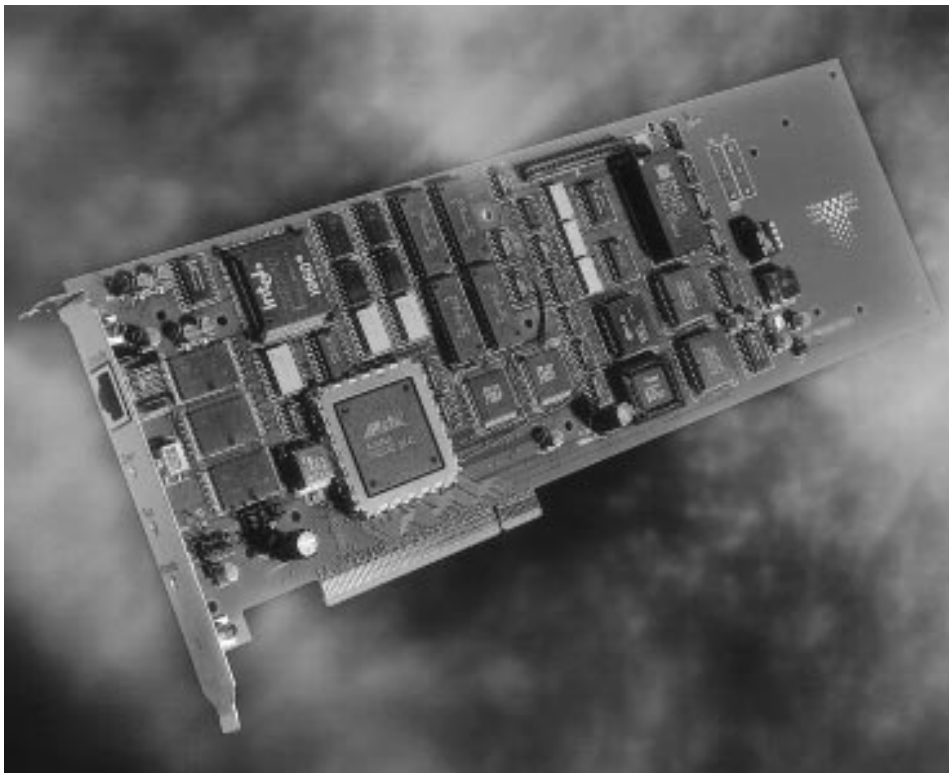
PERMIT* Secure Virtual Private Network Module

System Key Features

- Reliable and Comprehensive Network Security
  - IETF IPSEC Standard Network Security Solution
  - Dynamic Session Key Agreement and Automatic Secure Sessions Establishment
  - Transparent Data Confidentiality, Integrity and Authentication
- Central Management of Security Policy
  - Monitoring, Configuration, Authentication, Revocation and Permissions Control Via SNMP With Message Authentication
  - X.509 Certificates With Automatic Public Key Distribution
- Ease of Deployment; Maintenance and Use
  - Non-Intrusive “Plug and Play” Functionality Independent of Existing LAN/WAN Infrastructure Software Downloading of Updates and New Features
  - Transparent to the End-User and Existing Network Applications With No Impact on Real-Time Network Performance



PERMIT* SVPN* technology implements IETF IPSEC security standards to provide transparent end-to-end secure communications. The PERMIT SVPN system provides data integrity, confidentiality, authentication and access control.

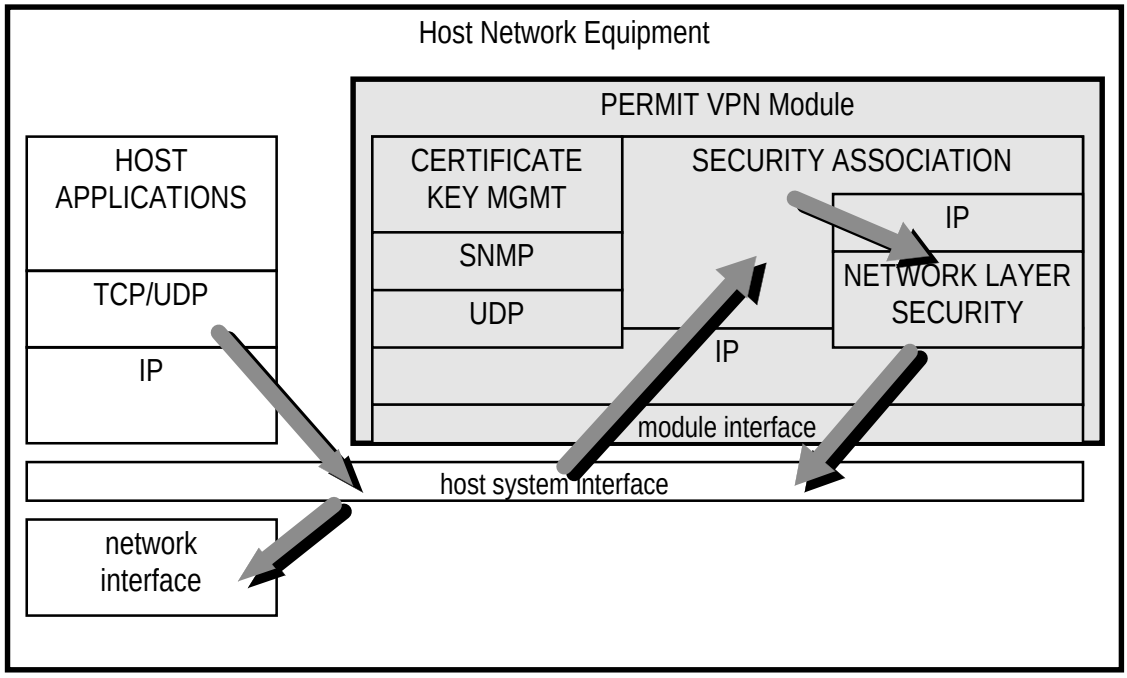
The PERMIT SVPN Module offers network equipment providers rapid deployment of highly effective network data encryption and authentication. The PERMIT SVPN Module enables network security for network equipment including routers, multiplexors and network servers and for PC and Sun workstations that are networked for the purpose of desktop workstation, file servers, firewalls and Web/FTP network servers.

The PERMIT SVPN family of products delivers a complete, centrally managed network security solution for authentication, data confidentiality and integrity for TCP/IP networks. The PERMIT SVPN system is comprised of a series of SNMP managed components that encrypts IP traffic transparently in the existing networking infrastructure for local and remote clients and servers. PERMIT SVPN technology is able to secure all network applications without costly software modifications or upgrades and without the replacement of the existing networking infrastructure (e.g. routers, hubs, switches). The PERMIT SVPN system enables the deployment of communications security transparently, throughout the Enterprise or beyond.

CONTACT:
Corporate Headquarters
TimeStep Corporation
362 Terry Fox Drive,
Kanata, Ontario
Canada K2K 2P5
Phone: (613) 599-3610
FAX: (613) 599-3617

U.S. Headquarters
TimeStep Inc.
593 Herndon Parkway,
Herndon, Virginia. 20170
Phone: (703) 478-5220
FAX: (703) 478-5222
e-mail: info@timestep.com
WWW: www.timestep.com

TIMESTEP



PERMIT* SVPN Module Software and Data Flow

System Applications

- Internal Network Security
  - – Protection of Sensitive Data From Internal Snooping and Manipulation
  - – Partitioning of Shared Corporate Networks into Private Workgroups
- Leased External Network Security
  - – Single Interoperable Solution For Any Wide Area Network Infrastructure
  - – Enable Private Use of Shared Network Services Such as ATM and Frame-Relay
- Telecommuting and Remote Office Connectivity Via the Internet
  - – Inexpensive and Widely Available Remote Connectivity Via the Internet
  - – Multiple and Scaleable Connectivity Options Including Modem, ISDN, T1, Cable Modem
  - – Elimination of Capital and Administrative Costs of Remote Access Equipment
  - – Elimination of Remote Access Toll Charges Due to Local Internet Point-of-Presence

TCP/IP data is passed to the PERMIT VPN Module via its dual-port RAM. The data is encrypted, authenticated and encapsulated or decapsulated, authenticated and decrypted by the PERMIT VPN Module based on the data's security associations.

PERMIT SVPN Module Feature Definition

- PC PCI Bus Adapter
- Automated Self Testing
- LED Indicators – Run, Secure, Alarm
- Recessed Panel Button For Clearing of Critical Data
- Physical Interface – Shared True Dual-Port RAM With Host Workstation
- Console Via Host Workstation
  - – Password Protected
  - – Network Address Configuration
  - – Firmware Download
  - – Diagnostic Statistics – Certificate Info, Permissions, Revocations, Associations, Error Logs
- Initial Certification With CA Via Predefined Password
- IETF IPSEC AH/ESP
- Hardware Encryption Algorithms – DES, DES40
- Public Key Algorithms – RSA
- Certificate Distribution
  - – From CA Via SNMP With Authentication
  - – Local Caching and iInband Exchange Via SAP
- Management – SNMP With Authentication For Any SETs
- Secure Proxy For a Single Red IP Address
- Permissions
  - – Controlled, Distributed and Signed By Manager
  - – IP Based With Wild-Cards
  - – DES, Clear or Blocked
- CRLs Controlled, Distributed and Signed By Manager