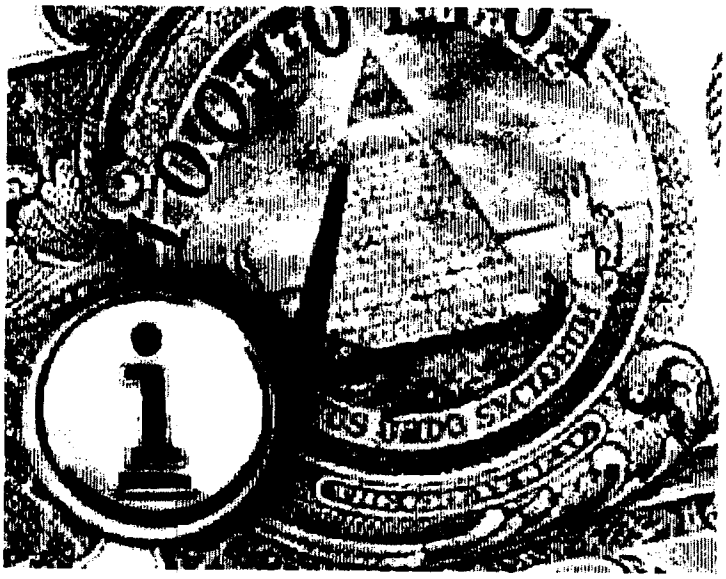
DALLAS SEMICONDUCTOR

DS1954
Cryptographic iButton™



FIPS 140-1 Non-Proprietary Cryptographic Module Security Policy

Level 3 Validation

Sept 1, 1998

Table of Contents

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Dallas Semiconductor DS1954 Cryptographic iButton ™ (Crypto iButton). This policy was prepared as part of FIPS 140-1 certification of the Crypto iButton. FIPS 140-1 (Federal Information Processing Standards Publication 140-1 -- *Security Requirements for Cryptographic Modules*) gives U.S. Government requirements for cryptographic modules, and defines the Security Policy as:

> "A precise specification of the security rules under which the cryptographic module must operate, including rules derived from the security requirements of this standard, and the additional security rules imposed by the manufacturer."

The DS1954 provides extraordinary security, meeting all FIPS 140-1 level 2 requirements, many level 3, and even some level 4 requirements. This security policy describes how the Crypto iButton meets these requirements, and how it can be operated in a secure fashion.

1.2 For more information

This document describes the operations and capabilities of the DS1954 Crypto iButton™ in the technical terms of a FIPS 140-1 cryptographic module security policy.

> For more detailed information about the Crypto iButton, please visit the iButton web site at http://www.ibutton.com. The web site contains non-technical descriptions of Dallas iButton products, technical specifications, product offerings, iButton functionality, iButton developer information, and much more.
>
> Fore more information about the FIPS 140-1 standard and validation program please visit the NIST web site at http://csrc.nist.gov/cryptval/.
>
> For answers to technical or sales related questions please refer to the contacts listed on the iButton web site at http://www.ibutton.com, or the Dallas Semiconductor web site at http://www.dalsemi.com.

1.3 Terminology

In this document the Dallas Semiconductor DS1954 Cryptographic iButton™ is referred to as the DS1954, Crypto iButton, cryptographic module, or module. The Crypto iButton is also referred to as simply "iButton", although this term also applies collectively to other iButtons such as the DS1990, DS1994, or DS1920 which cannot perform computations.

2 The DS1954 Crypto iButton™

The Crypto iButton provides hardware cryptographic services such as secure private key storage, a high-speed math accelerator for 1024-bit public key cryptography, and secure message digest (hashing). In FIPS 140-1 terminology the Crypto iButton is a "multi-chip standalone cryptographic module"; however, the Crypto iButton actually provides all its services using a single silicon chip packaged in a 16mm stainless steel case. Thus, the iButton can be worn by a person or attached to an object for up-to-date information at the point of use. The steel button is rugged enough to withstand harsh outdoor environments, and is durable enough for a person to wear everyday on a digital accessory like a ring, key fob, wallet, or badge.

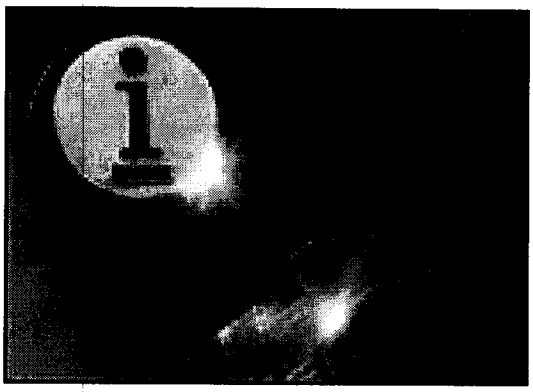


Figure 1 – The DS1954 Crypto iButton™ is laser–engraved in steel and silicon

2.1 The iButton Cryptographic Module

The cryptographic boundary for the iButton is the surrounding steel shell. This surrounding shell is factory-lasered with the module's unique 64-bit registration number as shown in Figure 2. The figure shows a button with registration number "1A1D2516"$_{16}$, which is engraved on the encased silicon chip.

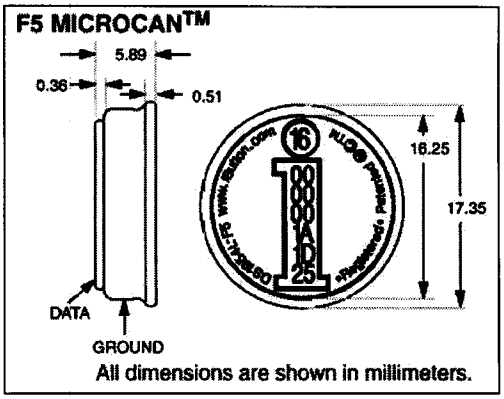


Figure 2 – Crypto iButton Case and Module Boundary

The ground side of the iButton may optionally be branded with logo facings. Registration numbers are also lasered into unalterable ROM on the iButtons, which can be read by any application communicating with an iButton. Strict factory controls ensure that registration numbers are globally unique, guaranteeing that no two iButtons ever share a registration number.

2.1.1 Module Interfaces

The button uses a single data contact on the front of the steel case to convey the module's five logical interfaces: data input, data output, control input, status output, and power. These interfaces are logically separated using the 1-Wire™ protocol, which regulates communications and separates reading, writing, and power applied to the module. The 1-Wire protocol utilizes a scratchpad buffer and features atomic, packetized transfers which assures error-free transmission, even with an intermittent connection, in addition to complete separation of input, processing, and output phases. Control commands and data must be input in error checked packets, and data and status are returned only after successful completion of processing.

2.1.2 Module Components

The active components of the iButton are shown below, and consist of a lithium cell (for backup power), an energy reservoir (to provide parasitic capacitance power), a quartz timing crystal (for a True Time Clock), and the single DS83C950 cryptographic chip.

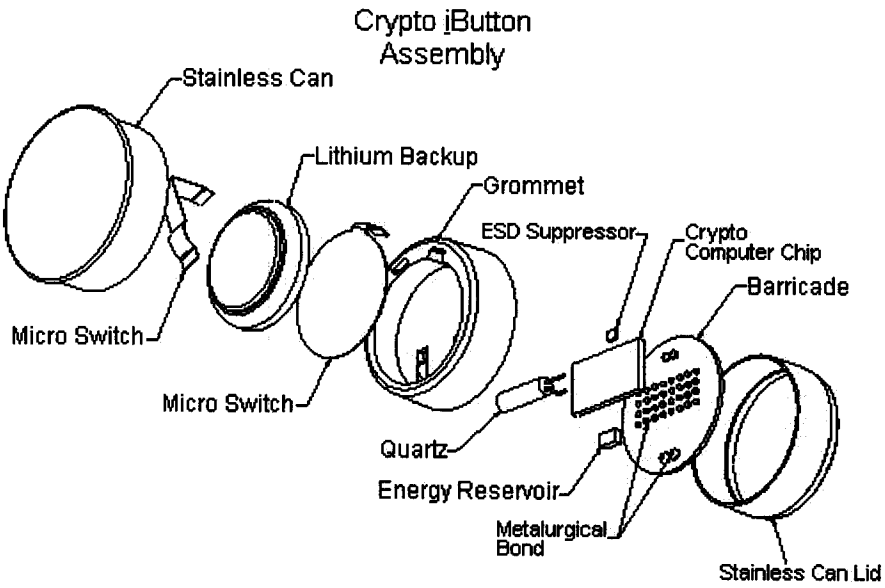


Figure 3 – Components of the DS1954 Crypto iButton™

2.2 Physical Security

The Crypto iButton boasts an incredible array of physical security safeguards packed into a small coin-sized device. Because the silicon chip is encased in stainless steel, the

iButton will stand up to the harsh conditions of daily wear, including dropping it, stepping on it, and inadvertently passing it through the washing machine and dryer.

Figure 3 – The Crypto iButton Mounted as a Signet Jewel of a Ring. It can be attached to any personal accessory

2.2.1 The Strength of Steel

The tough stainless steel case of the iButton also defines a contiguous perimeter and provides clear visual evidence of tampering. Tamper-signs include mangling and scratching of the data and ground plates and the smooth grommet separation. It is this outer case which satisfies FIPS 140-1 level 2 tamper evidence requirements for physical security. Along with other safeguards, the case even meets the FIPS 140-1 level 3 tamper response and level 4 Environmental Failure Protection (EFP) requirements.

2.2.2 Goes Down in a Blaze of Zeroization

If an iButton is pried open, a microswitch triggers an active zeroization of the chip's contents, destroying private keys and other sensitive information. The iButton constantly monitors the switch's contacts, and any separation of the cryptographic chip from the lithium cell switches the device to on-chip capacitor power to perform a complete zeroization as it's last powered action.

2.2.3 Neither snow nor rain nor heat...[1]

Orchestrated attacks to uncover iButton secrets by subjecting the iButton to extreme temperature or voltage conditions will generate a tamper response that results in zeroization. Deliberately exposure to temperatures outside the iButton's operational range of -20°C to +70°C (-4°F to +158°F) cause temperature monitors to trigger a cold-temp switch or high-temp effects that quickly zeroize to erase the contents of the

[1] "*Neither snow nor rain nor heat nor gloom of night stays these couriers from the swift completion of their appointed rounds.*" -- an inscription on the General Post Office, New York City. (see http://www.usps.gov/history/his8.htm)

memory. Voltages above or below maximum operating tolerances are clamped, and if excessive voltage is encountered, the I/O pin is designed to fuse and render the chip inoperable.

2.2.4 Fortresses large and microscopic...

In addition to these operation controls, the cryptographic chip is additionally protected. A substrate barricade is metallurgically- and glass epoxy-bonded to the active face of the chip. Attempts to remove the barrier to get to the chip cause a tamper response that results in zeroization. If a sophisticated attacker attempts to micro-probe the chip, they will encounter a shield of sub-micron pitch metal layers fabricated into a serpentine pattern directly on the chip. The chip will detect any break in this shield and immediately zeroize the chip.

2.3 DS1954 Firmware Capabilities

The Crypto iButton contains an 8051-compatible microcontroller, a tamper-evident real-time clock, a high-speed modular exponentiation accelerator for large integers up to 1024 bits in length, 32 Kbytes of ROM memory with preprogrammed firmware, 6 Kbytes of non-volatile RAM (NVRAM) for storage of critical data, input and output buffers with the standard iButton 1-Wire "front-end" for sending and receiving data, and control circuitry that enables the microcontroller to be powered up to interpret and act on the data placed in an input buffer, drawing its operating power from the 1-Wire line. The microcontroller, clock, memory, buffers, 1-Wire front-end, modular exponentiation accelerator, and control circuitry are integrated on a single silicon chip and packaged in a stainless steel case using packaging techniques which make it virtually impossible to probe the data in the NVRAM without destroying the data. Most of the NVRAM is available for use to support cryptographic applications such as those mentioned above.

The Crypto iButton firmware supports the Secure Hashing Algorithm (SHA-1) and conforms to Federal Information Processing Standard Publication (FIPS PUB) 180-1, *Secure Hash Standard (SHS)*.

2.4 Roles & Services

There are two separate roles in the operation of Crypto iButtons: Crypto Officer, and User. The Crypto iButton is intended to be activated by a service provider (Crypto Officer) who procures an iButton and co-issues the device to his own customers. These registered customers (Users) operate the devices as end users under a license agreement. The Crypto Officer loads the Crypto iButton with data to enable it to perform application specific functions. The User issues commands to the Crypto iButton to perform operations programmed by the Crypto Officer. For this reason the Crypto iButton offers functions to support the Crypto Officer in setting up the Crypto iButton for an intended

application, and it also offers functions to allow the authorized User to invoke the services offered by the Crypto Officer.

2.4.1 Transaction Groups, Objects and Scripts

A Crypto Officer can reserve a block of NVRAM memory to support services by creating a Transaction Group. A Transaction Group is simply a set of Objects that are defined by the Crypto Officer. These Objects include both data Objects (encryption keys, transaction counts, money amounts, date/time stamps, etc.) and Transaction Scripts which specify how to combine the data Objects in useful ways. The Crypto Officer creates a Transaction Group for a set of Users, which is independent of every other Transaction Group. Hence, a Crypto Officer could offer different sets of services in the same Crypto iButton using different Transaction Groups to support multiple functions for a single iButton. The number of independent Transaction Groups that can be supported depends on the number and size of the Objects defined in each Transaction Group. Examples of some of the Objects that can be defined within a Transaction Group are the following:

Modulus	Money	Register Input Data
Exponent	Clock Offset	Output Data
Transaction Script	Random Salt	Destructor
Transaction Counter	Configuration Data	

Within each Transaction Group, the Crypto iButton will initially accept certain commands that have an irreversible effect. Once any of these irreversible commands is executed in a Transaction Group, it remains in effect for the life of the Crypto iButton or until the Transaction Group to which it applies is erased from the Crypto iButton. In addition, there are certain commands that have an irreversible effect on the Crypto iButton as a whole, and remain in effect for the life of the Crypto iButton or until a master erase command is issued to erase the entire contents of the Crypto iButton. These commands are essential to give the Crypto Officer the necessary control over the operations that can be performed by the user. Examples of some of the irreversible changes made by a Crypto Officer are:

Privatize an Object	Lock an Object
Lock a Transaction Group	Lock the Crypto iButton

Since much of the Crypto iButton's utility centers on its ability to keep a secret, the Privatize command is the most important irreversible command. The fundamental concept implemented by the firmware is that the Crypto Officer can store Transaction Scripts in a Transaction Group to perform only those operations among Objects that he wishes the authorized User to be able to perform. The Crypto Officer can also store and privatize the private key or keys that allow the Crypto iButton to "sign" transactions on behalf of the Crypto Officer, thereby guaranteeing their authenticity. By privatizing and/or locking one or more Objects in the Transaction Group and locking the Transaction Group itself, the Crypto Officer maintains control over what the Crypto iButton is allowed to do on his behalf. After the group is locked the User cannot add new

Transaction Scripts to that Transaction Group and is therefore limited to the operations on Objects that can be performed with the Transaction Scripts programmed by the Crypto Officer.

2.4.2 Role-Based Authentication

The Crypto iButton uses role-based authentication, which satisfies level 2 FIPS 140-1 authentication requirements. There is a Crypto Officer personal identification number (PIN) for each iButton, which must be supplied with each and every service request reserved for the Crypto Officer. The Crypto Officer PIN (also called the iButton's common PIN) can be any value (numeric, alpha, or binary byte values), and from one to eight bytes in length. Similarly there is a User PIN for each Transaction Group, which must be supplied with every request for User services. There are also non-cryptographic services (related to iButton status) which are available to User and Crypto Officer without supplying an authenticating PIN.

There are additional optional identification and authentication (I&A) functions designed into the iButton which are not discussed in this policy. These advanced I&A features allow for identity based authentication using challenge-response protocols with automatic logout. When properly used, these I&A features meet level 3 and level 4 FIPS 140-1 roles and services and authentication requirements.

2.4.3 Crypto Officer services

A Crypto Officer can exercise the following services with appropriate authentication:

SetCommonPIN	MasterErase
CreateTransactionGroup	LockCiB

These allow the Crypto Officer to completely erase and zeorize an iButton, create new containers of User Objects and Scripts (Transaction Groups), and lock the iButton to prevent additional groups from being added or changed. The Crypto Officer may also authenticate and assume a user role in order to set up information within a particular Transaction Group.

A complete description of each Crypto iButton command can be found in the Crypto iButton Firmware Reference Manual.

2.4.4 User services

A User can exercise the following services with appropriate authentication:

SetGroupPIN	CreateCiBObject
SetCiBObjectAttr	LockGroup
InvokeScript	ReadCiBObject
WriteCiBObject	DeleteGroup
ReadTrueTimeClock	ChangeGroupName
GenerateRSAKeySet	GenerateRSAModAndExp

GenerateRSAKeySetNP	GeneratePrime
GenerateRandomExponent	

These services allow a user to change PINs, create objects and scripts within a Transaction Group (subject to restrictions already set up by the Crypto Officer), create keys, read and write information from Objects, invoke Scripts, and modify Transaction Group characteristics. Changing a group name affects only name the label and not the Transaction Group ID; however, Locking a Transaction Group disables subsequent creation capabilities.

A complete description of each Crypto iButton command can be found in the Crypto iButton Firmware Reference Manual.

2.4.5 Status Functions

A number of status functions can be used to find the state of the iButton and various configuration information about the iButton. These status functions can be used by both User and Crypto officer without supplying any PIN:

ReadGroupName	GetGroupID
GetCiBConfiguration	ReadRealTimeClock
CheckGroupCRC	ReadRandomBytes
ReadFirmwareVersionID	ReadFreeRAM
GetCiBError	

2.5 Key Management

The Crypto iButton has a unique internal 64-bit registration number which is not a key, is not private, and is also engraved on the outside of the module.

The iButton supports creation of RSA key pairs through the User functions GenerateRSAKeySet, GenerateRSAKeySetNP, GenerateRSAModAndExp and GenerateRandomExponent.

GenerateRSAKeySet generates a modulus, public exponent, and private exponent suitable for use as an RSA key pair. Modulus and Public exponent are locked (made read-only), and private exponent is privatized (only accessible by transaction scripts). GenerateRSAModAndExp performs the same function as GenerateRSAKeySet, but allows the public exponent to be chosen. GenerateRandomExponent generates a private exponent when modulus and public exponent are already defined

Hence, once keys are created the public keys cannot be modified, and only the scripts defined in the Transaction Group can use the private key. The private key can never be read. If the Transaction Group is locked, or the iButton is locked, the scripts cannot be changed.

GenerateRSAKeySetNP performs the same function as GenerateRSAKeySet but does not immediately privatize the private exponent. This would allow the newly generated

private key to be read from the iButton until the private key Object is privatized. Although some applications may require this functionality, it is not recommended in the absence of strong procedural controls to protect the private key.

Keys are destroyed by deleting the Transaction Group that contains them (which destroys all objects within it, calling the master erase command (which destroys all Transaction Groups), or by triggering a tamper response.

3 Secure Operation of the Crypto iButton

3.1 Crypto Officer Configuration

All Dallas Semiconductor DS1954 Crypto iButtons are delivered from the factory tested, operational, and loaded with a single Transaction Group. This first Transaction Group contains only a script to use SHA-1 and cannot be deleted (without executing a master erase to delete the entire button). Once received, it is recommended that Crypto Officers follow these steps for secure operation in accordance with FIPS 140-1 level 2 requirements.

- Verify that the Crypto Officer has received the Crypto Officer PIN
- Users should separately receive the user PIN for Transaction Group 1
- Delete any additional Transaction Groups on the iButton (Transaction Group 1 cannot be deleted)
- Set a new Crypto Officer PIN with the following bits in the OptionByte:
  - Set the PIN_TO_CREATE bit for CreateTransactionGroup
  - Set the PIN_TO_ERASE bit for MasterErase
- If desired, set up an additional Transaction Group as follows:
  - Create a Transaction Group, & Set the User PIN
  - Load scripts and objects for that Transaction Group
  - Lock and privatize objects according to local policy
  - Create privatized RSA keys following local policy for key generation
  - Lock the Transaction Group
- (Repeat for as necessary for additional Transaction Groups)
- Create a final empty Transaction Group
- Lock the iButton.

Keys must be generated for the User as specified in local policy before the Crypto iButton is locked. This might involve the Crypto Officer generating keys for the User. Alternative scenarios might involve the User in the iButton setup with the Crypto Officer, generating keys with both parties present. Although it is a matter for local policy, for security reasons it is not recommended that the non-private key generation command be used for generation of the private keys.

Crypto Officers should educate Users as to proper operation of iButtons and applications using them, including familiarizing Users with the tamper-evidence signs of an iButton.

3.1.1 Crypto Officer-loaded Script Validation

It is the responsibility of the Crypto Officer to ensure that any additional scripts in loaded onto the Crytpo iButton (beyond the first Transaction Group loaded by the factory) will operate in a safe and approved manner. The Crypto Officer must ensure that no scripts are loaded that will read a private key object and output it from the Crypto iButton. The Crypto Officer must ensure that no scripts are loaded that will modify public or private key objects.

3.1.2 User script validation

The user of an iButton should receive the User pin for the first Transaction Group directly from the iButton supplier and not from the local Crypto Officer. This is to ensure that the SHA-1 script in Transaction Group 1 has not been modified from the validated version created at the factory. If a Crypto Officer executes a master erase and creates a new primary Transaction Group with a SHA-1 script, the User PIN will not be the same as that sent directly to the User and will not be accepted by the iButton. The User should treat such an occurrence as a sign of possible tampering. Additionally, if multiple Users are sharing a PIN for a Transaction Group and one of the users leaves the group, the remaining Users should change the PIN (using SetGroupPIN).

3.2 FIPS 140-1 Mode

FIPS 140-1 mode is defined as using vendor initialized SHA-1 in transaction group 1. Any module that offers algorithms that are not currently FIPS approved (e.g. RSA digital signatures or RSA encryption) must have the capability to be operated in a FIPS-conformant manner. Although the Crypto iButton does not directly provide RSA digital signatures or RSA encryption, it does provide keys and an exponentiator that can be used to perform RSA algorithms.