White Paper 7
Thermochron Mission Authentication and Security

www.maxim-ic.com

INTRODUCTION

The Thermochron is an autonomous temperature-logging device in a small 16mm steel iButton® container. It has an internal energy source that is valid for typically well over one million temperature readings. The recording is done at a user-defined rate, both as a direct storage of temperature values as well as in the form of a histogram. Up to 2048 temperature values taken at equidistant intervals ranging from 1 to 255 minutes can be stored. The Thermochron also has 512 bytes of user-programmable memory.

The applications for the Thermochron range from shipping monitoring of perishable goods or containers of temperature-sensitive chemicals to process verification. The authenticity of the temperature measurements are important since they could be used to prove shipping mishandling or provide documentation of a correct process control.

A Thermochron that has gathered temperature data is said to have been on a mission. This document explains the Thermochron's build-in hardware protection and how to augment the validation of a given temperature mission with a certificate stored in user memory.

(Special terms, commands, or codes are shown in italics for clarity.)

TAMPER PROTECTION

Thermochrons have hardware mechanisms to detect tampering of a temperature mission. The log, histogram, and alarm register memory is read-only. The only way data gets into these memory locations are through temperature measurements performed by the device. When missioning a device, a required step is a memory-clear operation. Also the mission count register indicates which portion of the logging memory is valid. With these mechanisms there is never the possibility of reading old or invalid data in the memory.

Note that the alarm flag bits indicating a violation of the temperature high or low trip points can be cleared during a mission. This is to allow an iButton reader to clear the event until the next check. However the temperature alarm register that logs the duration of the temperature violation cannot be cleared without erasing the entire memory so should be used as the 'flag' for the entire mission.

Attempting to write to any of the read-only control registers will automatically stop an ongoing mission. If someone were to attempt to defraud a system by hiding temperature violations the only option available would be to stop and erase the old mission and then start a new one. If the mission is restarted then the *mission time stamp register* and the *sample rate register* will be rewritten. The histogram and log will be cleared. Consequently the mission will contain a lower than expected number of log values. This leads to the question: how does the recipient of a missioned Thermochron know if a valid agent started the mission?

MISSION AUTHENTICATION

While the hardware mechanisms that are present in the Thermochron will prevent altering an ongoing mission there is no way to conveniently decide that it was a valid mission. Inserting a certificate into user memory at the time the mission is started can solve this. A certificate format must have the feature that it can authenticate that the missioner was a valid agent of a system. There is a well-known cryptographic

technique called a message authentication code (MAC) that can validate a message between participants that share a common secret. More specifically a MAC that uses a hash is called an HMAC. The HMAC technique is detailed in ISO/EC 9797-3 and RFC 2104. See Table 1 below presenting the input data fields to the HMAC calculation. The *random field* is used to make each of the certificates unique. The *unique registration number* is common to all iButton devices including the Thermochron.

Table 1. HMAC INPUT DATA

DATA FIELD DESCRIPTION	LENGTH (IN BYTES)
Secret known to system participants	20
Unique registration number (ROM ID)	8
Mission time stamp register	5
Sample rate register	1
Random field to make each certificate unique (also called salt)	2

The input data is put through the HMAC algorithm to produce a digest that will be included in the certificate saved to the user memory of the Thermochron. The size of the HMAC output is dependent on the hash algorithm used. The HMAC-SHA1 uses the Secure Hash Algorithm (SHA-1), which is defined in ISO/IEC 10118-3 and FIPS-180. The SHA-1 output is 20 bytes.

The user memory of a Thermochron can be utilized to hold information other then the certificate. To accommodate multiple pieces of data the 1-Wire File Structure was created (see Application Note 114). The single page (32-bytes) of data that comprises the contents of the file are considered to be the *Mission Authentication Certificate*. See Table 2 below for a complete list of the fields in a certificate based on the HMAC-SHA1.

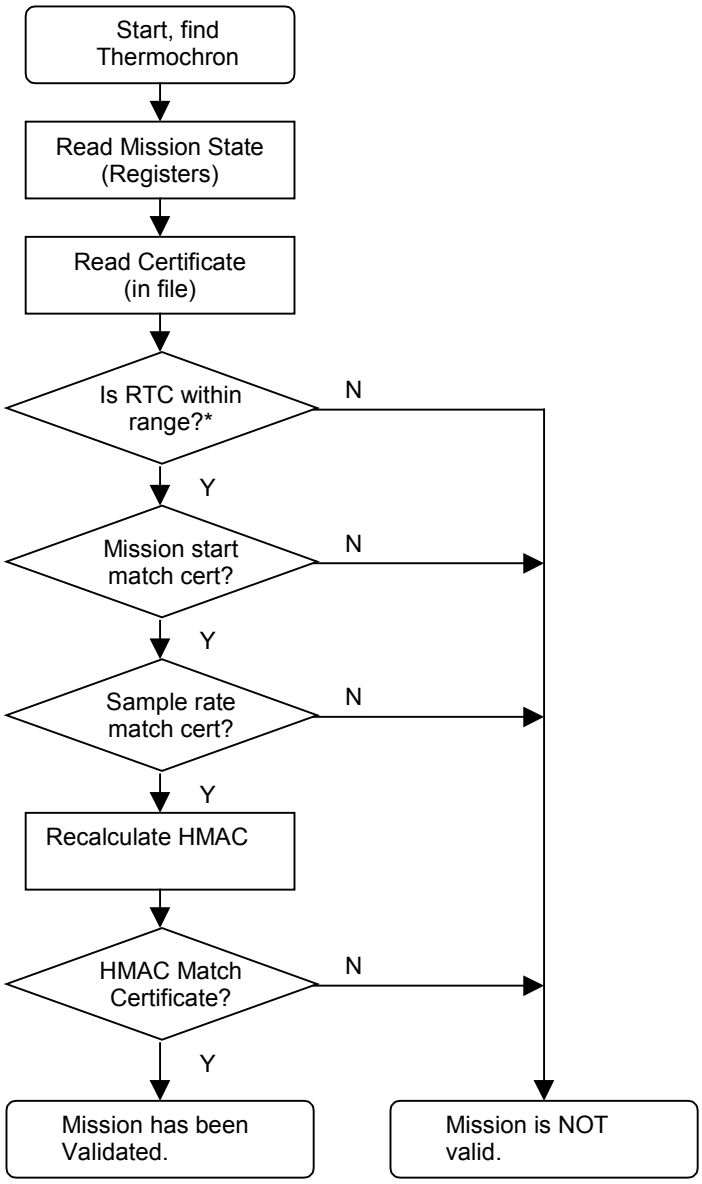
Table 2. MISSION AUTHENTICATION CERTIFICATE FORMAT

OFFSET (ON PAGE)	FIELD DESCRIPTION	LENGTH (IN BYTES)
0	Length (1-Wire file structure)	1
1	Mission start time register	5
6	Sample rate register	1
7	Random field (salt)	2
9	HMAC-SHA1 of input data	20
29	Page Pointer (1-Wire file structure)	1
30	CRC16 (1-Wire file structure)	2

The *Mission start time register* and *Sample rate register* are not strictly necessary for verification of the certificate since they can be read directly from the device's registers; however they can be valuable for tracking. If the mission is restarted and the certificate left unchanged with the old HMAC, then the original mission criteria could be recovered.

Figure 1 shows the flow a Thermochron reader uses to validate the mission of an arriving Thermochron using the defined *Mission Authentication Certificate*. Note that the real-time-clock (RTC) value must be checked against a known good source.

Figure 1. VALIDATION FLOW



*Note: The range the RTC is considered valid depends on the accuracy of the known source and the mission length.

TEMPERATURE ACCURACY

The accuracy of the Thermochron is currently specified to be ±1°C over most of the operating range. Dallas Semiconductor does not currently provide NIST traceably validation however an independent testing lab could do this and utilize the user programmable memory area to save the NIST certificate.

PHYSICAL ACCESS

Restricting physical access to the device can mitigate the risk or even the temptation of tampering of missioned Thermochron. The small size of the iButton package lends itself to inserting the entire logger inside shipping containers or even hidden.

CONCLUSION

The Thermochron has several build-in hardware mechanisms that can be utilized to detect tampering of the temperature-gathering mission. Further validation of the mission can be easily added by utilizing the user-programmable memory to hold a *Mission Validation Certificate*.

Future versions of the Thermochron family will have additional read and write password protection to help secure against tampering.

MORE INFORMATION

Federal Information Publication on SHA-1 (http://www.itl.nist.gov/fipspubs/fip180-1.htm)

RFC on HMAC (http://www.faqs.org/rfcs/rfc2104.html)

Thermochron data sheet (DS1921G) (http://pdfserv.maxim-ic.com/arpdf/DS1921G.pdf)

Thermochron data sheet (DS1921H/Z) (http://pdfserv.maxim-ic.com/arpdf/DS1921H-DS1921Z.pdf)

1-Wire file structure application note (http://pdfserv.maxim-ic.com/arpdf/AppNotes/app114.pdf)