SeguriDATA

SeguriTELNET

Sesiones Telnet
seguras y confidenciales

SeguriDATA Privada S.A. de C.V. Amores 1003-1. 03100, México D.F. México
Teléfonos: (525) 575-3407 / 6385 / 9658 / 9761 Fax: 559-5887

http://www.seguridata.com

SeguriTELNET

Objetivos

El esquema de operación de SeguriTELNET está basado en el uso de las tecnologías de Certificados Digitales X.509 y de criptografía de llave pública (Public Key Cryptography Standard, PKCS) para lograr dos objetivos fundamentales:

a) Asegurar la confidencialidad de la información durante una sesión de Telnet entre un cliente y el servidor.

b) Garantizar la autenticidad del servidor de Telnet al que se realiza la conexión. Esta posibilidad puede extenderse para realizar la autenticación de los clientes.

Procedimiento

Estos objetivos se logran en SeguriTELNET con el siguiente protocolo:

1) Cuando un cliente solicita una conexión, SeguriTELNET comienza un proceso para atenderla.
Por medio de SeguriTELNET, el cliente genera una llave simétrica de 128 bits para la sesión.

2) A conitinuación, se obtiene la llave pública del servidor SeguriTELNET, misma que es utilizada para encriptar la llave de sesión, y es enviada encriptada al servidor.

3) Al recibir la llave, el servidor la desencripta con su llave privada, obtendiendo la llave de la sesión.

Plataformas

De esta manera, toda la información que fluya entre cliente y servidor, será encriptada con la llave de la sesión hasta el momento en que la conexión Telnet se de por concluida.

SeguriTELNET funciona prácticamente sobre cualquier plataforma con ANSI C. Ha sido probado para los sistemas operativos:

- Solaris
- HP-UX
- LINUX
- MS Windows 95 / NT

Como software complementario a SeguriTELNET se encuentra SeguriSERVER, el cual permite la generación y administración de Certificados Digitales (X. 509) y utiliza algoritmos RSA con llaves hasta de 2048 bits, y RC4 con llaves de 128 bits de longitud, para la generación de las llaves asimétricas, tanto pública como privada.