PrivateWire™
Securing Internet for Business

PrivateWire Security Gateway & PrivateWire Client

FIPS 140-1 Non-Proprietary Security Policy

Level 1 Validation
April, 2000

Table of Contents

1 INTRODUCTION

1.1 Purpose

This is a non-Proprietary FIPS 140-1 Security Policy for PrivateWire. It describes how both the PrivateWire Client and Gateway meet all FIPS 140-1 Level 1 requirements. The Security Policy was prepared as part of the Level 1 FIPS 140-1 certification of both the PrivateWire Security Gateway and PrivateWire Client.

FIPS 140-1 (Federal Information Processing Standards Publication 140-1) is a U.S. Government standard entitled "*Security Requirements for Cryptographic Modules*." This standard mandates a set of strict design and documentation requirements that hardware and software cryptographic module must meet in order to be validated by the U.S. National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE).

1.2 References

This FIPS 140-1 Security Policy describes features and designs of the PrivateWire components using the technical terms of FIPS 140-1.

- For more information on the FIPS 140-1 standard and validation program readers are referred to the NIST web site at http://csrc.nist.gov/cryptval/.

- For more information on the PrivateWire product line, please visit the Algorithmic Research web site at http://www.arx.com.

1.3 Document Organization

This section provides a general introduction to the Security Policy. Section 2 introduces the PrivateWire software package. Section 3 discusses the PrivateWire Security Gateway and Client and how they meet FIPS 140-1.

2 PrivateWire

PrivateWire is a powerful software-based application, which employs the most advanced data security technologies to form a multi-layered protection system. The PrivateWire system consists of two separate modules: the Security Gateway Server (which can be run on Windows NT 3.51/4 and Sun-Solaris 2.6) and the Security Client (which can be run on Windows 3.x, Windows 98, and Windows NT 3.51/4). PrivateWire is designed to allow secure access to the organization's resources to multiple users over an untrusted TCP/IP network. The Gateway resides on a corporate server and secures connections to other Gateways or Clients. Together they transparently perform all of required security functions and provide the following high-level functionality:

- Screening of all incoming communications to ensure authorized user access
- Secure, authenticated and encrypted sessions between Client and Gateway
- Secure Virtual Private Network (VPN) between sub-systems
- Central security administration

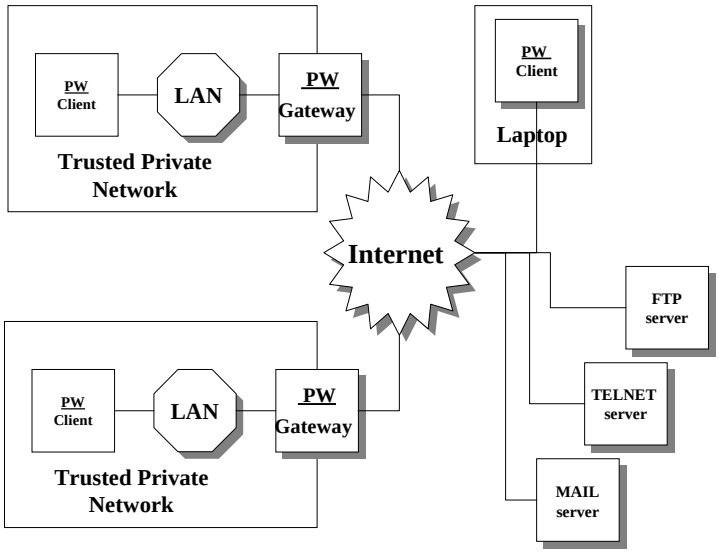

Figure 1: PrivateWire Creates an Enterprise-Wide VPN

A Virtual Private Network (VPN) provides a protected connection between two machines and sends private data traffic over a shared or public network, the Internet. This technology lets an organization extend its network service over the Internet to branch offices and remote users creating a private WAN (Wide Area Network) over the Internet. As shown in Figure 1, PrivateWire establishes a VPN by allowing an organization to secure communications between its different sub-systems.

The PrivateWire Client encrypts data being sent from a user's machine and the Security Gateway then decrypts data once it enters the organization's private network. Similarly, all data destined for a remote client is encrypted by the Gateway before it leaves the private network and is decrypted after it safely reaches the client.

PrivateWire also supports a Gateway to Gateway solution that enables organizations to deploy PrivateWire not only at the user level, but at the branch or office level as well. This option allows an organization to secure channels between offices and create an organizational VPN complete with remote user access and Intranet systems.

3 The PrivateWire Components

PrivateWire is a software cryptographic module, which secures all TCP/IP communications between an organization and its customers and employees. The PrivateWire Security Gateway is the software component installed in a server on the organization's network. The PrivateWire Client is the software component that is installed on a customer or employee's computer to communicate with PrivateWire Gateway. The PrivateWire components provide key generation, storage, digital signatures, dynamic package filtering, and user certification. In addition, the PrivateWire Client provides high-level encryption, with certificate-based two-way authentication, authorization, digital signatures and transparent communication security to its customers. This allows organizations to build a high-level security infrastructure for all TCP/IP applications including: WWW, FTP, Telnet, mail and any TCP/IP client/server application based on a single integrated solution that can be easily managed and deployed. All communications may be encrypted using DES, triple-DES or RC-4 symmetric encryption.

PrivateWire provides the following security services:

- Strong two-way authentication - using DSA and RSA 1024-bit keys.
- Powerful access control - using passwords or optional hardware tokens.

- Data confidentiality - using strong encryption e.g. DES, triple DES and RC-4.
- Data integrity - ensuring the accuracy and integrity of transactions.
- Digital signatures - to digitally sign transactions and ensure the highest level of security.
- Dynamic packet filtering - controlling all passing communications with full session monitoring.
- User Certification - providing foolproof digital identification using X509 certificates.

3.1 Module Interfaces

Both PrivateWire Client and PrivateWire Gateway are considered to be a multi-chip standalone modules for FIPS 140-1. As such the modules requires a general-purpose operating system (OS) run on a computer. The physical interfaces of the modules include the computer keyboard, CD-ROM drive, floppy drive, mouse, screen, and ports. The PrivateWire Client software logically interfaces to the network through the network-level after the information has been accessed through those physical interfaces.

The logical interfaces for the PW Client and PW Gateway (and the physical interfaces they cross) are:

- **Data input interface**: graphic user interface for the program (GUI), keyboard port, disk drive, network ports
- **Data output interface**: disk drive, screen, network layer IP packets via the Winsock interface (network ports), monitor port
- **Control input interface**: network layer IP packets via the Winsock interface (connection through the PW Gateway, which are secured)
- **Status output interface**: screen, network layer IP packets via the Winsock interface.

The logical interfaces are separated by the GUI that distinguishes between data input, data output, control input, and status output through its dialogues. Similarly, the module separates Network-layer traffic, distinguishing between data, control and status packets based on IP address, and protocol.

3.2 Roles and Services

PrivateWire supports two distinct roles using digital signatures and PIN codes for authentication: User role and Crypto-officer role. Both the Security Gateway and Client each support the User role and Crypto-Officer role.

An operator assuming the Gateway's Crypto-Officer role performs the primary configuration of PrivateWire. The PrivateWire Security Gateway administrator implicitly assumes the Crypto-Officer role after authentication and uses a powerful set of management tools to configure the Gateway. The Client is used to authenticate and connect securely to the Gateway. To connect, the operator assumes the Client User role and then the Gateway's User role while an authenticated, secure session is created. Thus, an authorized administrator may access the Gateway management from any local or remote location.

3.2.1 Gateway Crypto-Officer Role

The role of the Crypto-Officer includes refinement of administrative permissions, generation and destruction of keys, user access control, and creation of the information database. In addition, PrivateWire provides management tools for user certification. Certification can be done locally or remotely as required, in any hierarchical model. Only certain users authorized to administer the server are allowed to access the information and use the sensitive management functions. The following are Crypto-Officer services:

- User certification: Facilitate loading new users into the system, certifying their identity, adding and managing system users, and monitoring and generating reports.
- System Administration: By implementing criteria-based rules, PrivateWire enables system managers to assign specific administrative activities and administrators' extent of access.
- Access control: Assigning users to groups with pre-defined access privileges and control of user access to organization's network. These groups are defined according to the organization's security policy

- Monitoring: Provides detailed information for both monitoring of connection activities and for logging, alerting, and billing. Specific user information is logged and confirmed, activity reports can be issued on demand.
- Database information management: Holds all the information needed to execute the organization's local security policy.

Administration is implemented with the following functions, which are accessed by the Crypto-Officer through the gateway's remote user interface:

- Rules Table – Define and edit the selectivity criteria and action to be applied in packet filtering.
- Users – View and edit the uses list and users parameters.
- Groups – Define and edit the groups list and each groups' parameters. A group is a list of permitted services/actions. Each user is assigned to one or more groups which together determine his or her permitted services/actions.
- Auditing and Alerts – View logs based on definitions made by the security supervisor in the packet filtering rules table and Groups rules tables.
- Setup – Define and set limits to various system parameters.

3.2.2 Gateway User Role

Secure connections to the Gateway, implicitly assume the User role as they authenticate, negotiate session keys and create a secure tunnel. The only service available to the User role is the creation of these secure sessions with the Gateway.

3.2.3 Client Crypto-Officer Role

Administrators of the PrivateWire Client software assume the role of Crypto-Officer, and install, configure, and operate the Client. The Crypto-Officer role includes refinement of administrative permissions, generation and destruction of keys, user access control, and creation of the information database. In the PrivateWire Client, the role and services of the Crypto-Officer are limited, since the software module is designed for easy, simplified use by an end-user. Available Crypto-Officer services include:

- Generation of keys: to create new public-private key pairs. The Crypto-Officer supplies a user ID, name, type of key, and key size. The Crypto-Officer also enters random information via keystroke inter-timings to seed the PrivateWire Client's random number generation.
- Select Key Media: this is used to pick the location of the key for the current operator.
- Exporting keys: this service transfers the public keys to the organization for certification (here the user can copy their key to a file) or to an appointed certifier.
- Importing keys: this service allows the import of a certified public key from a file created by the certifying authority.
- Secure Sites Setup: specifies the sites that you can securely connect to (network configuration). In the setup window, the server address, mask, port range, KX mode, media type, and key file can be changed.
- User certification: facilitates loading new users into the system, certifying their identity, adding and managing system users, and monitoring and generating reports.

3.2.4 Client User Role

The User role includes the storage, generation of keys and configuration of the PrivateWire Client application. Client User services and configuration files include:

- TCP Configuration: For convenience, organizations can pre-define the applications/servers that require security. This configuration file can be created and provided to the user on the distribution media.
- Registry Parameters: These parameters can be configured to ensure easier installation and use of the Client application. Some of these parameters include disabling key-generation menu options, disabling window pop-ups in certain situations (anonymous), installation for software only.

- Authentication of user ID: To authenticate a User to the Client.
- Secure Session: The Client software creates secure sessions with the Gateway, and automatically prompts the user to enter his password. The user performs a local logon process using a personal password and a key media, after which a secure session is negotiated using the users private key for authentication.
- Logout: This ends the current session and enforces full authentication for later connections.
- Exit: Closes the PrivateWire client, and leaves all sessions unsecured.
- Refresh Module: update the secured site packet statistics for current connections.
- Key Info: used to view information on the currently selected key media.
- Change password: function to change the user's password. This service requires the valid password of the user and then once entered, prompts for the new password to be entered.

3.3 Physical and Software Security

The PrivateWire Gateway and Client consist entirely of software, and are tested for FIPS 140-1 compliance on a standard Personal Computer (PC). This PC has been tested and meets applicable Federal Communication Commission (FCC) Electromagnetic Interference (EMI) and electromagnetic Compatibility (EMC) requirements for business use as defined in Subpart B of FCC part 15.

PrivateWire Client is a software module and is available for users on multiple platforms including Windows 3.x, Windows 95, Windows 98, Windows NT 3.51, and Windows NT 4.0 operating systems. The PrivateWire Security Gateway is a software module and is available for users on multiple platforms including in Sun Solaris 2.5, Sun Solaris 2.51, Sun Solaris 2.6, Windows NT 3.51, and Windows NT 4.0 operating systems. PrivateWire is being tested for Level 1 physical security, which requires the use of commercial grade equipment.

The PrivateWire Client program optionally supports the use of Smartcard devices where hardware security is desired. Combining cryptographic session security, firewall technology and optional Smartcards and security hardware, PrivateWire provides the highest level of security available for organizations communicating with thousands of remote users.

PrivateWire software is written in the C and Visual C++ languages. As part of the FIPS 140-1 evaluation Algorithmic Research's Proprietary source code was tested by an independent testing laboratory to ensure correct design, implementation and conformance. The PrivateWire software is installed as executable code to discourage scrutiny and modification as required from FIPS, and is a single-user software module.

The Finite State Machine models for the PrivateWire Client and Gateway were independently evaluated and are described in the FIPS 140-1 Proprietary Finite State Machine model document.

3.4 Cryptographic Algorithms

Algorithmic Research's efficient implementation of standard cryptographic algorithms ensures the highest level of interoperability for both Client and Server. In addition, Algorithmic Research's implementations provide some of the fastest system performance available in software.

The PrivateWire Client implements the following FIPS-approved algorithms:

- Data Encryption Standard (DES) (in Output Feedback (OFB) mode) (FIPS 46-2)
- Triple DES (3DES) (in OFB and Cipher Block Chaining (CBC) modes) (FIPS 46-2)
- Secure Hash Algorithm (SHA-1) (FIPS 180-1)
- Digital Signature Standard (DSS) with SHA-1 (FIPS 186-1)

In addition, the PrivateWire Client provides the following non FIPS-approved algorithms

- RSA Digital Signatures (with ISO9796)
- Rivest Code 4 (RC4) with 128 bit-keys

- Message Digest 5 (MD5)
- Diffie-Hellman (DH) key exchange

3.5 Cryptographic Key Management

PrivateWire uses symmetric keys for encryption of session traffic and public-private key pairs for digital signature and key exchange. In addition, passwords are used to create password-based encryption keys for secure storage of private key information.

Session keys are established through a key agreement protocol that employs DH or RSA key exchange depending on the user's selected algorithm (RSA or DSS). Messages passing between a Client and security Gateway are encrypted using these session keys. Data integrity and authenticity is also ensured with a cryptographic checksum using the SHA-1 algorithm (or MD5 for RSA users) Each message includes a fingerprint protected with the session key. This provides each connection with confidentiality and data integrity, encrypting all TCP/IP data streams while ensuring that communications remain fully routable.

Public-private key pairs are created for users, crypto-officers and each Gateway. Public keys are certified and stored in certificates. The Security Gateway may have up to two private keys: an RSA private key whose public key is certified by the vendor's RSA certifying authority and another DSA, certified by the DSA certifying authority. Each user creates an RSA or DSS key pair, with the public key certified by the appropriate certifying authority. To operate in a FIPS 140-1 compliant mode, users must select DSS keys.

DSS and RSA keys are used for authentication (digital signatures) and key exchange using Diffie Hellman and RSA respectively. The protocol variant is automatically selected according to the user's private key type.

3.5.1 Generation of keys:

Public and private keys are generated locally on the user's machine using the PrivateWire Client. Private keys are not transferred over the network or exported by the module, and are stored locally on the hard drive to reduce exposure. Furthermore, private keys are stored in Ciphertext, encrypted with a user's password. Key files have the extensions ".pri" (private) and ".pub" (public). User IDs are included in plaintext in these files for identification and differentiation by PrivateWire software. These files can be deleted in case the need arises for manual destruction of keys.

Keys are internally generated; however, PrivateWire optionally offers the use of three types of key media for the storage of keys.

- KeyFile: PrivateWire encrypts the private keys and stores them in a KeyFile that resides on the user's hard drive.
- KeyDiskette: With this option, keying information is encrypted and stored on a specially-formatted diskette, allowing a user to separately secure private keys.
- PrivateCard: Keying information is encrypted and stored in a smartcard's embedded chip, adding hardware protection to PrivateWire.

Symmetric keys are generated for each session as a DES, triple DES, or RC4 session key. These keys are generated using a key exchange protocol, and then used to encrypt any further communication within the session as follows:

For a new connection, after a successful authentication, the Client and Gateway construct a 128-bit master session key using either, a hash of a 1024 bit shared DH session key, or a hash of partial keys created by Client and Gateway in an RSA key exchange protocol. A session key is then derived from this master session key using triple DES and connection information.

3.5.2 *Key Lifetime and Destruction*

The PrivateWire module does not use key archiving, automatically destroys session keys, and stores private keys in encrypted format.

Session keys are ephemeral, and are deleted once the session key lifetime has expired, or the session is terminated by the user or administrator. Subsequent connections require generation of a new session key from the master session key. The security gateway maintains a cache where the master session key is mapped to the user's certifier public key. The Crypto-Officer can define the lifetime of this master session key. The security gateway automatically deletes expired master session keys from the cache, forcing establishment of new master session keys. The Client also has a cache of recently accessed servers and master session keys which are destroyed if the Client Software is reloaded or the user logs out of a session.

Private keys are stored in encrypted form, and never as plaintext critical security parameters and hence do not need to be destroyed. However, the user has the option of manually destroying their public and private keys by locating the file on their local directory and physically destroying the file.

3.6 Self-Tests

The client application includes several tests to ensure the integrity and correct operation of the module as required by FIPS. These include the following:

The PrivateWire software module includes the following self-tests to ensure the integrity and correct operation of the module. These include the following:

- PrivateWire module Software/firmware test
- DES Encrypt Cryptographic Algorithms Known Answer Test
- DES Decrypt Cryptographic Algorithms Known Answer Test
- 3-DES Encrypt Cryptographic Algorithms Known Answer Test
- 3-DES Decrypt Cryptographic Algorithms Known Answer Test
- Continuous Random Number Generator
- Software/firmware test
- Pair-wise consistency test
- Critical functions test (client only)