The Ultralock Symmetric Module

nCIPHER™

Date: **5 February 2007**

Patents

UK Patent GB9714757.3. Corresponding patents/applications in USA, Canada, South Africa, Japan and International Patent Application PCT/GB98/00142.

Contents

The Ultralock Symmetric Module

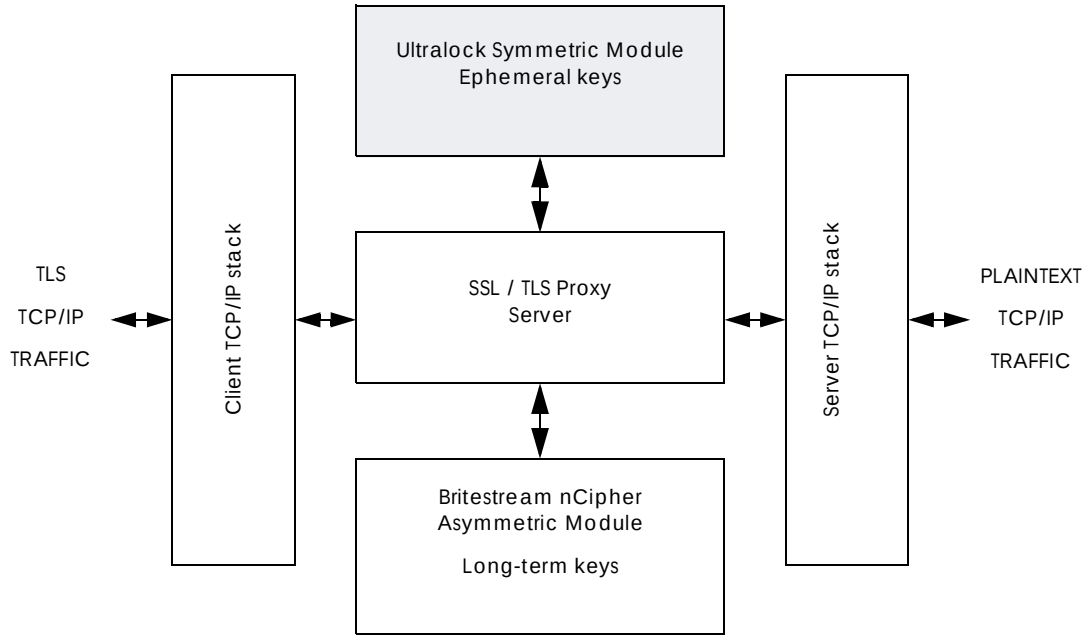
The Ultralock Symmetric Module is a FIPS 140-2 level 1 module that forms part of the Cipher nForce Ultra product - previously also sold as the Britestream BN1250.

Note *nCipher have aquired the assets of Britestream Networks Inc. This acquisition enables nCipher to take full ownership of the nForce Ultra line of cryptographic accelerator solutions originally developed jointly by Britestream and nCipher. These products will now be manufactured by nCipher.*

The nCipher nForce Ultra is a PCI cards that act as TLS proxy servers, with secure TCP/IP communication on one ethernet port and plain text TCP/IP communication on a physically separate port. These cards completely off load the TLS processing from the host computer, delivering secure internet communication at full line speeds.

The main components of the proxy server are physically resident on a single chip - the BN2010 chip - which has multiple processor cores plus dedicated hardware. This chip requires a small number of additional components, including memory, etc.

The BN2010 includes separate cryptographic modules for long term asymmetric keys and ephemeral symmetric keys - as shown in the following diagram:



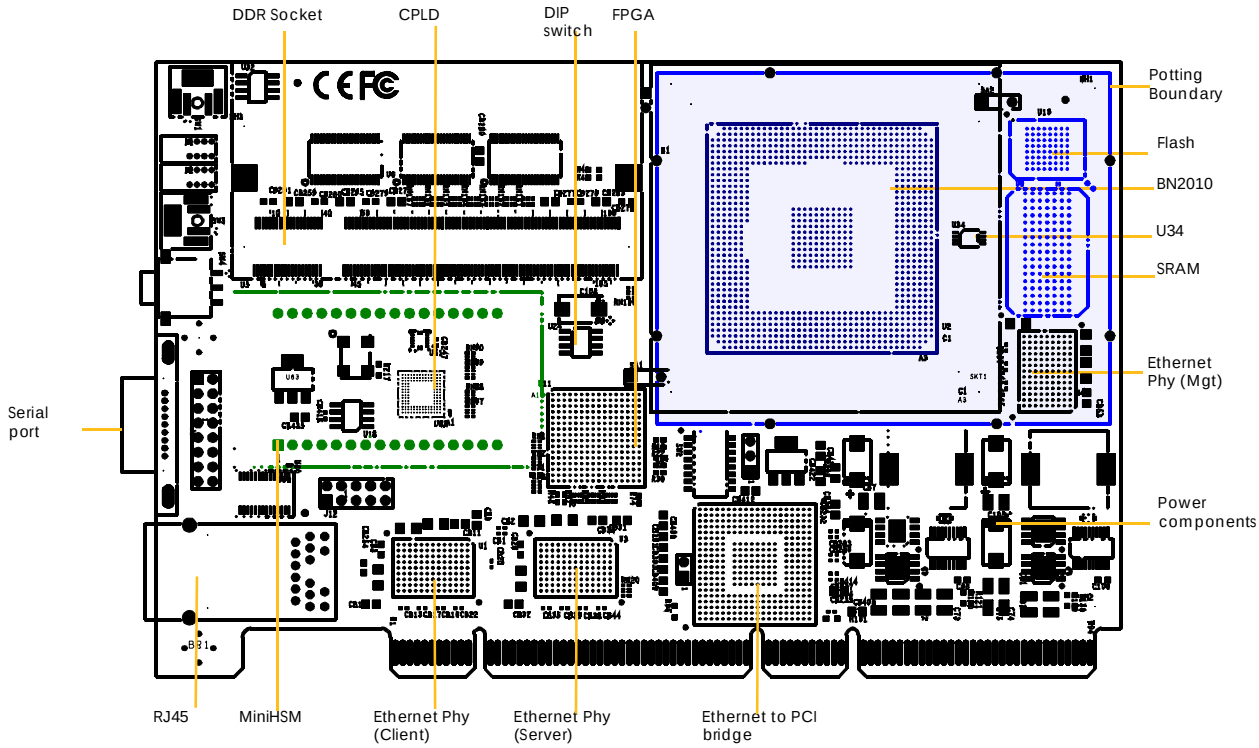
Note *This validation is for the Ultralock Symmetric Module only. There is a separate validation for the Britestream nCipher Asymmetric Module and the nCipher MiniHSM. Refer to the security policy for that module, FIPS 140-2 certificate 706, for details of asymmetric cryptographic operation of the BM2010 and to certificate 672 for details of the MiniHSM.*

The Ultralock Symmetric Module is a multichip embedded module as defined in FIPS 140-2.

The Ultralock Symmetric Module consists of all components on the PCI card, including the Britestream nCipher Asymmetric Module and nCipher MiniHSM which have been validated separately to FIPS 140-2 level 3.

The following diagram shows the Ultralock Symmetric Module with the components that form the Britestream nCipher Asymmetric Module highlighted in blue and the MiniHSM highlighted in green.

Figure 1 PCI board layout



The BN2010 chip - shown in the darker blue - contains several ARC processors. One processor - the management ARC - is used by the Britestream nCipher Asymmetric Module, the other processors and hardware form part of the Ultralock Symmetric Module.

The Ultralock Symmetric Module is hardware version 010-00007 a.00.

Ports and interfaces

The Ultralock Symmetric Module is supplied on a PCI card. The following table lists the data interfaces of the Ultralock Symmetric Module and how these are connected to physical interfaces on the PCI card.

There are separate logical channels - TCP/IP ports - on the PCI interface for data in, data out, control in and status out.

FIPS 140 Interface		Physical Interface
Data Input	Plain text	PCI Interface
	Cipher text	RJ-45 socket
Data Output	Plain text	PCI Interface
	Cipher text	RJ-45 socket
Control Input	Commands	PCI Interface
	Reset	Reset button
Status Output	Messages	PCI Interface
		RJ-45 socket
	TCP status	LEDs
Power		PCI interface

Note *Control and status information is routed through the Britestream nCipher Asymmetric Module.*

Pressing the reset button causes the module to perform the reset service.

Roles and Authentication

The module has one administrator role and two operator roles.

Role	Performs
Administrator	Initializes the module and receives status messages.
TLS Operator	Negotiates the TLS handshake, loads key seeds and causes keys to be derived by the module: based on TLS policies set by the Administrator.
TCP Operator	Routes TLS application traffic to the Symmetric Module, for symmetric encryption and decryption, based on TCP policies set by the Administrator.

A user assumes a role by connecting to the module on the appropriate interface. The module has a separate interface for each role.

Only one operator may assume each role at any time.

In order to assume the Administrator role, the operator must first log on to the *Britestream nCipher Asymmetric Module* in an Administrator role. They can then submit commands to the *Britestream nCipher Asymmetric Module* which passes the commands to the *Ultralock Symmetric Module*. The *Ultralock Symmetric Module* sends replies to the *Britestream nCipher Asymmetric Module* which in turn sends them to the operator.

Services

The module supports the services listed in the following table.

For each service, the table lists the roles that can use the service, the access to CSPs, and the available key types, with non-FIPS approved types listed in parenthesis.

The Ultralock Symmetric Module does not include any key generation functions. Keys used by the module are derived using TLS protocol (RFC 2246).

The module keeps all keys secret until they are destroyed - there are no facilities to export keys in any form.

Key access	Description
Derive	Derives a in-memory object., but does not reveal value.
Overwrite	Writes over the object from memory, or non-volatile memory without revealing value
Set	Changes a CSP to a given value
Use	Performs an operation with an existing CSP - without revealing or changing the CSP

Service name	Role			Description ***Key Use*** **Key types**
	Admin	**TLS**	**TCP**	
Show Status	Yes	No	No	Reports the status of the module
Zeroize	Yes	No	No	Clears all memory. The reset service can also be activated by pressing the reset button. ***Overwrites*** *all keys* All keys
Initialize/Self Test	Yes	No	No	Causes all power-on and known-answer self tests to run. ***Sets***, ***uses*** *and* ***overwrites*** *all keys* AES128, AES256, Triple DES, HMAC-SHA-1
Import Seed	No	Yes	No	Imports a seed in plain text. Three seeds are required to derive a TLS key set. ***Sets*** *a seed* TLS seed (SSL seed)

Service name	Role			Description *Key Use* Key types
	Admin	TLS	TCP	
TLS	No	Yes	No	Uses the three imported seeds to derive a set of keys using the TLS, or SSL, protocol. See "Algorithms" on page 16 for encryption strengths. ***Derives** a key from components* TLS (SSL) key
Decrypt	No	Yes	Yes	Decrypts a message using a TLS key. ***Uses** a TLS key* AES128, AES256, Triple DES (RC4, DES)
Verify HMAC	No	Yes	Yes	Verifies a MAC using the TLS HMAC key. Returns true or false. ***Uses** a TLS HMAC key* HMAC-SHA1 (HMAC-MD5)
Encrypt	No	Yes	Yes	Encrypts a message using a TLS key. ***Uses** a TLS key* AES128, AES256, Triple DES (RC4, DES)
Generate HMAC	No	Yes	Yes	Generates a TLS HMAC message digest using TLS HMAC KEY. ***Uses** a TLS HMAC key* HMAC-SHA1 (HMAC-MD5)
Hash	No	Yes	Yes	Hashes a message *No access to CSPs* SHA-1 (MD5)
Close connection	No	Yes	No	Invalidates all keys for this connection, keys cannot be reused. ***Overwrites** keys*

Rules

The module is specifically designed for use as part of a SSL Proxy server which implements the TLS and SSL protocols.

Every key used by the module must follow the state transitions laid down in the TLS specification.

1. Have the Britestream nCipher Asymmetric Module, decrypt the client's RSA encrypted premaster nonce.
2. Import the three seeds, client nonce, server nonce, premaster nonce.
3. Use the TLS key derivation function to derive a set of keys for this connection.
4. Use HMAC-SHA-1 to verify that the keys have been derived correctly, if verification fails discard keys.
5. Use the keys to encrypt data from server and decrypt data from client. Use HMAC-SHA-1 to derive the message authentication code for the server data. Use HMAC-SHA-1 to verify the message authentication code of the client data.
6. Close connection.

Delivery and Operation

In order to use the Britestream Symmetric Module you must first configure the "Britestream nCipher Asymmetric Module" FIPS 140-2 level 3 module, as described in its security policy, see FIPS 140-2 certificate 706.

Once this is configured you can configure the level 1 module.

1 Define the TCP addresses for which this proxy will process traffic using the setProxy command.

2 Define the cipher suites to use for this proxy using the setProxySSL command.

In order to offer compatibility with the maximum number of possible clients, the Ultralock Symmetric Module offers both FIPS approved and non-FIPS approved algorithms.

The module is in FIPS approved mode when using FIPS approved algorithms.

If you require the module to only operate in FIPS mode, configure the module to only use following cipher suites that use approved algorithms:

- RSA_3DES_EDE_CDC_168_SHA1
- RSA_AES_128_SHA1
- RSA_AES_256_SHA1

This is done using the setGlobalCipher command, see the security policy for the "Britestream nCipher Asymmetric Module" FIPS 140-2 level 3 module.

The following cipher suites may be used in FIPS-approved mode of operation:

3 Turn on this proxy using the setProxyState command.

Physical Security

The module is a multi-chip embedded cryptographic module.

The module's hardware consists of industry standard, production grade components in regards to power and voltage ranges, temperature, reliability, and shock and vibration.

Strength of Functions

Seeds are loaded separately and then keys are derived using the TLS key derivation mechanism. It is not possible to derive a key without all three components.

Once derived, key material cannot be accessed

Self Tests

The Ultralock Symmetric Module performs known answer tests on all algorithms at start up.

The module performs a continuous test of the non deterministic random·number generator in hardware.

The module also tests the bypass mode. The Bypass test is configured in the *Britestream nCipher Asymmetric Module* using the setPassThru service. However, the bypass rules are enforced within the level 1 boundary.

If any of these tests fail the module is put into an error state.

Algorithms

The Ultralock Symmetric Module uses the following algorithms.

Note *Algorithms marked with an asterisk are provided by* Britestream nCipher Asymmetric Module *certificate* 706.

FIPS approved algorithms

Triple DES (112-bit or 156-bit keys)

Provides 112 or 156 bits of encryption strength. Certificate 345.

AES (128-bit or 256-bit keys)

Provides 128 or 256 bits of encryption strength. Certificate 263.

SHA-1

Certificate 342.

HMAC-SHA-1

Certificate 75.

DSA*

Certificate 138.

Diffie Hellman*

Key agreement, key establishment methodology provides 112 bits of encryption strength.

RSA*

RSA signature verification. Certificate 103.

RNG*

Certificate 96.

Non Approved algorithms

DES

Note *Non-compliant due to CAVP DES transition policy.*

RC4

MD5

MD5 HMAC

RSA*

RSA key wrapping, as part of TLS and SSL protocols, provides 80- to150-bits of encryption strength.

Protocols

TLS

TLS key agreement is approved for use by FIPS 140-2 validated modules. 112-bit and 156-bit triple DES keys and 128-bit or 256-bit AES keys with up to 4096-bit RSA or 2048-bit Diffie-Hellman keys are supported in the modules FIPS-approved mode of operation.

SSL

SSL key agreement is a non FIPS-approved mode of operation.

Note *A non-complaint hardware RNG is used to generate the server nonce for TLS and SSL.*

Addresses

nCipher Corporation Ltd.

Cambridge, UK

Jupiter House
Station Road
Cambridge
CB1 2JD
UK

Tel: +44 (0) 1223 723600
Fax: +44 (0) 1223 723601

E-mail: sales@ncipher.com
support@ncipher.com

nCipher Inc.

Boston Metro Region, USA

92 Montvale Avenue, Suite 4500
Stoneham, MA 02180
USA

Tel: 800-NCIPHER
800-6247437
+1 (781) 994 4000
Fax: +1 (781) 994 4001

E-mail: sales@us.ncipher.com
support@ncipher.com

Internet addresses

Web Site:	http://www.ncipher.com/
Online Documentation:	http://active.ncipher.com/documentation/

Note *nCipher also maintain international sales offices. Please contact the UK, or the US, head office for details of your nearest nCipher representative.*