Algorithmic Research

Algorithmic Research
PrivateServer

FIPS 140-1 Non-Proprietary Security Policy

Level 3 Validation

October, 2002

Table of Contents

1 INTRODUCTION

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Algorithmic Research PrivateServer. This security policy describes how the PrivateServer meets the security requirements of FIPS 140-1, and how to operate the PrivateServer in a secure FIPS 140-1 mode. This policy was prepared as part of the level 3 FIPS 140-1 certification of the PrivateServer.

FIPS 140-1 (Federal Information Processing Standards Publication 140-1 -- *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-1 standard and validation program is available on the NIST web site at http://csrc.nist.gov/cryptval/.

1.2 References

This document deals only with operations and capabilities of the PrivateServer in the technical terms of a FIPS 140-1 cryptographic module security policy. More information is available on the PrivateServer and other Algorithmic Research products from the following sources:

- Algorithmic Research web site contains information on the full line of security products at www.arx.com.
- For answers to technical or sales related questions please refer to the contacts listed on Algorithmic Research site at www.arx.com .

1.3 Terminology

In this document the Algorithmic Research PrivateServer is referred to as the module, the device, the PrivateServer, or the PSV.

1.4 Document Organization

The Security Policy document is part of the complete FIPS 140-1 Submission Package. In addition to this document, the complete Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Module Software Listing
- Other supporting documentation as additional references

This document provides an overview of the PrivateServer and explains the secure configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the PrivateServer. Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

This Security Policy and other Certification Submission Documentation was produced by Corsec Security, Inc. under contract to Algorithmic Research. With the exception of this Non-Proprietary Security Policy, the FIPS 140-1 Certification Submission Documentation is Algorithmic Research-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Algorithmic Research.

2 The PrivateServer

The Algorithmic Research PrivateServer is a high-performance cryptographic service provider. Contained within a secure, tamper-responsive steel case, the PrivateServer performs high-speed cryptographic operations while protecting sensitive data. All keys and critical security parameters are protected within the cryptographic boundary by the physical security mechanisms of the module.

The PrivateServer supports various cryptographic algorithms including Triple-DES for encryption and SHA-1 for hashing. It can be used to securely store secret/private keys and has the ability to maintain an internal public key database. The PrivateServer performs all cryptographic operations internally, and through self-tests, it ensures that these operations are functioning correctly. There is no room for error when protecting mission critical data.

Whether performing the backend cryptography for a high-volume e-Commerce site or just providing authentication services for a small company, the PrivateServer satisfies the need with its wide-range of cryptographic functionality. It includes the following features:

- Strong cryptography using DES, Triple-DES, RSA, and SHA-1
- Public key database and certificate support
- Authenticated and encrypted communication with the module
- Secure storage of secret/private keys
- Software key medium and smartcard support
- Tamper-responsive enclosure
- High level API requiring no cryptographic expertise
- In-depth logging and auditing
- Secure backup capabilities

2.1 Secure by Design

The PrivateServer is a multi-chip standalone module. It has been evaluated as meeting all of the Level 3 FIPS 140-1 requirements. This means the module provides strong security both inside and out. Encased within a tamper-responsive and tamper-evident steel box, the module both protects against and reacts to attacks. Access to the module is only permitted through specific, well-defined interfaces detailed in the following section (2.2).

The PrivateServer Master Key is used to generate diversified keys, and one of these diversified keys is used to encrypt sensitive data stored in non-volatile memory. The PrivateServer Master Key is stored on the smartcards used to start the module. This key is loaded into the PrivateServer's volatile memory during startup and erased from memory when the module is terminated. The complete PrivateServer Master Key is never stored internally on non-volatile media.

The security features of the module ensure that access to sensitive information is granted only to authorized operators. Intrusion attempts cause power to be instantly cut off, preventing access to any useful information by zeroizing all plaintext critical security parameters including the PrivateServer Master Key and diversified keys. Without these keys, it is not possible to start the PrivateServer or to access the module's stored data.

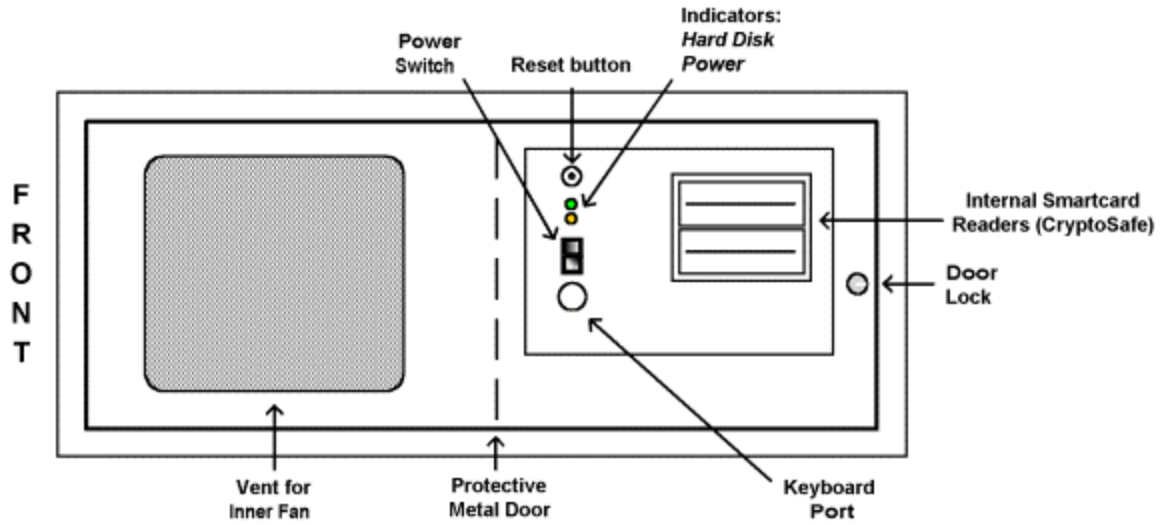
The units are encased in a solid metal case rigged with micro-switches and only the specified physical interfaces permit access to the module. Multiple tokens (including smartcards and passwords) are required to power-up the module, and all management services must be carried out through a secure session.

After a power failure or shutdown, smartcard tokens and passwords are required to power-up the module. After a detected tamper, the rack mountable box must be re-initialized with a special initialization smart card.

The adapter meets FCC requirements in 47 CFR Part 15 for personal computers and peripherals designated for home use (ClassB), and is labeled in accordance with FCC requirements.

2.2 Well-Defined Interfaces

The module is a hard, rack mountable box (Figure 1). The physical interfaces include the power connector, secure/unsecure network connections (Ethernet Interfaces using TCP/IP and UDP/IP), key slots, power switches, indicators, a monitor port, a keyboard port, and smart card readers. The module is encased in a steel cover, with only the specified interfaces providing access to the module. All ports use standard PC pin outs.



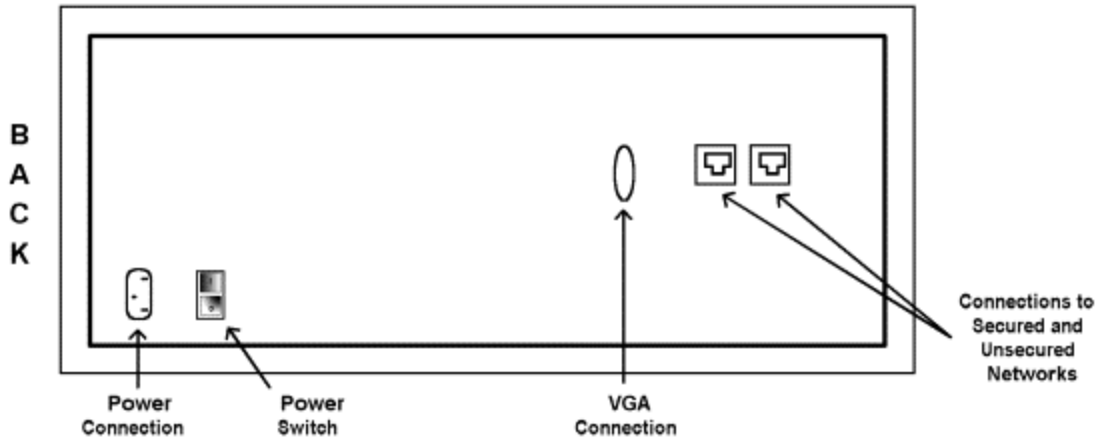


Figure 1 – Front and Rear Interfaces

For FIPS 140-1 purposes, both network ports are treated the same as only encrypted and authenticated session are permitted over either port when operating in a FIPS compliant manner. In a non-FIPS compliant manner, the module could be configured so that traffic over the secure Ethernet port was plaintext while traffic over the unsecure network was encrypted and authenticated.

Table 1 shows the mapping of the FIPS 140-1 logical interfaces to the module's physical interfaces.

FIPS 140-1 Logical Interfaces	**Adapter physical interfaces**
Data Input Interface	Network ports, keyboard port smartcard readers
Data Output Interface	Network ports
Control Input Interface	Network ports, keyboard port, buttons
Status Output Interface	Network ports, indicators, monitor port
Power Interface	AC power connector

Table 1 – Interfaces

All requests for cryptographic services are done through the PrivateServer API. This API, written primarily in C and based on RPC (Remote Procedure Calls), provides a high-level interface to the cryptographic services provided by the module, thus masking many of the complexities of cryptography from the developer. Figure 2 depicts this API model.

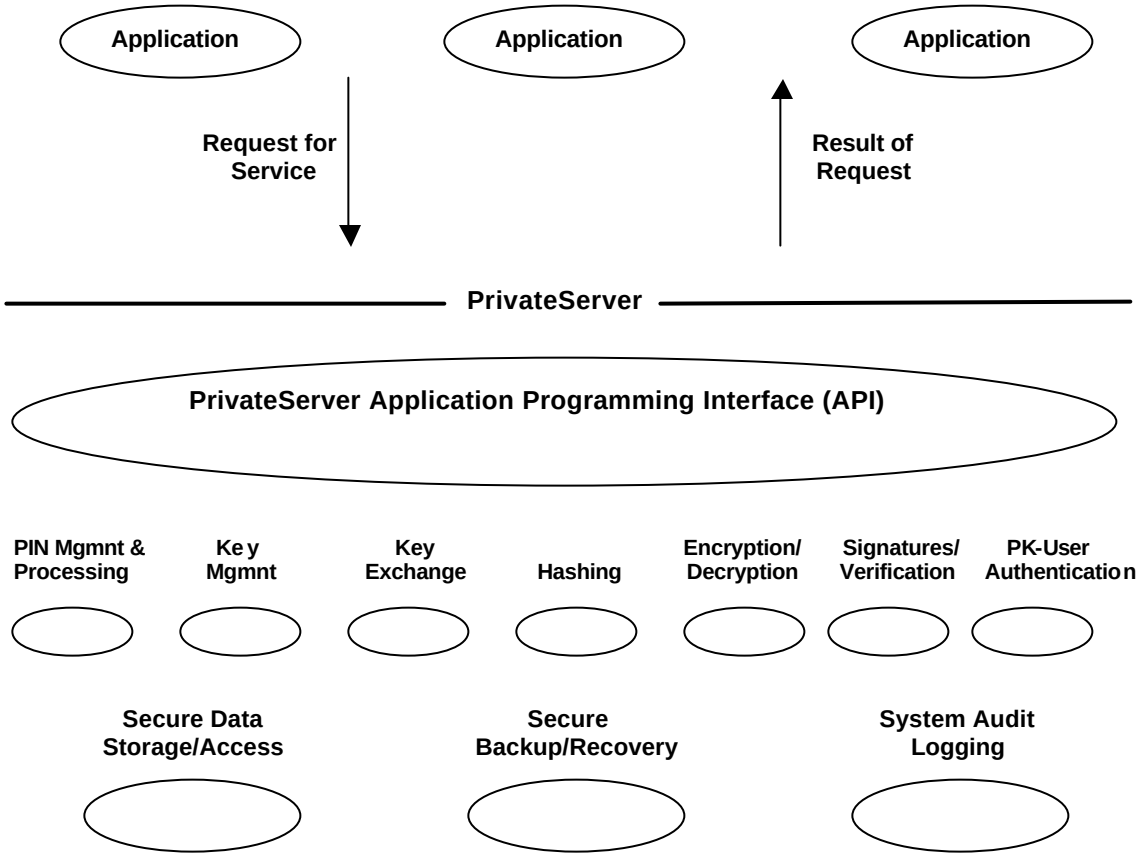


Figure 2 – PrivateServer API Model

2.3 Roles and Services

The PrivateServer employs identity-based authentication of users through the RSA challenge-response mechanism (supporting Smartcard tokens), and supports multiple, simultaneous operators. Each user has a public key and a user record that contains the user name, authorization mask, quotas for temporary keys created by the user, the certifier (CA) of the user, and the minimum access level. The authorization mask controls the actions a user can make, and the minimum access level restricts the type of session of user has to create. The session types are unauthenticated, encrypted, or both authenticated and encrypted. When operating in a FIPS compliant manner, all sessions are both authenticated and encrypted.

There are two primary roles a user can hold, User/Application and Supervisor (Crypto-Officer):

2.3.1 Supervisor (Crypto-Officer) Role

The Supervisor is responsible for user and key management, module initialization and startup, and the module's configuration. The Supervisor possesses the smartcards necessary to initialize and startup the PrivateServer. The Crypto-Officer can log into the module locally using the smartcards or remotely using the RSA challenge-response protocol. All authorization bits are turned on (ie, FFFFFFFF) for the Supervisor, providing the following functionality:

- *Delete any key (besides Special-Purpose keys)*
- *Create users*
- *Retrieve user information*
- *Retrieve information about all open sessions*
- *Retrieve all information about any key, except its value.*
- *Revoke users*
- *Perform shutdown*
- *Perform software update.*
- *Perform backup of all data in the module*
- *Restore previously backed up data*
- *Retrieve information from the log file*
- *Create a non-authenticated user.*
- *Update user records*
- *Reset the log file.*
- *Terminate a specific session.*

In addition, the Supervisor can access all cryptographic and miscellaneous services, including:

- *Symmetric cryptographic services*
- *Asymmetric cryptographic services*
- *Hashing services*
- *Authentication services*
- *Session services*
- *All management services (keys, users, etc.)*
- *All administrative services*

Locally, the Crypto-Officer has the ability to access certain management operations of the module, including:

- *Initializing the module and it's databases*
- *Starting the module*
- *Configuring the module's IP information*
- *Resetting a tamper condition*

2.3.2 User/Application Role

The User/Application is for accessing the cryptographic services provided by the module. The User logs into the module remotely using the RSA challenge-response protocol. None of the authorization bits (see 2.3.1 for the functionality listing of those bits) are turned on for the User/Application. The User can access all of the following services:

- *Symmetric cryptographic services*
- *Asymmetric cryptographic services*
- *Hashing services*
- *Authentication services*
- *Session services*

- *Key management services on keys the user owns*
- *Specific certified public-key database services*
- *Specific administrative services*

An operator who has access to the role of User/Application must first authenticate to the module, and then an encrypted, authenticated session is created. The RSA challenge-response protocol used by the module is a key distribution scheme, and this is used to authenticate the operator and to establish a temporary session key (that is destroyed at the close of the session). Through this session, the operator may perform the cryptographic services for which they have permissions.

An operator who has access to the role of Crypto-Officer must first create an authenticated, encrypted session. Through this session, the operator may perform cryptographic and management services. This operator may also login to the module locally using the startup and initialization smartcards. Before the module is initialized, access control for the Crypto-Officer role is provided through the use of default smartcards.

Table 2 provides a high-level summary of the services provided by the module.

Service	Information Summary
Key management and control	Secure storage and management of cryptographic keys (DES/Triple-DES keys, RSA public and private keys, Special-purpose keys).
Public-key database	Centralized storage and management of public keys (RSA public keys).
Data encryption and decryption	Symmetric [DES, Triple-DES (CBC and ECB modes are FIPS approved, Stream mode is not FIPS approved)] and Asymmetric Cryptography (RSA – not FIPS approved).
Digital signatures	Generate and verify digital signatures (RSA).
Data hashing	Generate message digests [SHA-1 (FIPS 180-1) and MD5 (not FIPS approved)].
User authentication	Two-way user authentication using the RSA challenge-response key distribution mechanism. A smartcard token can be used.
Logging, auditing, administration, and management	Administrative and management operations as well as logging and auditing.
Internal real-time clock	Used for accurate time stamps.

Table 2 – Service and Description

2.4 Strong Cryptographic Algorithms and Secure Key Management

The PrivateServer supports a variety of strong cryptographic algorithms, and implements these algorithms based on the cryptographic standards. It provides the following FIPS-approved algorithms:

Data Encryption

- DES (FIPS 46-2) in ECB and CBC modes – 64 bits
- Triple-DES (ANSI X9.52) in ECB and CBC modes – 128 bits, 196 bits

Data Packet Integrity

- DES-MAC (FIPS 113) – 64 bits
- Triple-DES-MAC - 128 bits, 196 bits

Message Digest

- SHA1

Authentication

- RSA Digital Signatures
- RSA Challenge-Response Key Distribution Scheme

The PrivateServer stores the private/secret keys in a key database. This database is stored encrypted (with Triple-DES) on the PrivateServer's internal hard drive. Within the key database, keys have properties associated with them. These properties determine which operations may be performed on a particular key and establish which users are authorized to carry out these operations.

There are two levels of access to the keys stored on the module, Owner and User. The Owner of a key can perform all operations on the key and can grant or revoke key access rights to other entities. The User of a key may access it for cryptographic operations only and is not able to read the key or perform administrative functions on it. Keys can be read-locked so that even key owners cannot read the key (either in plain or encrypted form).

The Special-Purpose keys, used internally by PrivateServer, are not accessible for general cryptographic operations. These keys include the customer's organization-wide root public key, PrivateServer's RSA private/public key pair, the PrivateServer Master Key, and the PrivateServer Master Key diversified keys.

Public keys and certificates stored in the public key database are accessible through the anonymous services (anonymous services are disabled when operating in a FIPS compliant manner). Certificates loaded onto the module must be signed by the organization's private key and this signature is verified before addition to the public key database.

In the FIPS compliant mode of operation, all operator sessions are authenticated and encrypted so that no secret or private keys are passed in or out of the module unprotected. The module also provides the ability to back up the key database in encrypted form.

2.5 Self Testing

The PrivateServer monitors firmware operations through a set of self-tests to ensure proper operation in accordance with FIPS 140-1. The module includes the following self-tests:

Hardware Tests: When power is first applied to the module, the hardware performs a series of checks to ensure it is functioning properly.

Firmware Integrity Test: After the hardware tests, the module performs RSA digital signature verification to ensure firmware has not been modified.

Cryptographic Algorithm KATs: Known Answer Tests (KATs) are run at power-up for the DES and Triple DES encryption/decryption, and Message Authentication Codes.

- **DES-CBC and DES-ECB KAT**
- **Triple-DES-CBC and Triple-DES-ECB KAT**
- **DES-MAC KAT**
- **Triple-DES-MAC KAT**
- **SHA-1 KAT**

RSA Pairwise Consistency Test: All RSA operations are tested to ensure the correct operation of the RSA key generation, encryption/decryption, and signatures.

Statistical Random Number Generator Test: This test runs a monobit test, poker test, runs test, and long run test to verify the correct operation of the random number generator.

Continuous Random Number Generator Test: This test is constantly run to detect failure of the random number generators in the PrivateServer.

Firmware Upgrade Test: Module firmware can only be remotely upgraded from the management system with proper authentication to the module. However, in order to strictly control the loading of new firmware to the PrivateServer, the new firmware must be digitally signed by Algorithmic Research.

3 FIPS 140-1 Level 3 Compliant Mode

The module is shipped with either a FIPS or non-FIPS configuration file. This is as requested by the customer at the time of purchase. In order to switch a module to a FIPS configuration file, a configuration file signed by Algorithmic Research must be loaded onto the module. Once this configuration is accepted, the module is shutdown and restarts using that configuration file.

When operating with a FIPS configuration file, certain functionality is unavailable. The anonymous functions, non-FIPS compliant PrivateServer certificates, and non-FIPS compliant challenge-response mechanism are all disabled.

For FIPS 140-1 compliance, the session type for both Users and the Crypto-Officer must be set to 3 (ie, ACC_AUTHEN - authenticated and encrypted session) as depicted in Table 3. This can be set using the management utility provided by Algorithmic Research (mng.exe) or API calls. The CO's authorization mask is FFFFFFFF, and the User's authorization mask is 00000000. These can be set using the Algorithmic Research management utility provided or API calls.

Session / Role	Non-Authenticated Session	Encrypted And Authenticated Session
User/ Application	No	Yes
Supervisor (Crypto-Officer)	No	Yes

Table 3 - Roles vs. Session Type

Cryptographic services should only use FIPS-approved algorithms. A list of these algorithms can be found in section 2.4.

There can be only one individual holding the role of Crypto-Officer. Only the Crypto-Officer may possess the smartcards and passwords necessary to initialize and startup the module.