Algorithmic Research

ARX (Algorithmic Research)
PrivateServer

FIPS 140-2 Non-Proprietary
Security Policy

Level 3 Validation

February 2007

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 140-2, and how to operate the PrivateServer in a secure FIPS 140-2 mode. This policy was prepared as part of the level 3 FIPS 140-2 validation of the PrivateServer.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 -- *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 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 140-2 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 or the PrivateServer.

1.4 Document Organization

The Security Policy document is part of the FIPS 140-2 Submission Package. In addition to this document, the 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 140-2-mode of operation.

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation 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:

- Cryptography using DES, Triple-DES, AES, DES-MAC, Triple-DES-MAC, RSA, SHA-1, SHA-256 and SHA-512. (DES and DES-MAC are for legacy use and transitional phase only - valid until May 19, 2007)
- 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. PrivateServer hardware version 4.0 with firmware version 4.2 has been designed to meet all of the Level 3 FIPS 140-2 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 security features of the module ensure that access to sensitive information is granted only to an authorized operator. Tamper seals provide evidence of any attempt to tamper with module cover. The tamper seals are placed over a screw that joins the top cover and bottom enclosure.

The units are encased in a solid metal case rigged with micro-switches and only the specified physical interfaces permit access to the module. 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 Critical keys. Without these keys, it is not possible to

start the PrivateServer or to access the module's stored data. 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 module meets FCC requirements in 47 CFR Part 15 for personal computers and peripherals designated for home use (Class B). It is labeled in accordance with FCC requirements.

2.2 Well-Defined Ports

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

The ports are shown in Figure 1. On the front of the module behind the access door you have a smart card reader in the top middle. Below that, from left to right, you have an on/off button, keyboard port, and three indicator lights. On the back of the module, left to right, you have the power connector and power switch below the fan and the monitor port and two network connections on the top right. These ports are all listed in table 1.

Figure 1 – Front and Rear Interfaces

For FIPS 140-2 purposes, both network ports are treated the same as only encrypted and authenticated sessions are permitted over either port when operating in a FIPS 140-2 compliant manner. In a non-FIPS 140-2 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 140-2 logical interfaces to the module's physical interfaces.

FIPS 140-2 Logical Interfaces	**Adapter physical interfaces**
Data Input Interface	Network ports, keyboard port smartcard reader
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.

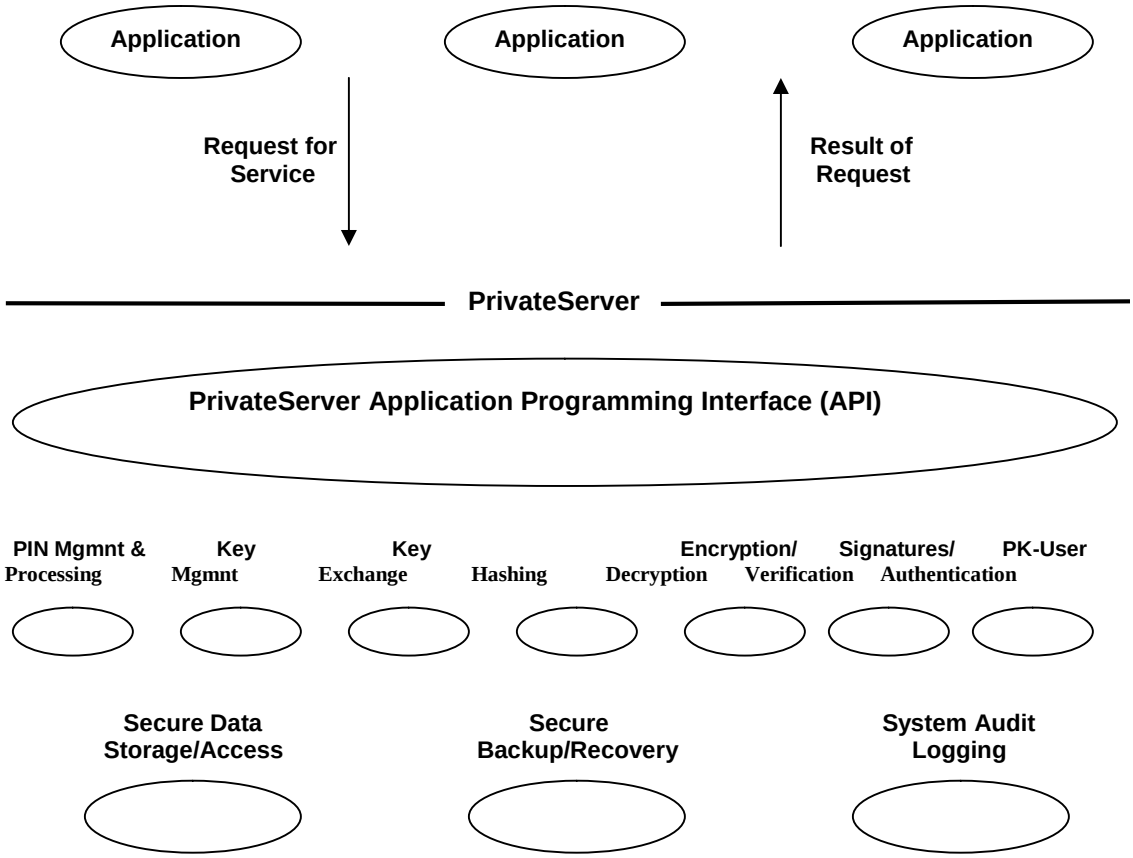

Figure 2 – PrivateServer API Model

2.3 Roles and Services

The PrivateServer supports multiple, simultaneous operators. A database record entry is created by the PrivateServer for each operator and contains the operator name, authorization bits, quotas for operator temporary keys created by the operator, the certifier (CA) of the operator, and the minimum access level. The authorization mask controls the operator's permissions.

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

2.3.1 Supervisor (Crypto-Officer) Role

The Supervisor is responsible for operator and key management, module initialization and startup, and the module's configuration. All authorization bits are turned on (i.e., 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.)*
- *Administrative services*

There can be only one individual holding the role of Supervisor. Only the Supervisor may possess the smartcards and passwords necessary to initialize and startup the module. This must be done locally, using the PrivateServer smartcard reader and a keyboard attached to the module. No other operator that can authenticate using this local interface. By connecting directly through the PrivateServer, the Supervisor 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 through s device that communicates with the PrivateServer application program interface 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, the User can only access the following services:

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

A User 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, 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.

The session keys (MAC and encryption/decryption) are negotiated during authentication of a user when creating a session. The PrivateServer creates these keys during the opening of an encrypted session, and they are destroyed when the session is terminated. These keys are temporary and are only stored in volatile memory.

2.3.3 Authentication

The PrivateServer employs identity-based authentication of operators through the RSA challenge-response mechanism. The RSA challenge-response mechanism requires the exchange and verification of the operator's private key. All keys used for authentication are private keys generated externally and certified by a CA signature. The probability that random access will succeed is far less than one in 1,000,000 attempts using this authentication mechanism. In addition, the authentication provides 1 in 2^161/(1000*60) probability of a successful random attempt during a one-minute period.

The Supervisor possesses the smartcards and password necessary to initialize and startup the PrivateServer. The Supervisor can log into the module locally using the smartcards or remotely using the RSA challenge-response protocol. A Supervisor attempting to authenticate directly to the module through the keyboard port must use the startup smart card and password. The password must be at least 6 alphanumeric characters. This yields a minimum of 36^6 (over 1,000,000,000) possible combinations. Therefore the possibility of correctly guessing a password is less than 1 in 1,000,000. After fourteen failed authentication attempts the startup smartcard is locked and hence the possibility of randomly guessing a password in 60 seconds is less than 1 in 100,000. The module also suppresses feedback of authentication data being entered by returning '*' characters.

2.3.4 Services

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/AES 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, AES (CBC and ECB modes are FIPS 140-2 approved, Stream mode is not FIPS 140-2 approved and not relevant for AES)] and Asymmetric Cryptography (RSA – not FIPS 140-2 approved).
Digital signatures	Generate and verify digital signatures (RSA). The digital signature generation supports the following schemes: PKCS#1 v1.5, PSS and ANSI X9.31. Also, digital signature verification service is supported based on the above algorithms.
Data hashing	Generate message digests [SHA-1, SHA-256 and SHA-512 (FIPS 180-2) and MD5 (not FIPS 140-2 approved)].

User authentication	Two-way user authentication using the RSA challenge-response key distribution mechanism. A smartcard token can be used for local access by the Supervisor.
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

Table 3 shows each specific service and which role has access to it.

SERVICES	**ROLE**
Delete any key	CO
Create users	CO
Retrieve user information	CO
Retrieve information about all open sessions	CO
Retrieve al information about any key, except its value	CO
Revoke users	CO
Perform shutdown	CO
Perform software update	CO
Perform backups	CO
Restore backups	CO
Retrieve log file	CO
Create a non-authenticated user	CO
Update user records	CO
Reset the log file	CO
Terminate a session	CO
Symmetric cryptography	CO/User
Asymmetric cryptography	CO/User
Hashing	CO/User
Authentication	CO/User
Session	CO/User
Management (keys, users, etc.)	CO/User
Administrative	CO/User

Table 3 – Role Access to each Service

2.4 Cryptographic Algorithms and Secure Key Management

The PrivateServer supports a variety of cryptographic algorithms, and implements these algorithms based on the cryptographic standards. It provides the following FIPS 140-2-approved algorithms:

Data Encryption

- DES (FIPS 46-3) in ECB and CBC modes – 64 bits (Transitional phase only - valid until May 19, 2007; Cert. #331))
- Triple-DES (ANSI X9.52) in ECB and CBC modes – 128 bits, 192 bits; Cert. #409
- AES (FIPS PUB 197) in ECB and CBC modes – 128 bits, 192 bits and 256 bits; Cert. #349

Data Packet Integrity

- DES-MAC (FIPS 113) – 64 bits (Transitional phase only - valid until May 19, 2007; Cert. #331)
- Triple-DES-MAC - 128 bits, 196 bits; Cert. #409

Message Digest

- SHA1; Cert. #424
- SHA256; Cert. #424
- SHA512; Cert. #424

Random Number Generator

- FIPS 186-2; Cert. #185

Authentication

- RSA Challenge-Response Key Distribution Scheme
- Password Authentication (Supervisor with local access only)

Key Establishment

- RSA (key wrapping; key establishment methodology provides 80 bits of encryption strength)

Digital Signature Generation Algorithms (RSA Based)

- PKCS#1 v1.5
- PSS
- ANSI X9.31

Digital Signature Verification Algorithms (RSA Based)

- PKCS#1 v1.5
- PSS
- ANSI X9.31

Non Approved Algorithms:

1. MD5
2. ISO9796
3. ARDFP (an Algorithmic Research proprietary hashing algorithm)
4. DES Stream (non-compliant)

The PrivateServer stores all non-volatile keys in the database. The database is stored encrypted (with Triple-DES) on the PrivateServer's internal hard drive. Within the 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. This should not be confused with the User Role as both levels of access are applicable to the User or Supervisor Role. 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.

User Keys are keys that are generated upon request or inputted by the user for various key operations. User keys consist of two types of keys: User Normal Keys, and User Temporary keys. Users choose what type of key they want to create or input. Users can generate or input any of the following key types: DES 64 bit keys, TDES 128 and 192 bit keys, AES 128, 192 and 256 bit keys, RSA 1024, 2048, and 4096 bit keys. The only difference is that a User Normal key can be reused whereas a User Temporary key cannot. User Normal keys are stored in memory and then written to the database before the close of a user session. User Normal keys can be reloaded by the user for a new user session. User Temporary keys are only stored in memory and are erased upon close of a user session.

2.4.1 Initial Configuration

The PrivateServer has three 2-key TDES Critical keys externally generated. One half of each of the Critical keys is stored on the Startup smartcard and the other three halves are stored on the Initialization smart card. The Critical keys are then created by XORing the split keys from the Startup smart card and Initialization smart card and loading the result into the PrivateServer's volatile memory during startup. These keys are only stored in volatile memory. All three keys are erased from memory when the module is terminated.

The three critical keys are used for the following internal operations:

- Encrypting key values in the keys database
- Encrypting the database during a backup operation
- Checking the integrity of database records using a MAC key.

The Special-Purpose keys are only used for internal operations on the PrivateServer. These keys include the customer's organization-wide root public key, PrivateServer's RSA private/public key pair, the PrivateServer critical Keys, and the PrivateServer key for continuous operations context encryption.

Public keys and certificates stored in the public key database are inaccessible through the anonymous services (anonymous services are enabled when operating in non-FIPS 140-2 compliant mode). 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 140-2 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.

Table 4 provides a list of all the keys, their key types, and access control.

Cryptographic Keys and CSPs	**Key Type**	**ACCESS (R/W/X)**
Software Key	TDES 128 bit key, FIPS 46-2	X
Critical Key for key value encryption of database keys	TDES 128 bit key, FIPS 46-2	X
Critical Key for Backup encryption	TDES 128 bit key, FIPS 46-2	X
Critical Key for database Record MAC calculation	TDES 128 bit key, FIPS 46-2	X
Key for continuous operations context encryption	TDES 128 bit key, FIPS 46-2	X
PrivateServer RSA Public/private key pair	RSA 1024 bit key	X
Organization Root Public Key	RSA 1024 bit key	W,X
Algorithmic Research/ AR RSA public key	RSA 1024 bit key	X
Session encryption/decryption keys	TDES 128 bit keys, FIPS 46-2	X
Session MAC keys	TDES 128 bit key, FIPS 46-2	X
User keys – (Two types: user Normal keys and user Temporary keys.)	Multiple key types: DES 64 bit keys, TDES 128 and 192 bit keys, AES 128, 192 and 256 bit keys, RSA 1024, 2048, and 4096 bit keys	X,R
Public key certificates	RSA 1024, 2048 and 4096 bit public keys stored in certificates	X,R
User Authentication	Authentication of operators uses RSA challenge-response mechanism. Authentication provides 1 in 2^161/(1000*60) probability of a successful random attempt during a one-minute period.	X
Password Authentication	At least 6 alphanumeric characters long. Yields a minimum of 36^6 (over 1,000,000,0000) possible combinations.	X

Table 4 – Keys, Key Types, and Access

2.5 Self Testing

The PrivateServer monitors firmware operations through a set of self-tests to ensure proper operation in accordance with FIPS 140-2. The module includes the following self-tests:

Power-Up Self Tests:

Low-Level 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, Triple DES and AES encryption/decryption, Message Authentication Codes and Hash Algorithms.

DES-CBC and DES-ECB KAT
Triple-DES-CBC and Triple-DES-ECB KAT
AES128, AES192, AES256 CBC and ECB KAT
DES-MAC KAT
Triple-DES-MAC KAT
SHA-1 KAT
SHA-256 KAT
SHA-512 KAT
RNG KAT

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

Conditional Tests:

RSA Pairwise Consistency Test: All RSA operations are tested to ensure the correct operation of the RSA key generation, encryption/decryption, and signatures.
Continuous RNG Test: This test is constantly run to detect failure of the RNG.
Firmware load 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. The load of a firmware update takes place using RSA signatures. The successful load of this update would render the module non FIPS validated unless the update has also been validated.

2.6 Mitigation of Other Attacks:

The PrivateServer does not include any mechanisms to prevent against special attacks.

3 FIPS 140-2 Level 3 Approved Mode

The module is shipped with either a FIPS 140-2 approved or non-approved mode. This is as requested by the customer at the time of purchase. In order to switch a module to a FIPS 140-2 approved mode, 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 in an approved mode, certain functionality is unavailable. The anonymous functions, non-FIPS 140-2 compliant PrivateServer certificates, and non-FIPS 140-2 compliant challenge-response mechanism are all disabled.

For FIPS 140-2 compliance, the session type for both Users and the Supervisor must be set to 3 (i.e., ACC_AUTHEN - authenticated and encrypted session) as depicted in Table 3. This can be set using management utilities, GMNG and MNG, provided by Algorithmic Research (mng.exe or gmng.exe) or through 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 5 - Roles vs. Session Type

Cryptographic services shall only use FIPS 140-2-approved algorithms. A list of these algorithms can be found in section 2.4.

The FIPS mode is displayed in the title of the GMNG utility after the Crypto Officer is connected securely to the PrivateServer. It is also displayed in the server->properties dialog of the GMNG utility.

3.1 Module Inspection:

The cryptographic officer must perform a scheduled inspection of the module to detect tamper evidence. The cryptographic officer shall inspect three areas for tamper evidence:

1. The cryptographic officer shall inspect both of the tamper seals, which are located on the back of the module.
2. The cryptographic officer shall check the module's front physical interfaces that are located behind the module's front door.
3. The cryptographic officer shall remove the front ventilation cover to check for tamper evidence behind it.