



Trusted. Certified. Secure.



AEP SmartGate® is an identity-based logical access management product designed for rapid deployment of 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. With customers such as Kanoria Petrochemicals Ltd., San Jose State University (SJSU), Cal Poly San Luis Obispo, and Software Technology Group, eWebUniversity's solutions are built to address the needs of both corporations and educational institutions.

### Government Grade Security

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

### Compliance Features

- Supports HSPD-12 program objectives, HIPAA and Sarbanes-Oxley requirements
- End-to-end encryption assures data privacy and integrity
- End Point Security protection can be configured for compliance-based policy enforcement
- 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
- IS4 Compliant

### Strong Authentication

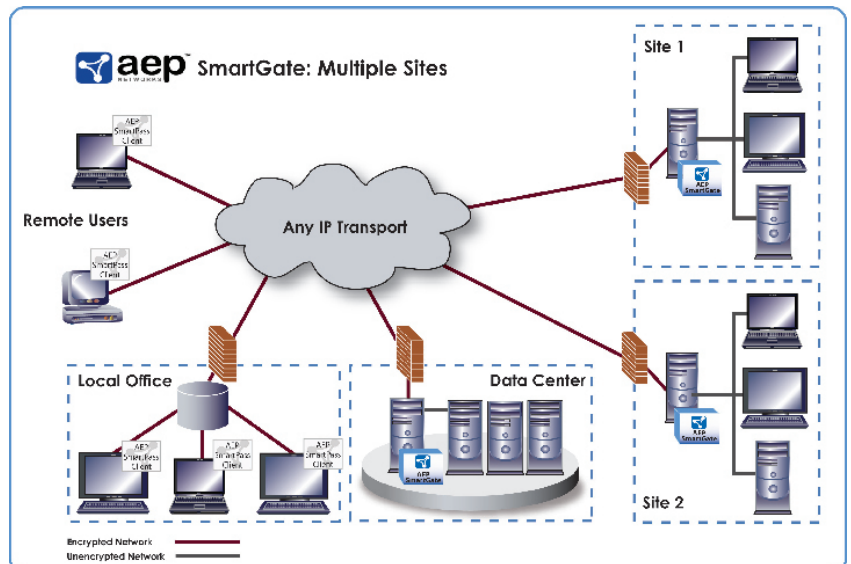
- Integrated government approved FIPS-validated software token for digital identity and multi-factor authentication
- Token stored on user's machine or on variety of token storage devices
- Supports third-party authentication mechanisms, including LDAP, RSA SecurID, X.509 PKI, RADIUS and biometric devices
- 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, 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





Trusted. Certified. Secure.

## General

- Software-based certified cryptographic algorithms
- 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 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)
- FIPS 201 Compatible

## Key Capabilities

- Delivers framework for universal access management with data encryption, access control, strong two-factor user authentication, and audit logging
- Fine-grained access controls allow secure user access to specific TCP/IP-based applications, URLs, and other resources
- Allows PKI-enabling of TCP/IP applications without modification
- 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
- Patented on-line registration establishes user identity and activates credentials
- Scalability to more than 100,000 users, proven in real-world implementations
- Geographical separation and redundancy for high availability and continuity of operations
- Works well over any IP networking infrastructure – terrestrial, wireless, and satellite
- Integrates easily within enterprise-wide security framework to secure internal and external network access

## About AEP Networks

AEP Networks offers a comprehensive Policy Networking solution that provides complete security starting at the endpoints and working throughout a network – from the edge to the core. AEP's integrated portfolio of security products includes network admission control enforcement points, identity-based application security gateways, SSL VPNs, CAPS approved high assurance IPSec-based VPN encryptors, and FIPS certified hardware security modules for key management. Our products address the most demanding security requirements of public-sector organizations and commercial enterprises internationally. The company has design and development offices in its headquarters in Somerset, New Jersey, USA and Hemel Hempstead, UK.

## Contact Us:

### United States

Toll-Free: 1-877-638-4552

Tel: +1-732-652-5200

### Europe

Tel: +44 1442 458 600

Email: [sales@aepnetworks.com](mailto:sales@aepnetworks.com)

Web: [www.aepnetworks.com](http://www.aepnetworks.com)

## Accreditation

