Lucent Technologies
Bell Labs Innovations

# Brick 201

# FIPS 140-1 Non-Proprietary Security Policy

**Version 4.0**

**Level 2 Validation**

**February 20, 2003**

# Table of Contents

# 1 INTRODUCTION

## *1.1 Purpose*

This is a non-proprietary Cryptographic Module Security Policy for the Brick 201 from Lucent Technologies. This security policy describes how the Brick 201 meets the security requirements of FIPS 140-1, and how to operate the Brick 201 in a secure FIPS 140-1 mode. This policy was prepared as part of the Level 2 FIPS 140-1 validation of the Brick 201.



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 website at http://csrc.nist.gov/cryptval/.

## *1.2 References*

This document deals only with operations and capabilities of the Brick 201 in the technical terms of a FIPS 140-1 cryptographic module security policy. More information is available on the Brick 201 and the entire Brick series from the following sources:

1. The Lucent Technologies website (www.lucent.com) contains information on the full line of products from Lucent Technologies.

2. The NIST Validated Modules website (http://csrc.ncsl.nist.gov/cryptval/): contains contact information for answers to technical or sales-related questions for the Brick 201

## *1.3 Document Organization*

The Security Policy document is one document in a 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 Security Policy and other Certification Submission Documentation were produced by Corsec Security, Inc. under contract to Lucent. With the exception of this Non-Proprietary Security Policy, the FIPS 140-1 Certification Submission Documentation is proprietary to Lucent and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Lucent.

## 2 The Brick 201

The Brick 201 is a carrier-grade integrated firewall and virtual private network (VPN) gateway appliance specifically designed for web/application data center security, large-scale managed security services, and remote access VPN services. Called the Brick because of its rugged, reliable design, this is an ideal platform for service providers seeking wide scalability, ready manageability, and industry-leading performance. Its next-generation capabilities include full 1-Gigabit throughput, VLAN support with security policy filtering, and high availability with state-sharing. The Brick 201 can be deployed in a variety of configurations to support the business goals of large service providers.

The Brick 201 VPN Firewall supports the following features:

- Dynamic stateful packet filter with content security proxies for command blocking, URL blocking, virus scanning.
  - IPSec ESP with DES, 3DES, RC4 encryption.
  - MD5 and SHA1 authentication.
  - Operates as a layer 2 bridge, making it completely invisible in the network.
  - Runs on Bell Labs' Inferno® operating system.
- Superlative performance for enterprise-class requirements - supports up to 350 Mbps cleartext firewall throughput at 55,000 packets per second, 90 Mbps 3DES throughput.
- Feature-rich VPN platform – Each Brick 201 provides concentration support for up to 3,000 concurrent encrypted VPN tunnels and 100,000 simultaneous connections with complex security policies.
- Industry-leading scalability.
- "No-touch" CPE - advanced capabilities for remote deployment and management.
- Easy, economical administration and maintenance - requires no costly routing configuration changes, OS upgrades and patches, or hard-drive backups.
- Denial-of-service protection - defends against attacks with SYN flood protection, intelligent cache management, robust fragment reassembly.
- Supports 801.1Q VLAN tagging - allows a Brick 201 to be partitioned into as many as 200 "virtual firewalls", while ensuring that each customer's unique firewall service is completely secure.

The Brick 201 comes in two different FIPS 140-1 configurations:

- VPN Firewall FIPS 140-1 Model 201 Basic (SKU 300546884) [4-10/100 Ethernet Ports, Internal AC Power Supply, Internal Floppy Drive, FIPS-140 Hardware Kit]
- VPN Firewall Brick Model 201 VPN (SKU 300546892) [4-10/100 Ethernet Ports, Internal AC Power Supply, Installed Encryption Accelerator Card, Internal Floppy Drive, FIPS-140 Hardware Kit]

The following diagram depicts the robust system architecture, including the Lucent Brick 201, the Lucent Security Management Server (LSMS), and remote users.

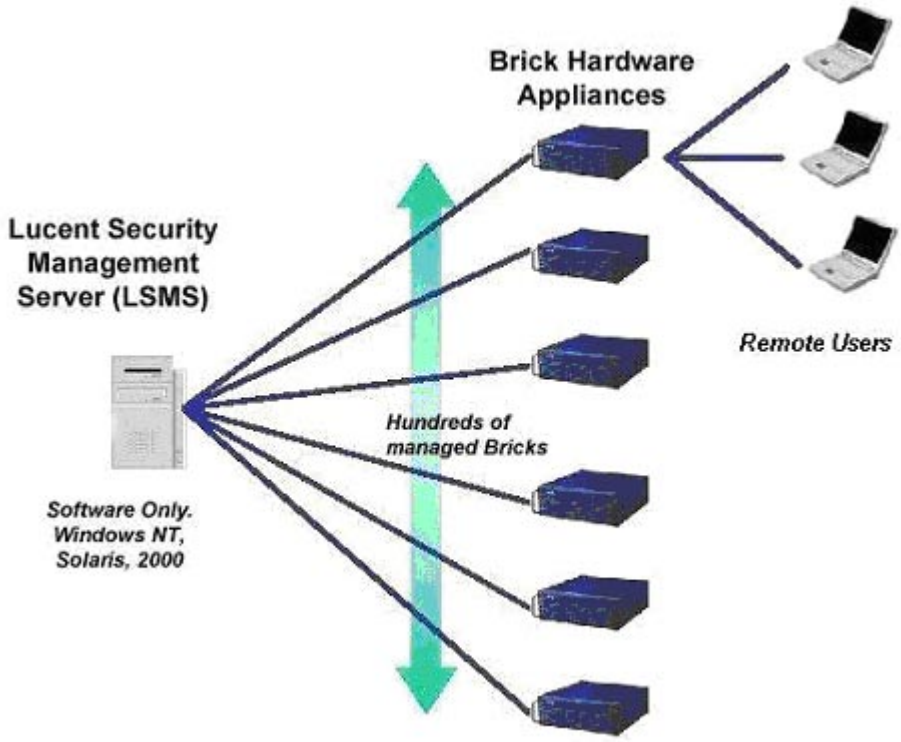


**Figure 1 – Brick 201 System Architecture**

### *2.1 Cryptographic Modules*

The metal casing that fully encloses the module establishes the cryptographic boundary for the VPN Firewall, all the functionality discussed in this document is provided by components within the casing. The Brick 201 features remote access VPNs, 20,000 simultaneous IPSec tunnels, distributed DoS attack protection, 350 Mbps of cleartext firewall throughput, 90 Mbps @ 3DES max throughput with encryption acceleration card, and premium authentication services make this module an ideal platform for building managed IP services.

### *2.2 Module Interfaces*

The interfaces for the VPN Firewall are located in the rear of the box, with the exception of the I/O controller. The physical interfaces are separated into the FIPS 140-1 logical interfaces from as described in the following table:

| Physical Port | FIPS 140-1 Logical Interface |
|---|---|
| 10/100 Base-TX Ethernet Port<br>Floppy drive | Data Input Interface |
| 10/100 Base-TX Ethernet Port | Data Output Interface |
| 10/100 Base-TX Ethernet Port<br>Power Switch<br>PS/2 Keyboard Port | Control Input Interface |
| SVGA Video Port<br>LAN Port LEDs | Status Output Interface |

| Physical Port | FIPS 140-1 Logical Interface |
|---|---|
| 10/100 Base-TX Port LEDs<br>Encryption Acceleration Card LEDs<br>Power LED<br>Disk Activity LED<br>On/Off Indicator LED | |
| Power Plugs | Power Interface |

**Table 1 – FIPS 140-1 Logical Interfaces**

**The serial and USB ports on the Brick 201 are disabled.*

The module's status interfaces are located on the front and rear panels. These LEDs provide overall status of the module's operation. Descriptions for these LEDs are in Table 2 and Table 3, respectively.

| LED | Indicator | Description |
|---|---|---|
| Power Indicator | Green | Power is supplied to the Firewall and the Firewall is operational |
| | Off | The Firewall is not powered on |
| Disk Drive | Blinking Green | The disk drive is reading a disk |
| | Off | The disk drive is not in use |
| Disk Activity | Blinking Amber | The disk drive is reading a disk |
| | Off | The disk drive is not in use |
| | Off | The power supplies are on and functioning |

**Table 2 – Front panel LEDs**

The following table provides detailed information about the LEDs found on the rear panel:

**Front Panel LEDs for the Brick 201**

| LED | Indicator | Description |
|---|---|---|
| 10/100BaseTX (LNK) | Green | An Ethernet link has been established |
| | Off | No Ethernet link established |
| 10/100BaseTX (ACT) | Blinking Green | The port is transmitting or receiving data |
| | Off | No data is being transmitted or received |
| 10/100BaseTX (100TX) | Green | The speed of the interface is 100Mbps |
| | Off | The speed of the interface is 10Mbps |
| Encryption Accelerator (Bottom LED) | Green | The Encryption Accelerator Card is powered on |
| | Off | The Encryption Accelerator Card is powered off |
| Encryption Accelerator (Middle LED) | Green | The Encryption Accelerator Card is active |
| | Off | The Encryption Accelerator Card is idle |
| Encryption Accelerator (Top LED) | Green | The Encryption Accelerator Card is active |
| | Off | The Encryption Accelerator Card is idle |
| Power Supply | Green | Power is supplied to the Firewall |
| | Off | There is no power going to the Firewall |

**Table 3 – Rear panel LEDs**

## *2.3 Roles and Services*

The Brick 201 meets level 2 FIPS 140-1 requirements for Roles and Services by employing identity-based authentication (for the LSMS and VPN client identities) and implicitly providing the authenticated identities with one of the two supported roles: Crypto-Officer role and User role.

The Brick 201 provides the LSMS identity exclusively with the Crypto-Officer role, a role responsible for the primary configuration and management of the Brick 201. The Crypto-Officer communicates with the Brick 201 through an encrypted session and authenticates to the Brick 201 using a digital certificate.

The Brick 201 provides its VPN clients exclusively with the User role. VPN clients authenticate to the Brick 201 per (network-layer) packet using a shared secret HMAC-SHA-1 key configured by the Crypto-Officer.

### *2.3.1 Crypto Officer Services*

The Crypto-Officer is responsible for the configuration and management of the Brick 201. The Crypto-Officer first provides an initial configuration for the Brick 201 and then is able to access the Brick 201 over an encrypted session. Through this session, the Crypto-Officer can perform full management of the Brick 201, including loading IPSec SAs onto the Brick 201 for Users.

During the initial configuration of the Brick 201, the Crypto-Officer generates a disk using the LSMS and this information is then loaded onto the Brick 201 over the Brick 201's floppy disk drive. The files on this disk include the following configuration information:

- Lucent Security Management Server (LSMS) certificate containing the LSMS CA DSA public key
- DSA key pair for the module (the public key is contained in a certificate generated by the LSMS)
- Diffie-Hellman public parameters
- IP address of the LSMS
- DNS Host Name given to identify the Brick 201

The Brick 201's public key (of the DSA key pair loaded onto the Brick 201) is contained in a certificate generated by the LSMS CA. Each Brick 201 is given such a unique certificate, and this is used during the LSMS handshake protocol to authenticate the Brick 201 to the LSMS. Additionally, the LSMS possesses a certificate, to allow the Brick 201 to authenticate the LSMS. Collectively, these certificates provide mutual authentication between the LSMS and every Brick 201, so an intruder cannot masquerade as either the LSMS or a Brick 201.

Once the Brick 201 has been initialized, the Crypto-Officer may begin management of the Brick 201 through a TDES encrypted IP session. Looking at Figure 1 above, the Brick 201 provides the Crypto-Officer role exclusively to the LSMS after the initial configuration is completed. Digital certificates are used to authenticate the Crypto-Officer (LSMS) to the Brick 201 and the

Brick 201 to the LSMS, and a Diffie-Hellman key agreement is performed to negotiate encrypted session keys (HMAC-SHA-1 and Triple-DES keys). After the encrypted session is established, the Crypto-Officer accesses the Brick 201's services through this session.

Through an encrypted session, the Crypto-Officer configures the module for use by IPSec clients. The Crypto-Officer loads IPSec SAs onto the module over the encrypted session, including any IPSec SA session keys. As part of these SAs, the Crypto-Officer configuration shared secret HAMC-SHA-1 keys used to authenticate the User to the module.

An operator assuming the Crypto Officer role performs all administrative functions listed below:

"begin tableload", // prepare brick for complete policy download
"begin tableadd", // prepare brick for policy download after failover
"begin load", // prepare brick for a single zone download
"sign table", // signature for complete policy download
"sign domain",// signature for a single zone download
"abort load", // stop load
"end tableload", // signal end of complete policy download
"end load", // signal end of a single zone download
"switch over", // make policy just downloaded current
"add table", // add a single zone/policy assignment
"add ethertype", // add an ethernet type to the brick
"switch ethertype", // make the pending ethernet type list active
"add dsap", // add a dsap type to the brick
"switch dsap", // make the pending dsap list active
"add route", // add a static route
"add proxy", // add a proxy (ie, for virus scanning)
"add dynamic proxy", // same, but make it active immediately
"delete dynamic proxy", //
"add rule", // add a rule to the currently loaded policy
"add dynamic rule", // same, but make it active immediately
"delete dynamic rule",//
"add mask", // add a dependency mask entry
"add hostgrp", // add a host (range) to a host group
"add dynamic hostgrp",// same, but make it active immediately
"delete dynamic hostgrp",
"add srvgrp", // add a service to a service group
"add dynamic srvgrp",// same, but make it active immediately
"set comm", // change the serial port settings (baud rate, parity)
"disable firewall", // make the firewall inactive
"reenable firewall", // activate the firewall after a disable
"refresh mac table", // allow current mac table entries to be updated once
"refresh arp table", // allow current ARP table entries to be updated once
"add ipsec", // add a single Security Association for IPSec VPN
"add dynamic ipsec", // same, but make it active immediately

"delete dynamic ipsec",

| | |
|---|---|
| "what are you", | // ask the brick what version, hardware is installed |
| "delete session", | // delete an entry from the session cache |
| "config", | // configure Intelligent Cache Management, UDP encapsulation, or NAT table features |
| "add interface", | // configure interface settings |
| "add vlanip", | // configure VLAN settings |
| "set timeoffset", | // control the brick clock |
| | |
| "read rules", | // read the current rules |
| "read table", | // read the current zone assignment table |
| "read cache", | // display certain information about session cache entries (IP address, services, # of bytes) |
| "read dominfo", | // display name and date of signer for a zone policy |
| "read tblinfo", | // display name and date of signer for zone assignment table |
| "read sas", | // retrieves some information about the Security Association, specifically , SPI, algorithm, IP addresses, TEP, timeouts. Keys are not retrievable. |
| "read hostgroups", | // retrieve contents of host groups |
| "read servicegroups", | // retrieve contents of service groups |
| "read routes", | // retrieve route list |
| "count dynamic sas", | // display count of SAs involved in IKE |
| "read minos", | // display basic info about the brick such as software version, MAC move settings, Encryption card present/active, firewall enabled. |
| "read vlans", | // display vlan info |
| "reboot" | // reboot brick |
| "failover" | // makes a failover pair of bricks switch over |
| "rehome" | // makes a brick try to connect to a particular LSMS from its list. |
| "set clock" | // sets clock |
| “memory peek” | //allows the Crypto-Officer to view the contents in memory |
| “poke show” | //allows the Crypto-Officer to write to the memory |

### *2.3.2 User Services*

The User role has access to the IPSec services of the module as a VPN client. Looking at Figure 1 above, the Brick provides the User role to the Remote Users in that diagram. A User authenticates to the module per packet using the shared secret HMAC-SHA-1 key configured by the Crypto-Officer. Through IPSec, the User role has access to some of the module’s cryptographic functionality, including Triple-DES encryption/decryption and HMAC-SHA-1 calculation/verification.

### *2.3.3 Unauthenticated Services*

The Brick also provides the following unauthenticated services to an operator with physical access to the Brick (keyboard and monitor). These services include viewing the module's LEDs, powering the module on and off, and the following status commands:

"help", //prints list of commands"
"help <cmd>", //prints help for <cmd>
"logout", //logout from remote port
"repeat", //repeat the previous command
"refresh <table>", //refresh brick's mac or arp table
"display arptable", //display contents of the arp table
"display configuration", //prints the inferno.ini file
"display encapsulation <zone>", //display UDP encapsulation info for the zone
"display failover", //display failover status
"display files <filepath>", //print the names of the files
"display hostgroups <zone>", //display a zone's hostgroup definitions
"display icm", //display ICM info
"display interfacestatus [<if>]", //display information about an interface's NIC
"display lsms", //print the current LSMS connected (or the lst LSMS)
"display mactable [<if>]", //display MAC table for the specified interface
"display mempools", //print information on 5 memory pools of the brick
"display nat <zone>", //print information about NAT tables for a zone
"display policy zone>", //prints the ruleset for the specified zone
"display remoteconsole", //display information about the remote console
"displayroutes [<if>]", //display routing information for an interface
"display sa <zone>", //display a zone's current security associations
"display servicegroups <zone>", //display a zone's servicegroup definitions
"display sessions <zone> [<IP-addr>], //prints the zone's session cache optionally filtered by an IP address
"display time", //print the brick's current time in GMT
"display vlans", //displaly vlan ip subnets and port membership
"display zonetable", //display the brick's zone assignment table
"failover", //display a failover status
"failover yield [force]", //switch from active to standby
"trace arp on [yes|no]", //trace arps (with optional full packet dump)
"trace arp off", //disable arp tracing
"trace audit filter <filter-list>", //define an audit filter
"trace audit modify <filter-id><filter-list>", //modify existing audit filter
"trace audit delete <filter>", //delete the specified filter
"trace audit on [<filter-id|a|p>]", //enable all filters or the specified filter
"trace audit off [<filter-id|a|p>]", //disable all filters or the specified filter
"trace packet list", //print the list of current packet filters
"reboot [<msg>]", //reboots the brick with an optional message in the audit log
"set screensize [<size>]", //set or display the screensize, default=23
"set printing [on|off]", //set or display the tracing print value
"set baudrate <rate>", //set or display the baudrate of the remote port

"set throttle <interval>", //set number os seconds b/w identical audit msgs
"set errors [on|off]", //set or display the critical error value
"modem <cmd>", //send the <cmd> to the brick's modem, use " to enclose blanks

### *2.4 Physical Security*

The module is enclosed in a strong steel enclosure that completely covers all of the module's internal components. Access to the module is provided through well-defined interfaces as described in section 2.2. In order to provide evidence of attempts to physically tamper with the Brick 201, the module's case must be affixed with tamper-evident labels. The application of tamper-evident labels is described in section 3.

### *2.5 Cryptographic Key Management*

The module supports the following FIPS-approved algorithms for use in a FIPS mode of operation: DES, Triple-DES, SHA-1, and DSA. Additionally, the module supports the following algorithms for use in a FIPS mode of operation: HMAC with SHA-1 (for authentication purposes only) and Diffie-Hellman. The module also supports MD5 and RC4, which are not approved for use in FIPS mode of operation. The following table describes the keys used by the module:

| Key | Key type | Generation | Storage | Use |
|---|---|---|---|---|
| LSMS CA public key | DSA public key | Externally generated and entered by CO | Non-volatile memory in plaintext | Verify public key certificates |
| LSMS public key | DSA public key | Externally generated and exchanged during LSMS session handshake | RAM only | Authentication during LSMS session handshake |
| DSA key pair for Brick | DSA key pair | Externally generated and entered by CO | Non-volatile memory in plaintext | Authentication during LSMS session handshake |
| Diffie-Hellman key pairs | Diffie-Hellman key pair | Diffie-Hellman key generation | RAM only (Diffie-Hellman public parameters stored in non-volatile memory) | Key agreement during LSMS session handshake |
| Policy Signatory public key | DSA public key | Externally generated and entered by CO | Non-volatile memory in plaintext | Verification of Brick 201 policy integrity |
| Session keys for LSMS | DES/TRIPLE-DES keys and HMAC-SHA1 | Generated by LSMS session handshake | RAM only | Secure LSMS session traffic |
| Session keys for IPSec | DES/TRIPLE-DES key | Externally generated and entered by the LSMS | RAM only | Secure IPSec traffic and authenticate |
| Session keys for IPSec | HMAC-SHA1 key | Externally generated and entered by the LSMS | RAM only | Authenticate Users via HMAC-SHA-1 verification |

**Table 4 – Description of the Module's Keys**

The LSMS CA public key is the public key (loaded during initialization) stored in plaintext in the module's non-volatile memory. The module uses this key to verify the authenticity of signed certificates.

The LSMS public key is the key of the LSMS. This key is contained within a certificate signed with the CA private key. The LSMS provides the Brick 201 this key during establishment of an encrypted session to allow the Brick 201 to authenticate the LSMS. This key is only stored in volatile memory during the LSMS session handshake and can be destroyed by powering off the module.

The DSA key pair for the Brick 201 is generated externally by the LSMS. This key pair is loaded onto the module during initialization of the module via the disk drive. This key pair is stored in non-volatile memory on the module and can be destroyed by loading a new key pair during re-initialization the module from a diskette.

The Diffie-Hellman key pairs are generated as needed by the LSMS session handshake to perform LSMS session key agreement. These keys are stored in volatile memory and can be destroyed by powering down the module. Additionally, the public parameters are stored the module's non-volatile memory.

The Policy Signatory public key is a DSA public key generated external to the Brick 201 and is contained in a digital certificate signed by the LSMS CA private key. This public key is loaded onto the module by the Crypto-Officer and is stored with the module's configuration policy. This key is used to verify the integrity of the module's configuration policy. It can be zeroized by the Crypto-Officer by loading a new Policy Signatory public key onto the Brick 201.

Session keys for LSMS are established by the LSMS session handshake protocol. These keys are used to encrypt the LSMS session with the Brick 201 and are stored in volatile memory. The keys can be destroyed by powering down the module.

Session keys for IPSec are ephemeral keys established for IPSec connections. These keys are automatically loaded onto the module by the Crypto-Officer over a secure LSMS session as part of an IPSec SA. These keys can be destroyed by powering down the module.

### *2.6 Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)*

The module has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC rules. Thus, the module meets FCC requirements in 47 CFR Part 15 for personal computers and peripherals designated for Business use (Class A). The module is labeled in accordance with FCC requirements with the appropriate FCC warnings.

### *2.7 Self Tests*

The Brick 201 runs self tests during power-up and conditionally. The self-tests run at power-up include known answer tests (KAT) on the FIPS-approved cryptographic algorithms (DES,

Triple-DES, SHA-1), a sign and verify test for DSA, a firmware/software integrity, a Diffie-Hellman critical function test. The following tests are also run conditionally: a bypass test run whenever the configuration file is modified, and a continuous RNG test run each time the PRNG is used to generate random data.

A software integrity test using a CRC-32 is also performed at startup. The bootstrap verifies the CRC-32 of the compressed OS image is correct before booting from flash. If the image is valid, the OS is uncompressed and boots. Otherwise, the OS load is aborted. The CRC-32 check must be also done after downloads to RAM when a run command is performed to boot the OS.

The module contains the following FIPS-approved Power-up Tests for the Brick 201's Encryption Accelerator card (EAC):

- DES Known Answer Test
- 3DES Known Answer Test
- SHA-1 Known Answer Test

The EAC does not do a separate firmware CRC check. However, this EAC firmware is embedded in the Brick 201 firmware and both are included in the Brick 201's CRC check. The process of loading the EAC firmware into the EAC is a copy from the memory space on the motherboard to the memory space on the EAC (followed by starting the processor).

# 3 Secure Operation

The module is capable of both a FIPS mode of operation and a non-FIPS mode of operation. The following instructions detail how to configure the module for a FIPS mode of operation.

The module is initialized by loading configuration information from a floppy disk. This disk must be generated by the Crypto-Officer using version 6.0.554 of the LSMS and only version 6.0.544 of the Brick 201 firmware is allowed for FIPS mode of operation. Once the configuration is loaded onto the module, the Crypto-Officer is able to access the module over an authenticated and encrypted LSMS session.

After the Brick 201 has been configured via the floppy disk drive, tamper-evident labels must be affixed to the module. The floppy drive is not accessible after the module has been initiated. The Crypto Officer must apply tamper-evidence labels as follows:

1. Clean the cover of any grease, dirt, or oil before applying the tamper evidence labels. Alcohol-based cleaning pads are recommended for this purpose. The ambient air must be above 10° C, otherwise the labels may not properly cure.
2. Having the front cover facing you, place the first label on the top left of the module as shown in figure 2. The tamper evidence label should be placed so that the one half of the tamper evidence label covers the enclosure and the other half covers the side of the module. Any attempt to remove the enclosure will leave tamper evidence.
3. Place the second label on the top right of the module as shown in figure 2. The tamper evidence label should be placed so that the one half of the tamper evidence label covers the enclosure and the other half covers the side of the module. Any attempt to remove the enclosure will leave tamper evidence.
4. Place the third label on front bezel of the module as shown in figure 2. The tamper evidence label should be placed so that the one half of the tamper evidence label covers the enclosure and the other half covers the front of the module. Any attempt to remove the enclosure will leave tamper evidence.
5. With the front cover facing you, turn the Brick 201 so that the bottom is facing up. Place the fourth label on the top left of the module, as was done in step 2. The tamper evidence label should be placed so that the one half of the tamper evidence label covers the enclosure and the other half covers the side of the module. Any attempt to remove the enclosure will leave tamper evidence.
6. Place the fifth label on the top right of the module, as was done in step 3. The tamper evidence label should be placed so that the one half of the tamper evidence label covers the enclosure and the other half covers the side of the module. Any attempt to remove the enclosure will leave tamper evidence.

**Figure 2 – Tamper evidence label placement on front panel/top**

The placement of the labels should be consistent with the instructions and the images above. The tamper evidence seals have a special adhesive backing to adhere to the module's painted surface. Removing the power panel, network interface panel, bottom cover or top cover will damage the tamper evidence seals. Tamper evidence labels can be inspected for signs of tampering, which include the following: curled corners, bubbling, and rips.

In addition, the word "Opened" will appear on the label if it was peeled away from the surface of the module. The tamper evidence labels have individual, unique serial numbers, and the labels may be inspected periodically and compared against the applied serial numbers to verify that the fresh labels have not been applied to a tampered module.

The Crypto Officer must securely store tamper evidence labels before use. After applying the tamper-evidence labels, the Crypto Officer must securely store any unused labels.

In order to ensure only FIPS-approved algorithms are used on the module, the Crypto-Officer must disable failover and only configure the module with IPSec SA's that use FIPS-approved algorithms. These algorithms are HMAC with SHA-1, DES, and 3DES. Additionally, the Crypto-Officer must ensure that all IPSec SA's provide both integrity (HMAC with SHA-1) and confidentiality (DES or 3DES). 3DES is the recommended algorithm to be used for encryption and decryption. DES is only to be used in legacy systems.

***Non-FIPS Approved Algorithms***

The following algorithms are implemented in the module but cannot be used in FIPS-mode of operation:

- MD-5
- RC4