Keywords: multikey, ibutton, replacement, alternative, security, password, authentication, challenge, response

APPLICATION NOTE 4421

Alternatives to the DS1991L MultiKey iButton®

By: Bernhard Linke, Principal Member Technical Staff

Jun 04, 2009

Abstract: The DS1991L multikey iButton was manufactured by Maxim in a 6-inch wafer fabrication facility using a manufacturing process that eventually became outdated and unsustainable. The password protection provided by the DS1991 is also no longer a state-of-the-art form of data security. Maxim has introduced other devices with higher levels of security that are cost effective relative to the DS1991L. Therefore, in light of the prohibitive development cost of moving the older device to a newer manufacturing process, Maxim performed a last-time build of the DS1991L and is encouraging all DS1991L customers to transition to newer and more secure iButton devices before the existing stock runs out. This application note discusses three alternatives for upgrading existing DS1991L applications. Each alternative takes advantage of these newer products.

Introduction and Background on the DS1991L

Password protection is no longer *state-of-the-art*. The major weakness of password-based system is that eavesdropping on the communication eventually reveals the password.

Since the DS1991L does not provide any write protection, a malicious attacker can easily overwrite a key's information (identifier, password, data) to make the device fail in its application. Devices with challenge-and-response authentication and the encryption of application data are more secure and cost-effective alternatives.

The 1-Wire® master in a DS1991L application must know how to identify the key of interest and must know the respective password. Before a DS1991L can be used, the identifier, password, and key data must be installed. After that, the device is ready for the field, where key data is accessed and often changed. The NV SRAM technology with internal battery is an advantage here, since the copy process from the scratchpad to the key's data field progresses undisturbed even if contact with the master (probe) is lost.

Alternatives to the DS1991L

Three iButtons can be considered as a replacement for the DS1991L. These devices are the DS1977, DS1961S, and DS1963S. **Table 1** shows how these devices compare to the DS1991L and to each other.

Like the DS1991L, the DS1977 uses password security and could generally be regarded as a close relative. The DS1961S and DS1963S employ SHA-1-based authentication, which uses secrets. Unless encrypted, application data is open and readable. The DS1961S and DS1977 use EEPROM technology.

The DS1963S uses NV SRAM.

Table 1. Device Comparison

	Part Numbers			
Characteristic	**DS1991L**	**DS1977**	**DS1961S**	**DS1963S**
User memory	3 x 48 bytes, called keys	32K bytes	128 bytes	8 x two pages of 32 bytes (total 512 bytes)
Security	Three individual 8-byte passwords (one for each key); same password for read and write	Two 8-byte passwords (one for read and one for full access)	One 8-byte secret; secure write	Eight 8-byte secrets
Data management	Three 8-byte key identifier fields (one for each key)	1-Wire file system recommended	1-Wire file system recommended	1-Wire file system recommended
Data buffer for intermediate storage and data verification	64-byte scratchpad	64-byte scratchpad	8-byte scratchpad	32-byte scratchpad
Authentication	—	—	3-byte challenge; 20-byte MAC response	3-byte challenge; 20-byte MAC response
Write cycle counters	0	0	0	16 (8 for memory pages and 8 for secrets)
Technology	NV SRAM	EEPROM	EEPROM	NV SRAM
Power source	Internal battery	Parasitic supply from master	Parasitic supply from master	Internal battery
1-Wire speed	Standard	Standard and overdrive	Standard and overdrive	Standard and overdrive
Relative cost[1]	—	Higher than DS1991L	Much lower than DS1991L	Somewhat higher than DS1991L
Temperature range	-40°C to +70°C	-40°C to +85°C	-40°C to +85°C	-40°C to +85°C
Extras	Pseudo-random data generator to create false data when the password does not match	Can be used without password protection	Write protection of memory and secret; EPROM emulation mode	Pseudo-random number generator; can be used as SHA-1 coprocessor

[1] For the actual product prices, please refer to the ordering information and price data on the Maxim website.

DS1977 Password-Protected 32KB EEPROM iButton

Compared to the DS1991L, the DS1977 has significantly more memory (32KB); supports 1-Wire overdrive speed; and uses two passwords, one for read access and the other for full access. The password protection can be disabled, making the DS1977 usable in applications that do not need security. Although higher in cost than the DS1991L, the per-byte cost of the DS1977 is the lowest of all alternatives and the DS1991L.

Due to the EEPROM technology, the 1-Wire master in a DS1977 application must implement a strong pullup to deliver power for read and write access. In a touch environment this can cause reading errors and requires extra precautions when writing. The 1-Wire master must know at least one password (read access or full access) if passwords are enabled. As with any password-based system, eavesdropping on the communication may eventually reveal the passwords.

Before the DS1977 can be used with password protection, the passwords need to be installed and enabled. For optimal use of the large memory, it is recommended that you format and use the memory according to the 1-Wire file system. (See application note 114, "1-Wire File Structure.") Next, the application's files (or data) need to be written to the DS1977. After that, the device is ready for use in the field, where memory data is accessed and often modified.

To upgrade an existing DS1991L application for the DS1977, one needs revised application software that recognizes the new part, knows its commands, and operates the strong pullup for power delivery at the right time. As a general recommendation, before changing passwords one first should disable the passwords. When installing a password, it is critical to ensure that all eight bytes of the password are defined. Always verify the scratchpad contents before issuing the Copy Scratchpad command. After a new password is successfully copied from the scratchpad to its memory location, the scratchpad should be overwritten with different data to erase any remains of the password in the "open space." For reliable operation in a touch environment, it is highly recommended that you implement the data integrity measures described in application note 159, "Software Methods to Achieve Robust 1-Wire® Communication in iButton® Applications."

DS1961S 1Kb Protected EEPROM iButton with SHA-1 Engine

The DS1961S offers significantly higher security than the DS1991L. The DS1961S uses EEPROM technology and supports 1-Wire overdrive speed. Instead of passwords, the device's security is based on a secret that is installed, but never again communicated (exposed) in the field. This secret can be device specific, e.g., computed according to the SHA-1 algorithm using a master secret, memory data, registration number, and constants. Except for the secret, all the data stored in the DS1961S is readable to the public. Write access, however, requires the knowledge of the secret. Encryption is required to prevent the public from understanding the data stored in the device. The DS1961S has the lowest cost of these alternatives, including the DS1991L. Due to its EEPROM technology, the DS1961S gets its energy for operation from the 1-Wire master. In a touch environment, the risk of data corruption when writing is higher than with an NV SRAM device.

In a 5V-environment with a pullup resistor of 2.2kΩ or lower, the 1-Wire master in a DS1961S application need not implement any special power-delivery feature. If the pullup voltage is less than 5V, one could lower the pullup resistor value (this is the easiest way, see application note 4255, "How to Power the Extended Features of 1-Wire Devices") or implement a strong pullup to provide the extra power for writing and running the SHA-1 engine in the device. The DS1961S master must know, or be able to compute, the secret necessary to authenticate a DS1961S as member of the system and to modify its EEPROM data. Instead of computing SHA-1 MACs (message authentication codes) itself, the master could use the DS2460 SHA-1 coprocessor with EEPROM.

Before the DS1961S is ready for use, the device's secret must be defined and installed. A computed secret is more secure than a fixed (constant) secret that is loaded like a password. Next, the data needed in the application must be written to the device. With the relatively small memory, the use of the 1-Wire file system is optional. If appropriate, one or all memory pages as well as the secret can be write protected to prevent changes in the field. One of the memory pages can be put into EPROM emulation mode, where bits can only change from 1 to 0; this feature may be useful in some applications. After the initial setup, the DS1961S is ready for use in the field, where memory data is accessed and often modified.

To upgrade an existing DS1991L application for the DS1961S, two changes are necessary:

1. Revised application software that recognizes the new part and knows how to use it.
2. If operating in a low-voltage environment, the software must activate the strong pullup for power delivery during the computation and installation of a new secret, for the computation of a page MAC, and for updating the EEPROM.

Always verify the scratchpad before issuing the Copy Scratchpad command. For reliable operation in a touch environment, it is highly recommended that you implement the data integrity measures described in application note 159 (see above). For additional reading about SHA-1 security, refer to the application notes listed at the end of this document. Of particular interest is application note 1820, "White Paper 1: SHA Devices Used in Small Cash Systems," which describes the use of the DS1961S as token in an electronic cash application.

DS1963S SHA iButton

The DS1963S offers a significantly higher level of security than the DS1991L. The DS1963S uses NV SRAM technology, implements write cycle counters for memory pages and secrets, and supports 1-Wire overdrive speed. Like the DS1961S, the DS1963S uses secrets for authentication; the secrets are installed but never communicated (exposed) in the field. The device supports 8 secrets, which are associated to two memory pages each. These secrets can be device specific, e.g., computed according to the SHA-1 algorithm using a master secret, memory data, registration number, page number, and constants. Except for the secrets, all the data stored in the DS1963S is readable to the public. Encryption is required to prevent the public from understanding the data stored in the device. Unlike the DS1961S, data in the DS1963S can be changed without knowing any secret; the device does not have a write-protect function for memory pages or secrets. The DS1963S costs less than the DS1977; if four or more applications share a DS1963S, the per-application cost is lower than any other alternative. Due to its NV SRAM technology, the read, write, and SHA-1 computation energy is taken from an internal battery. This is particularly advantageous for writing. Once the Copy Scratchpad command is accepted, the connection to the master can be lost without affecting the data transfer to a memory page or secret.

The memory data in the DS1963S can be modified without knowing any secret. Consequently, a portion of the device's available application data space must be reserved for storing a "signature", which is used to verify the authenticity of the application data. This additional authentication step takes place after the device has been authenticated through challenge and response, using the internal secret associated to the memory page of interest. The signature could be a 20-byte SHA-1 MAC. The secret used to compute the signature is typically not stored in the DS1963S; in addition to the device authentication secret, the signature's secret must be known to the master so it can verify the authenticity of data and create authentic data to be written to the device. Instead of computing SHA-1 MACs itself, the master could use the DS2460 SHA-1 coprocessor with EEPROM. To prevent replay attacks where old data is restored (e.g., in an electronic cash application after a purchase is made), the computation of the embedded signature must include the page's write-cycle counter value.

Before the DS1963S is ready for use, the application's device authentication secret must be defined and installed. A computed secret is more secure than a fixed (constant) secret that is loaded like a password. Next, the data needed in the application, including a valid embedded signature for data authentication, must be written to the device. To allow multiple applications to share a single DS1963S, the use of the 1-Wire file system is recommended. After the initial setup, the DS1963S is ready for use in the field, where memory data is accessed and often modified.

To upgrade an existing DS1991L application for the DS1963S, one needs revised application software that recognizes the new part; knows its commands; can identify the relevant data page(s); and can verify the authenticity of the device and the data stored in it. Typically, the application changes memory data in the field, which requires computing and embedding a valid signature in the new page data. Always verify the scratchpad before issuing the Copy Scratchpad command. For reliable operation in a touch environment, it is highly recommended that you implement the data integrity measures described in application note 159. For additional reading about SHA-1 security, refer to the application notes listed at the end of this document. Of particular interest is application note 1820, which describes the use of the DS1963S as token as well as SHA-1 coprocessor in an electronic cash application.

Making a Decision

Each of the device alternatives presented above requires either major changes to the existing software (i.e., the DS1977) or new software development. The DS1977 will, and the DS1961S may, also require a 1-Wire master upgrade to implement strong pullup for power delivery. **Table 2** illustrates the strengths and weaknesses of each approach.

Table 2. The Alternatives at a Glance

	DS1977	DS1961S	DS1963S
Required Master Hardware Changes	Add strong pullup	Add strong pullup (if necessary)	None
Application Software Change	Revision to existing software	New software development required	New software development required
Strengths	• Much more memory than with the DS1991L, or the DS1961S and DS1963S alternatives • Separate passwords for read and full access	• Lowest cost • No password to capture • Write access requires knowledge of the device's secret • Higher security due to challenge-and-response authentication and secure write access	• No password to capture • Higher security due to challenge-and-response authentication, signature embedded in data, and write cycle counters • Up to 8 applications sharing a single device
Weaknesses	• As secure as the DS1991L • Single application or multiple applications using the same secret	• Single application or multiple applications using the same secret	• Data can be changed or invalidated without knowing any secret

If hardware changes (strong pullup) are not an option, then the DS1977 is not a viable alternative.

If the hardware interface does not support enough current to communicate with a DS1961S, then the DS1963S is the only choice. Since the security with this device is based on secrets (not passwords), the DS1963S is more secure and can be more cost effective if four or more applications share a single device. The application software for the DS1963S is more complex, but not necessarily slower than with the DS1991L because of 1-Wire overdrive speed. The downside to the DS1963S is that it has less space for data per application due to the embedded signature. However, a single application can use multiple data pages and secrets to compensate for that.

If a system overhaul to implement strong pullup is an option or not required, then the DS1961S is a very cost-effective option. Using the DS1977 requires the smallest changes in the application software since its concept is closest to the DS1991L.

Summary

This application note discusses three devices to upgrade existing DS1991L applications and take advantage of newer technology. Each device requires changes—some significant—to the application software and the 1-Wire master hardware, except for the DS1963S and probably the DS1961S. Although significant software changes will be required, converting to the SHA-1 authentication-based application improves the security and can be more cost effective than the DS1991L. Software changes to implement SHA-1 security can be simplified using the DS2460 SHA-1 coprocessor.

Further Reading

Application Note #	Title	Comment	Applicability
114	1-Wire File Structure	Full disclosure of the details of the 1-Wire file system.	Any memory iButton; N/A for DS1991L
152	SHA iButton Secrets and Challenges	General recommendations on the use of secrets and challenges for challenge-and-response applications.	DS1961S, DS1963S
159	Software Methods to Achieve Robust 1-Wire® Communication in iButton® Applications	Detailed recommendations to create software for iButton communication in a touch environment.	Any memory iButton
190	Challenge and Response with 1-Wire® SHA devices	Introduction of the challenge-and-response authentication concept.	DS1961S, DS1963S
1098	White Paper 3: Why are 1-Wire SHA-1 Devices Secure?	Explanation of various attack methods and how they are defeated by SHA-1 security.	DS1961S, DS1963S
1099	White Paper 4: Glossary of 1-Wire SHA-1 Terms	Explanation of technical terms found in conjunction with challenge-and-response authentication.	DS1961S, DS1963S
1201	White Paper 8: 1-Wire® SHA-1 Overview	Explanation of SHA-1 security plus listing of additional reading.	DS1961S, DS1963S
1820	White Paper 1: SHA Devices Used in Small Cash Systems	Describes use of DS1961S and DS1963S in a monetary application; very detailed with example flow charts.	DS1961S, DS1963S
4255	How to Power the Extended Features of 1-Wire® Devices	Guidance on how to ensure power delivery for 1-Wire devices.	DS1977, DS1961S

1-Wire is a registered trademark of Maxim Integrated Products, Inc.
iButton is a registered trademark of Maxim Integrated Products, Inc.

Related Parts		
DS1961S	1Kb Protected EEPROM iButton with SHA-1 Engine	
DS1963S	SHA iButton	
DS1977	Password-Protected 32KB EEPROM iButton	Free Samples

More Information
For Technical Support: http://www.maximintegrated.com/support
For Samples: http://www.maximintegrated.com/samples
Other Questions and Comments: http://www.maximintegrated.com/contact

Application Note 4421: http://www.maximintegrated.com/an4421
APPLICATION NOTE 4421, AN4421, AN 4421, APP4421, Appnote4421, Appnote 4421

Additional Legal Notices: http://www.maximintegrated.com/legal