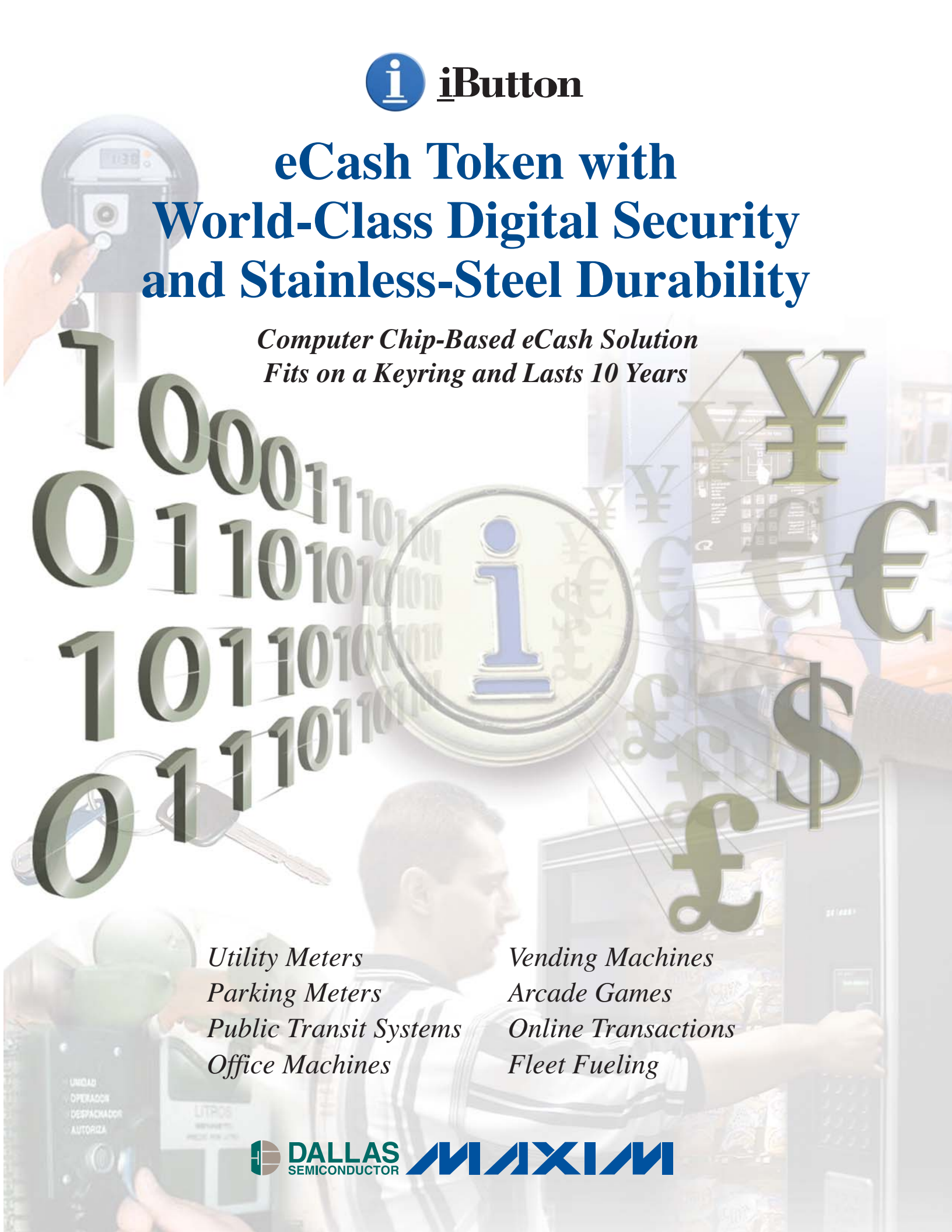
iButton

eCash Token with World-Class Digital Security and Stainless-Steel Durability

Computer Chip-Based eCash Solution
Fits on a Keyring and Lasts 10 Years



Utility Meters
Parking Meters
Public Transit Systems
Office Machines
Vending Machines
Arcade Games
Online Transactions
Fleet Fueling

DALLAS SEMICONDUCTOR MAXIM

Delivering a Secure and Reliable eCash System

What is an iButton?

An iButton® is a computer chip with a globally unique address, factory-lasered at time of manufacture (think of it as a URL for each iButton), enclosed in a 16mm stainless-steel case. iButtons can include read/write memory, real time clocks, and temperature/humidity data loggers. They deliver or record data wherever needed. All this power and capability make iButtons ideal for a wide range of applications including eCash transactions, access control, asset tracking, and environmental data logging.

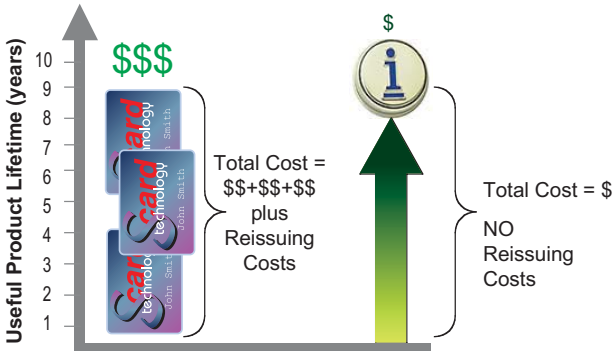
The Globally Unique Key— 281,000,000,000,000 Different Combinations!

An iButton's 64-bit address provides a simple, secure way of identifying a person or asset. It becomes your personalized token and acts like a small change purse for one or multiple applications. The correct token must be presented to a service control unit (SCU) to enable the desired transaction, like dispensing a candy bar or metering a prepaid volume of water. SCUs are microprocessors or any computing device that authenticate a user token, validate its data, and update an account balance as transactions occur. Common SCUs are found inside vending machines, POS terminals, or prepay utility meters. iButtons eliminate the need to carry small amounts of cash, and a single iButton can service multiple, independent applications. They are perfect for a wide variety of eCash functions like mass transit systems, parking meters, and fleet refueling.

The unique address uses 8 bits to identify the type of iButton and 48 bits to generate a serial number. That's enough numbers to assign 50,000 different tokens to each person on the planet!

So Rugged It Lasts Forever!

iButtons bring unparalleled durability to eCash applications. Sit on it. Step on it. Drop it in water. There is no need to worry about destroying it because iButtons withstand harsh indoor or outdoor environments. The durable iButton is wear-tested to last a minimum of ten years, unlike flimsy plastic cards which need constant replacing. There is an additional environmental benefit. In an application using one million tokens over a ten-year period, for example, the durable iButton will keep about 15 metric tons of discarded plastic cards out of the landfill. This robustness also makes them convenient. iButtons easily attach to a key fob, ring, or a watch so your electronic cash is always available when you need it.



iButtons are an exceptional value for security and durability. Every iButton delivers a minimum of 10 years of trouble-free performance. They can last up to 3 times as long as a smart card, which significantly reduces operating costs.

So Simple It Interfaces to Virtually Anything and Uses Almost No Energy!

iButtons require a physical/electrical connection to whatever is writing or reading data. However, a novel digital communication scheme called a 1-Wire® interface reduces the number of electrical contact points to just one, plus a ground reference. A single conductor for both power and data communications is all that is needed. Devices that read and write to iButtons seal all the electrical components inside and expose only the two electrical contact points, separated by a wide gap. With the connection so simplified, you get very durable, dust- and moisture-immune probes that interface to most surfaces.

An iButton reader draws virtually no power in standby mode and less than 2mA during communications, making them ideal for battery-powered devices such as stand-alone electronic parking meters or transit turnstiles. With power requirements this low, you change batteries every few years instead of every few months. Reading an iButton's unique address is also quick, taking no more than 10ms. A complete authentication, account validation, and balance update take less than 100ms.

A Choice of Products for Any eCash Need

iButton with a Globally Unique Account Identifier

The DS1990A, simplest of all iButtons, contains only the unique 64-bit ROM address. Used in online systems, this unique ID replaces less durable and unreliable alternatives like plastic cards with embossed alphanumerics, barcodes, or magnetic-stripe account identifiers.

iButtons with Password-Protected Access

You can limit access to secure data, like an account balance, by using the DS1991 or DS1977. These iButtons require a host to know the password for any read or write operation. The DS1991 has three service data pages, so a single device accommodates three completely independent service providers. Each 48-byte page of secure memory has its own 64-bit access password and service ID. Additionally, an unprotected 64-byte scratchpad memory serves as an intermediate buffer. With the correct password supplied, copying data from the scratchpad to the appropriate secure memory page is a highly reliable write operation, even in the presence of intermittent connections. Such dependable operation is critical, as it ensures that monetary balances are updated without corruption, and no loss of electronic cash occurs. For greater memory needs, the DS1977 can secure up to 32KB of data.

iButtons with Challenge-and-Response Authentication

For even greater security, we offer challenge-and-response secure memory iButtons based on the ISO/IEC 10118-3 standard hashing algorithm called Secure Hash Algorithm 1 (SHA-1). A challenge-and-response system allows two parties to share a common secret, yet never reveal that secret during communication. This permits the safe exchange of secure data. An integrated 512-bit SHA-1 engine can be activated to compute 160-bit message authentication codes (MACs) based on information stored in the iButton.

Challenge-and-response iButtons use proven algorithms and provide the best security features to thwart the most sophisticated attacks. These devices can defeat numerous known, logical security attacks including copy attack, replay attack, eavesdrop attack, A-B-A attack, and emulation attack. For more details see White Paper 8: 1-Wire SHA-1 Overview at www.iButton.com.

DS1961S—1kb EEPROM with SHA-1 engine

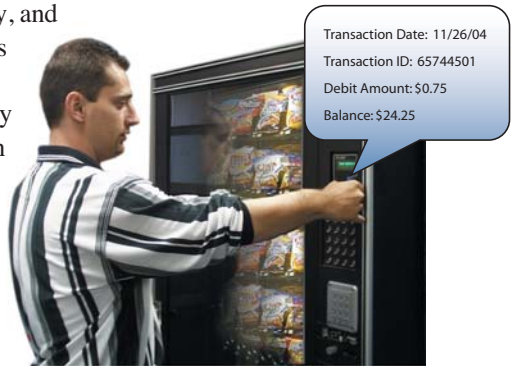
With 1kb of application memory, the DS1961S stores a single 64-bit secret that can be used in conjunction with the on-chip SHA-1 engine to prove its authenticity to an SCU. Likewise, the SCU is required to prove it is authentic before it is allowed to write data to the DS1961S. This security mechanism, called mutual authentication, is ideal for eCash applications. The account balance can be read by anyone, but only authorized SCUs can execute a transaction and alter the stored value.

DS1963S—4kb NV RAM with SHA-1 engine

The DS1963S has 4kb NV RAM and supports up to seven different applications or service providers, each with their own 64-bit secret that is never revealed to other service providers. Special counters in this iButton ensure that previous or current data patterns like cash balances cannot be extracted from the device and fraudulently rewritten later. Thus, the DS1963S treats every instance of data as unique. NV RAM technology makes brute-force physical attacks virtually impossible.

iButton with Java-Powered Cryptography

For your highest level of security, we offer the DS1955B Java™-powered cryptographic iButton. It contains a Java Card 2.0 compliant virtual machine, 6kB of NV RAM memory, and is NIST validated for conformance to FIPS PUB 140-1. The security level of this device is so high that it has U.S. Government approval for downloading postage over the Internet and printing postage from a standard printer. You are effectively printing money! In addition, with PKI challenge/response authentication you can grant access privileges to information on web pages. Even sign and approve documents so others can be assured of their origin.



Java is a trademark of Sun Microsystems.

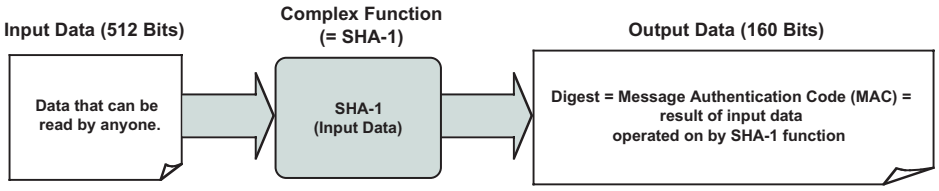
Why SHA-1 iButtons Make Exceptional eCash Purses

eCash Tokens Are Like Cash

REQUIREMENTS	CASH	eCash iButton
Must be proven authentic.	General familiarity with the look and feel of the materials, the quality of printing.	Electronically authenticated using a complex, non-reversible mathematical algorithm plus 64-bit secret.
Cannot be easily altered or duplicated.	Crude alterations are obvious; sophistication of printing process, unavailability of raw materials, legal repercussions make duplication very difficult/risky.	Same complex algorithm plus 64-bit secret ensure data has not been altered or the entire device duplicated/emulated.
Encryption versus digital signature.	Someone can directly observe the value of cash and generally determine its authenticity. No need to "encrypt" the currency value (i.e., have its value be a secret).	Anyone can directly read the value of the eCash token. Like cash, there is no need to encrypt the value, only ensure that it cannot be altered.

ISO Standard SHA-1 Algorithm Has Excellent Mathematical Properties

General Case

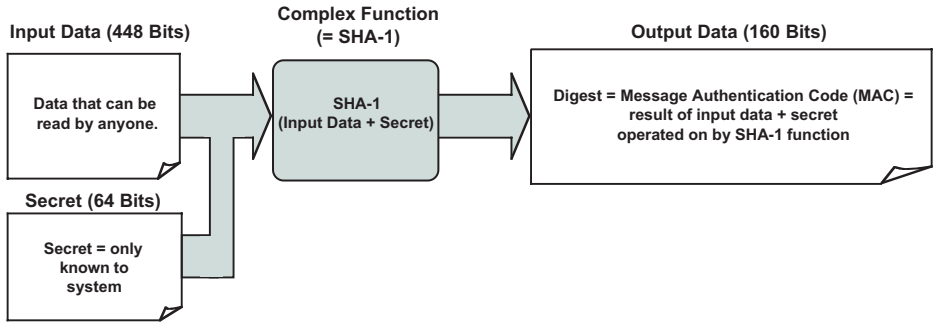


1) Input data is public.

2) SHA-1 function is public.

3) Anyone can compute corresponding output data.

Special (Secure) Case



1) Input data is public.

2) SHA-1 function is public.

3) Secret is NOT public.

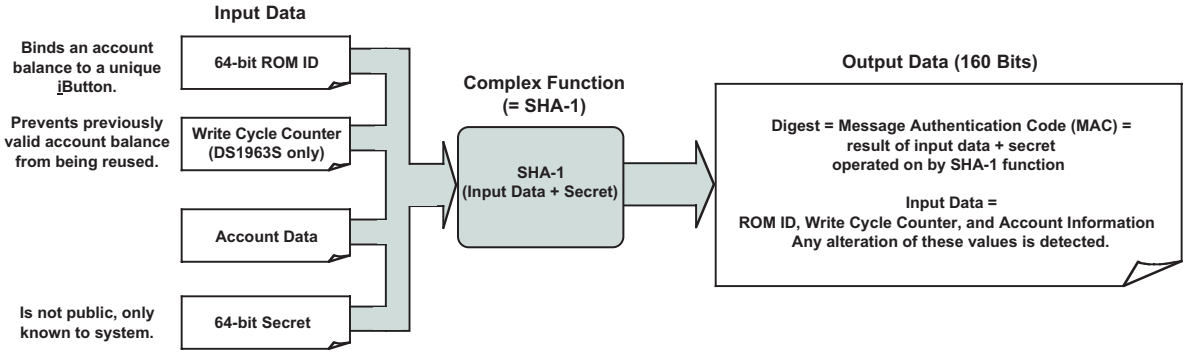
4) The SHA-1 algorithm applied to the input data plus the system secret generates a corresponding 160-bit MAC.

5) Security is created by including the 64-bit secret as part of the input to the SHA calculation.

a) The system can tell if the input data has been altered. (Recompute MAC; compare to MAC stored with input data. Match = unaltered. No Match = altered.)

b) Knowing the input data, the SHA-1 algorithm, and the 160-bit MAC still does not allow reversing the SHA-1 operation to reveal the secret.

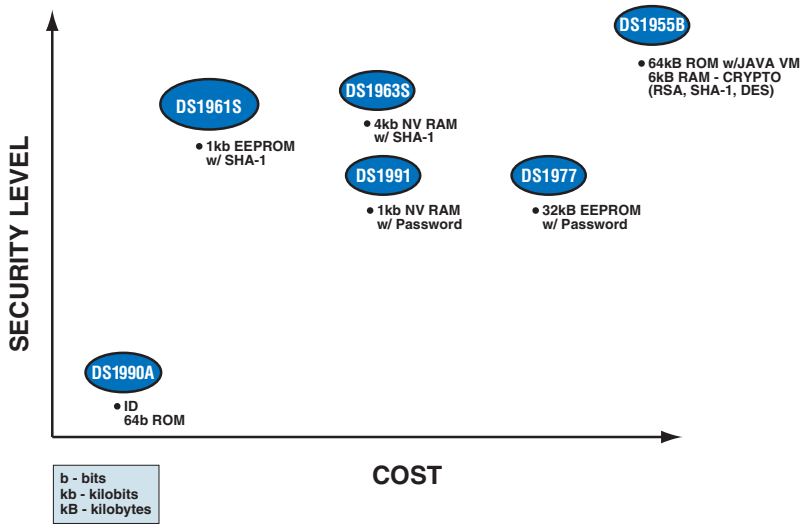
SHA-1 iButtons



iButton eCash Products Selection Guide

iButton Products' Security Continuum

iButtons are available in a wide variety of security levels to provide the most appropriate protection for your application.



REQUIREMENTS	SUGGESTED PARTS	REMARKS
Need unique ID only.	DS1990A	Easiest to implement. Ideal for simple systems that only require a unique account number as in a credit card system.
Need password-protected memory for user-access authorization.	DS1991L DS1977	Good security and easy to implement. Some customers further encrypt the service data with the device ID as one of the encrypting input parameters. The DS1991L can support three independent services.
Need challenge-and-response authentication. Want to protect against losing secret to interception.	DS1961S DS1963S	Offers higher security than static password approach. DS1961S supports four services that share the same access secret. DS1963S supports seven independent services with separate secrets.
Need strong encryption support (1024-bit key). Need PKI support.	DS1955B	The highest level of security available. FIPS PUB 140-1 compliant.
Starter Kit to explore iButton-based eCash systems.	DSECASH	The kit demonstrates the speed, reliability, and security of our DS1961S and DS1963S SHA-1 based iButtons. Kit contains all hardware and software needed to perform debits/credits and build a complete eCash system.

Turnkey Systems Available

Our Authorized Solutions Developers (ASDs) have already developed turnkey iButton systems for many eCash applications. These developers can also design custom iButton software and/or hardware solutions. Review our partners and their products at www.iButton.com/solutions.

Interface Is Simple and Low Cost

One-Touch Interface

How do I communicate with an iButton? Interfacing an iButton to any type of electronics is easy. Information transfers between an iButton and a PC, PDA, or microcontroller with a momentary contact, at up to 142kbps. Simply touch the iButton to a Blue Dot™ receptor or probe, which is connected to a port adapter. We provide low-cost adapters for USB, serial, and parallel ports.

A typical iButton probe is simple, robust, and forgiving of alignment inaccuracies and electrical resistance. Card-based systems, however, require complex electro-mechanical readers where card slots are easily vandalized, numerous electrical contacts must remain completely clean and precisely aligned, and maintenance is both difficult and constant.

iButtons are also designed to comprehend intermittent connections. Remove an iButton from the SCU at any time without worry. When the iButton touches the probe point again, the interrupted transaction is recovered successfully and completed without loss or corruption of data.

The iButton system even compares favorably to a contactless card-based system. Contactless systems' readers are significantly more complicated than contact-based readers. This adds cost and potential interoperability issues due to different frequencies and/or modulation schemes being used.

Free Software Development Tools

iButton and other 1-Wire software development kits, which address different platform and programming language preferences, are available to download from our website for free. Multiple Application Notes and White Papers reduce the development burden and help ensure your success.

PLATFORM	RESOURCE	DESCRIPTION
Windows® 32-bit (95, 98, NT, 2K, ME, XP)	1-Wire SDK	Programming language-independent library. Supports all 1-Wire adapter types with traditional API* (TMEX) and Windows COM interfaces.
Any platform with a 'C' compiler	1-Wire Public Domain Kit	Portable C library. Supports both a serial port plus DS2480B bridge or custom 1-Wire interface.
Any Java platform	1-Wire API for Java	Portable Java library. Supports both a serial port plus DS2480B bridge or custom 1-Wire interface.
Microprocessor	• Application Note 126* (I/O port pin for 1-Wire) • Application Note 192* (Serial port + DS2480B bridge for 1-Wire) • Some I/O port assembly examples in 1-Wire Public Domain (PD) Kit	Documentation to add a 1-Wire port to a microprocessor. Some assembly examples available. If the microprocessor has a 'C' compiler, the 1-Wire Public Domain code can be used.

**Refer to Application Note 155: 1-Wire Software Resource Guide for an overview of all available APIs. For all iButton application notes visit www.iButton.com.*

iButtons—More than Just an eCash Token

The iButton family has over 20 different products that meet all application needs—eCash, access control, guard tour monitors, maintenance and inspection data management, device and software authorization, and temperature data logging.

Product Quickview

	PART	DESCRIPTION		
Address Number Only	DS1990A	64-bit ROM ID		
NV RAM Memory	DS1992/3/5/6L	1kb/4kb/16kb/64kb NV RAM		
EEPROM Memory	DS1971/3/7	256-bit/4kb/32kB EEPROM		
EPROM Memory	DS1982/5/6	1kb/16kb/64kb EPROM		
Password-Protected Secure Memory	DS1991L/DS1977	Three 384-bit partitions NV RAM/One 32kB partition EEPROM		
Challenge-and-Response Secure Memory	DS1961S	1kb EEPROM with SHA-1		
	DS1963S	4kb NV RAM with SHA-1 and counters		
Real-Time Clock	DS1904/DS1994L	RTC/RTC with 4kb NV RAM		
Temperature Sensor	DS1920-F5	Enables user to collect current temperature upon contact with a reader. Digital thermometer, ±0.5°C accuracy (-55°C to +100°C)		
Temperature Data Loggers	**PART**	**TEMP RANGE**	**MAX ACCURACY**	**DATA LOG SIZE**
	DS1921G-F5	-40°C to +85°C	±1°C (-30°C/+70°C)	2k points
	DS1921H-F5	+15°C to +46°C	±1°C	2k points
	DS1921Z-F5	-5°C to +26°C	±1°C	2k points
	DS1922L-F5	-40°C to +85°C	±0.5°C (-10°C/+65°C)	4k/8k points
	DS1922T-F5	0°C to +125°C	±0.5°C (+20°C/+100°C)	4k/8k points
Temperature/Humidity Data Logger	DS1923L-F5	-20°C to +85°C	±0.5°C, 5%RH	4k/8k points

Accessories Quickview

COMM. PORT ADAPTERS		
	DS9490R	1-Wire USB Adapter: 1-Wire to USB interface. Connects to all reader/probes with RJ-11 interface.
	DS9490B	USB iButton Holder/Dongle: 1-Wire to USB interface. Insert iButton into device.
	DS9097U-S09/009/E25	Universal 1-Wire COM Port Adapter: 1-Wire to RS-232 COM port interface (DB9). Connects to all reader/probes with RJ-11 interface. 009 version includes DS2502 for ID. E25 version includes a 12V power port for writing to EPROM iButtons and comes in a DB25 package.
	DS1410E-001	1-Wire Parallel Port Adapter: 1-Wire to parallel port interface. Insert iButton directly or use with DS1402D-DB8 or DS1402BP8.
PROBES/RECEPTORS *(READER/WRITER INTERFACES)*		
	DS1402D-DR8/DB8	Blue Dot Receptor Cable: iButton read/writer interface. iButtons communicate through Blue Dot interface with just a touch or can be snapped into the Blue Dot for continuous connection. DR8 has RJ-11 interface. DB8 has button interface.
	DS1402RP8/BP8	iButton Touch and Hold Probe Cable: iButton read/writer interface. iButtons communicate through probe with just a touch or can be snapped into the probe for continuous connection. DR8 has RJ-11 interface. DB8 has button interface.
	DS9092GT	iButton Handheld Wand: Plastic wand with an integrated iButton probe, shaped to self-align with iButtons. Gives tactile feedback. The wand comes with a 10cm handle and a 1m cable that is terminated with an RJ-11 jack.
	DS9092/T/L	Panel Mount Probe. T version has tactile feedback. L version has LED and is recommended for outdoor use.
	DS1402D-041	Blue Dot probe component for embedded touch and hold applications.
iBUTTON MOUNTS		
	DS9093Ax/F/N	Key Fobs: Allow an iButton to be carried conveniently on a key chain. Available in three different versions and five different colors.
	DS9093S/P	Wall Mounts: Allow you to securely mount iButtons to most surfaces. Available in two versions.
	DS9096P	iButton Adhesive Pads. Allow you to easily mount iButtons to anything.

iButton®

Touch the Future!

WHAT'S NEW?

Overview
- What is an iButton?
- Applications
- Brochures
- Videos

iButtons
- ID Only
- Memory
- Real-Time Clock
- Secure
- Temperature

Accessories
- Readers & Adapters
- Mounting Options
- Starter Kits

Sales
- Direct
- Buy Online
- Partners
- Distributors
- Samples
- Trade Shows

Solution Partners
- Solutions Search
- Become a Partner

Contact Us
- Contacts and Support
- Sales Information

Technical Support
- Software Developer's Tools
- Data Sheets
- Application Notes
- Support
  - FAQs
  - Discussion Groups
  - E-mail Updates
- Photo Library

Translations
- Chinese 简体中文
- Japanese 日本語

Visit Our Website to Find the Latest Information on iButtons

www.iButton.com

DALLAS SEMICONDUCTOR MAXIM

Corporate Headquarters
Maxim Integrated Products
120 San Gabriel Dr.
Sunnyvale, California 94086
1-888-maxim-ic
www.maxim-ic.com

Dallas Semiconductor
iButton Product Group
4401 Beltwood Parkway
Dallas, Texas 75244
Phone: 1-888-maxim-ic
FAX: 972-371-3715
www.iButton.com

Get started today with our DSECASH iButton Starter Kit.