecurID
- LDAP
- RADIUS
- Entrust
- X.509 PKI
- Windows PC
- Mutual authentication (client/server)
- SmartGate Aware® credential passing
- Compatible with numerous token storage devices including smart cards and AEP SmartKey™

Encryption

- 256, 192 and 128 -bit AES
- 168-bit 3DES
- DES, RC4, SHA-1, MD5
- Dynamic session keys
- FIPS 197 validated cryptographic algorithms

Access Control

- Granular access control and policy enforcement for users and groups to access applications, data, and URLs
- Dynamically updated access permissions
- Time based access control options

End Point Security

- End point security applications verified for existence, version level and execution
- Access determined by compliance levels
- Cache cleaning and track removal

Administration/Management

- Simple, web based administration
- Self-provisioning patented online registration system
- Individual, group and nested group operations
- Four role-based administrator levels
- Separation of authentication and proxy/encryption servers
- Identity entitlement across domains
- Primary/secondary, dual-active backup
- Audit logging on client and server
- Numerous administrator configurable security parameters for client and server

Server Requirements

- Intel Celeron or equivalent processor with at least 950 MHz, 128KB RAM
- 200 MB minimum free hard disk space
- Two or more network interface cards
- TCP/IP connection to a network

Supported Platforms

Version information available upon request.

> SmartGate Server

- Windows Server 2003
- Windows 2000 Server
- Windows NT 4.0
- Red Hat Linux, Fedora
- Sun Solaris

> SmartPass Client

- Java agent
- Microsoft Windows
 - Windows XP Professional, Home
 - Windows 2000 Professional
 - Windows NT 4.0 Workstation
 - Windows 98 SE
 - Windows Me
- Windows CE
- Pocket PC
- Red Hat Linux, Fedora
- Sun Solaris
- Macintosh

> Browsers

- Internet Explorer
- Netscape Navigator
- Mozilla Firefox

Government Certifications

- FIPS 140-2 (NIST certificate #510)
- FIPS 140-1 (NIST certificate #141)
- FIPS 197 (NIST certificate #35)
- DoD JITC PKI certification (12/04)
- Other agency-specific credentials

Contact us:

CORPORATE HEADQUARTERS

347 ELIZABETH AVE., SUITE 100
SOMERSET NJ 08873
TOLL-FREE: 1 877 638 4552
TEL: (+1) 732 652 5200

GOVERNMENT SOLUTIONS GROUP

40 WEST GUDE DRIVE, SUITE 200
ROCKVILLE, MD 20850
TOLL-FREE: 1 800 495 8663
TEL: (+1) 240 399 1200

EUROPE

FOCUS 31, WEST WING
CLEVELAND ROAD
HEMEL HEMPSTEAD
HERTS HP2 7BW U.K.
TEL: (+44) 1442 458 600

ASIA-PACIFIC

2107 TOWER 2
LIPPO CENTRE 89 QUEENSWAY
HONG KONG
TEL: (+852) 2845 1118

JAPAN

JOYO BLDG 6-22-6
SHIMBASHI MINATO-KU
TOKYO 105-0004
JAPAN
TEL: (+81) 3 3432 3336

Accreditation

