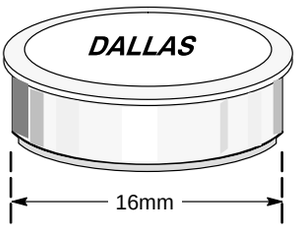
DALLAS SEMICONDUCTOR

DS1425
Multi iButton

FEATURES

- Provides a unique 64–bit serial number and three 384 bit fields of password protected RAM
- Intelligent response generator included
- No external power required
- Uses inexpensive 1–Wire™ protocol
- Universally portable across platforms

PACKAGE OUTLINE



DESCRIPTION

Authorization iButtons are sophisticated microelectronics, sealed into miniature stainless steel cans, creating a low cost, portable medium for storing and controlling access to sensitive information.

iButtons are used with port adapters as a hardware based protection system for software. iButtons help protect the right to copy software by actually protecting the right to execute it. Software can now be locked to a user, a machine, or an application with a complete audit trail and guaranteed uniqueness.

The DS1425 provides a 64–bit unique ID number, and three 384 bit fields of password protected RAM. The DS1425 is used to provide nested levels of protection, or to protect multiple applications.

Hardware communication with the iButtons is conducted via a 1–Wire interface. The conversion from a PC I/O port to the 1–Wire interface is the responsibility of the port adapter.

Software applications communicate with the iButton using Dallas' Access System, which is contained in any of the port adapter Developer's kits. The Access System provides easy to use commands which are embedded into the application in order to utilize the iButton resources during run time.

Each Dallas iButton is uniquely serialized with a 64–bit code that is laser–etched in the silicon. This unique ID provides a basic level of security, is traceable in the field, and makes it possible to identify the specific iButton in a field of many.

The serial number is divided into three parts (see Figure 1). The 8–bit family code tells the Access System (and consequently the developer) what type of iButton is being used. The next 48 bits are lasered sequentially with no two numbers the same. The last 8 bits contain a Cyclic Redundancy Check (CRC) value that has been calculated across the family code and the 48–bit serial number. The CRC ensures that iButton communication is error free.

High levels of security are achieved by storing application code and/or data necessary for execution in the iButton memory.

Each 384–bit secure data area is prefaced by a 64–bit identification field and an unreadable 64–bit password. Note that this password is user selected and programmed. This means no one, including Dallas Semiconductor, can access that data.

If the DS1425 is presented with a valid password from the host application, the contents of the secure data will be returned. However, if the DS1425 is presented with an invalid password, the on–board intelligent response generator will return what seems to be a normal response, but is not. The false response will be unique to the false access.

By using seemingly random data in both the password and secure data fields, and by generating many false accesses for each valid access, even sophisticated attackers are defeated.

DS1425 MULTI iButton ORGANIZATION Figure 1