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

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 14.1kb 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 Pckg. (mm^2)	Budgetary Price
							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

More Information

New Product Press Release[2002-09-04]

Didn't Find What You Need?

Next Day Product Selection Assistance from Applications Engineers
Parametric Search
Applications Help

Information Index

Rev 3; 2009-09-02
This page last modified: 2011-04-04