IP Security (IPSec)

The IP Security (IPSec) is an Internet Engineering Task Force (IETF) standards suits of protocol between 2 communication points across the IP network that provide data authentication, integrity and Confidentially.

Uses of IP Security.

To Encrypt Application layer data.

To provide Security for Routers Sending routing data across the public Internet.

To protect network data by setting up circuits using IPSec tunneling in which all data is being sent between the two endpoints is encrypted, as with a Virtual Private Network (VPN) connection.

SNMPV3

In Contrasts to SNMP version-1 (SNMPv1) and SNMP version-2 (SNMPv2), SNMP version-3 (SNMPv3) supports authentication and encryption.

SNMPv3 uses the User-based security Model (USM) for messages and the view-based security access control model (VACM) for access control.

USM uses the Concepts of a User for which security parameters (levels of security) authentication, privacy protocols, and Keys are Configured for both the agent and the manager.

Messages sent using USM are better protected than a message with Community strings, where passwords are sent in the clear.

across the enter enterprise.

X.509.

In Cryptography, X.509 is a standard defining the format of public key certificate.

X.509 Certificates are used in many internet protocols, including TLS / SSL, which is the basic for HTTPS, the Secure protocol for browsing the web.

They are also used in offline application like electronic Signature.

X.509 is designed by international Telecommunication Union's Standardization Sector (ITUT), and is based on ASN.1 another ITU-T Standard.