

DS1961S

1Kb Protected EEPROM iButton with SHA-1 Engine

World-Class Security in Stainless Steel Case for Access Control and eCash Applications

[Overview](#) [Technical Documents](#) [Ordering Info](#) [Related Products](#) [User Comments \(0\)](#) [All](#)Status 

Part Number	Status
DS1961S	Active: In Production. See Ordering Information for details.

Data Sheet

[Request Full Data Sheet](#)
NDA Required

Description

The DS1961S combines 1024 bits of EEPROM, a 64-bit secret, an 8-byte register/control page with up to five user read/write bytes, a 512-bit SHA-1 engine and a fully featured 1-Wire® interface in a rugged iButton®. Data is transferred serially via the 1-Wire protocol, which requires only a single data lead and a ground return. The DS1961S has an additional memory area called the scratchpad that acts as a buffer when writing to the main memory, the register page or when installing a new secret. Data is first written to the scratchpad from where it can be read back. After the data has been verified, a copy scratchpad command will transfer the data to its final memory location, provided that the DS1961S receives a matching 160-Bit message authentication code (MAC). The computation of the MAC involves the secret and additional data stored in the DS1961S including the device's Identity Register. Only a new secret can be loaded without providing a MAC. The SHA-1 engine can also be activated to compute 160-bit MAC when reading a memory page or to compute a new secret, instead of loading it.

The DS1961S understands a unique command "Refresh Scratchpad." Proper use of a refresh sequence (see Writing with Verification section) after a copy scratchpad operation reduces the number of weak bit failures in a touch environment. The refresh sequence also provides a means to restore functionality in a device with bits in a weak state.

Each DS1961S has its own 64-bit ROM registration number that is factory lasered into the chip to provide a guaranteed unique identity for absolute traceability. The durable stainless steel package is highly resistant to environmental hazards such as dirt, moisture, and shock. Its compact coin-shaped profile is self-aligning with mating receptacles, allowing the DS1961S to be easily used by human operators. Accessories permit the DS1961S to be mounted on almost any surface including plastic key fobs and photo-ID badges.

Key Features

- 1128 bits of 5V EEPROM memory partitioned into four pages of 256 bits, a 64-bit write-only secret and up to five general purpose read/write registers
- Write access requires knowledge of the secret and the capability of computing and transmitting a 160-bit MAC as authorization
- Secret and data memory can be write-protected (all or page 0 only) or put in EPROM-emulation mode ("write to 0", page 1)
- On-chip 512-bit SHA-1 engine to compute 160-bit MAC and to generate secrets
- Reads and writes over a wide voltage range of 2.8V to 5.25V from -40°C to +85°C
- Communicates to host with a single digital signal at 14.1kbps per second using 1-Wire protocol
- On-chip 16-bit CRC generator for safeguarding data transfers
- Overdrive mode boosts communication speed to 125kbps
- Operating temperature range from -40°C to +85°C
- Minimum 10 years of data retention at 85°C

Common iButton Features

- Unique, factory-lasered and tested 64-bit registration number (8-bit family code + 48-bit serial number + 8-bit CRC tester) assures absolute traceability because no two parts are alike
- Multidrop controller for 1-Wire net
- Digital identification and information by momentary contact
- Chip-based data carrier compactly stores information
- Data can be accessed while affixed to object
- Button shape is self-aligning with cup-shaped probes
- Durable stainless steel case engraved with registration number withstands harsh environments
- Easily affixed with self-stick adhesive backing, latched by its flange, or locked with a ring pressed onto its rim
- Presence detector acknowledges when reader first applies voltage

Key Specifications:

iButton Products								
Part Number	Applications	Memory Type	Memory Size	Security Features	Unique Ware	Real Time Clock	Smallest Available Pkg. (mm²)	
							max w/pins	See Notes
DS1961S	Electronic Access Control eCash	EEPROM	1K bits	SHA-1 Write-Only Secrets	No	No	301	\$2.22 @1k

[See All iButton Products \(26\)](#)

Pricing Notes:

This pricing is BUDGETARY, for comparing similar parts. Prices are in U.S. dollars and subject to change. Quantity pricing may vary substantially and international prices may differ due to local duties, taxes, fees, and exchange rates. For volume-specific prices and delivery, please see the [price and availability](#) page or contact an authorized distributor.

Diagram



Technical Documents

Product Guide 5163 1-Wire® Products

Tutorial 148 Guidelines for Reliable Long Line 1-Wire® Networks

App Note 151 Maxim Digital Monetary Certificates

App Note 154 Passwords in SHA Authentication

App Note 159 Software Methods to Achieve Robust 1-Wire® Communication in iButton® Applications

App Note 190 Challenge and Response with 1-Wire® SHA Devices

Reference Design 244 Advanced 1-Wire Network Driver

App Note 1098 White Paper 3: Why are 1-Wire SHA-1 Devices Secure?

App Note 1099 White Paper 4: Glossary of 1-Wire SHA-1 Terms

Tutorial 1201 White Paper 8: 1-Wire® SHA-1 Overview

App Note 1770 Securing Electronic Transactions Using SHA-1 Secure Hash Algorithm

App Note 1820 White Paper 1: SHA Devices Used in Small Cash Systems

App Note 3522 White Paper 9: Are SHA-1 Devices Still Secure Enough?

Tutorial 3675 Protecting the R&D Investment—Two-Way Authentication and Secure Soft-Feature Settings

App Note 3808 What Is an iButton?

App Note 4255 How to Power the Extended Features of 1-Wire® Devices

App Note 4421 Alternatives to the DS1991L MultiKey iButton®

Reference Design 4477 Reference Design of a 1-Wire® Bidirectional Voltage-Level Translator for 1.8V to 5V

App Note 4784 Secure Access Control Through Challenge and Response Authentication

Brochure 5039 Access Control Brochure

Product Guides

1-Wire® Products (PDF)

Reliability Reports

Reliability Report: [DS1961S.pdf](#)

Software/Models

none

Ordering Information

Filters: Part Number: <input type="text"/> Package: <input type="button" value="Any"/> Temperature: <input type="button" value="Any"/> <input type="checkbox"/> Tape and Reel <input type="checkbox"/> Sample <input type="button" value="Go"/>								
Part Number	Notes	Free Sample	Buy	Status 	Recommended Replacement	Package: TYPE PINS FOOTPRINT DRAWING CODE/VAR *	Temp	RoHS/Lead-Free? Materials Analysis
DS1961S-002/2-F5		N/A	No Longer Available	DS1961S-002+2-F5	CAN; Land Pattern: Not Available	0°C to +70°C	See data sheet	
DS1961S-002/3-F5		N/A	No Longer Available	DS1961S-002+3-F5	CAN; Land Pattern: Not Available	0°C to +70°C	See data sheet	
DS1961S-002/5-F5		N/A	No Longer Available	DS1961S-002+5-F5	CAN; Land Pattern: Not Available	0°C to +70°C	See data sheet	
DS1961S-002/6-F5		N/A	No Longer Available	DS1961S-002+6-F5	CAN; Land Pattern: Not Available	0°C to +70°C	See data sheet	
DS1961S-002/7-F5		N/A	No Longer Available	DS1961S-002+7-F5	CAN; Land Pattern: Not Available	0°C to +70°C	See data sheet	
DS1961S-F3		N/A	No Longer Available	DS1961S-F3+	CAN; Land Pattern: Not Available	-40°C to +85°C	See data sheet	
DS1961S-F3#		N/A	No Longer Available	DS1961S-F3+	CAN-F3;2 pin;301 mm² Outline Drawing: 21-0252 (PDF) Land Pattern: Not Available Use PkgCode/Var: IB#3NT*	-40°C to +85°C	RoHS/Lead-Free: RoHS Qualified Materials Analysis	
DS1961S-F3+		Buy	Active		CAN-F3;2 pin;301 mm² Outline Drawing: 21-0252 (PDF) Land Pattern: Not Available Use PkgCode/Var: IB#3NT*	-40°C to +85°C	RoHS/Lead-Free: Lead Free Materials Analysis	
DS1961S-F5	F5 MicroCan	N/A	No Longer Available	DS1961S-F5+ DS1961S-F5#	CAN; Land Pattern: Not Available	0°C to +70°C	See data sheet	
DS1961S-F5#		N/A	No Longer Available	DS1961S-F5+	CAN-F5;2 pin;301 mm² Outline Drawing: 21-0266 (PDF) Land Pattern: Not Available Use PkgCode/Var: IB#5NT*	-40°C to +85°C	RoHS/Lead-Free: RoHS Qualified Materials Analysis	
DS1961S-F5#		N/A	No Longer Available	DS1961S-F5+	CAN-F5;2 pin;301 mm² Outline Drawing: 21-0266 (PDF) Land Pattern: Not Available Use PkgCode/Var: IB#5NT*	-40°C to +85°C	RoHS/Lead-Free: RoHS Qualified Materials Analysis	
DS1961S-F5#V		N/A	No Longer Available		CAN; Land Pattern: Not Available	0°C to +70°C	See data sheet	
DS1961S-F5+		Buy	Active		CAN-F5;2 pin;301 mm² Outline Drawing: 21-0266 (PDF) Land Pattern: Not Available Use PkgCode/Var: IB#5NT*	-40°C to +85°C	RoHS/Lead-Free: Lead Free Materials Analysis	

Notes:

1. Other options and links for purchasing parts are listed at <http://www.maxim-ic.com/finds>, parts, usually within one business day.
2. Didn't Find What You Need? Ask our applications engineers. Expert assistance in finding parts, usually within one business day.
3. Part Number or Maxim Product Naming Conventions: + = RoHS/lead-free; # = RoHS/lead-exempt; -U/+U = cut tape; More. See [Full](#)
4. Some packages have variations in the drawing. "PkgCode/Var" tells which variation the product uses. Note that "+" "-" "#" "-" in the part

number suffix describes RoHS status. Package drawings may show a different variation suffix which character the part uses.

Similar Products by Function

[See All iButton Products \(26 Products\)](#)

Similar Products by Application

[Networked Access Control > iButton](#)

More Information

New Product Press Release [2002-09-04]

Didn't Find What You Need?

Next Day Product Selection Assistance from Applications Engineers

Applications Help

Technical Support

Product Information

Lead-Free Information

RoHS/Lead-Free

RoHS/Lead-Free