DSECASH
eCash 评估套件

www.maxim-ic.com.cn

概述

eCash 评估套件演示基于 SHA-1 的 iButton® eCash 系统的速度、可靠性以及安全性。所提供的 eCash 支付板是完整的单机运行模块，能够在短短的 100ms 内完成资金支付。eCash 支付电路板具有串行接口，支持 PC 或微处理器监控或由人工控制支付过程。利用串口，可以将该演示板轻松地集成到实际 eCash 系统或接入控制系统。

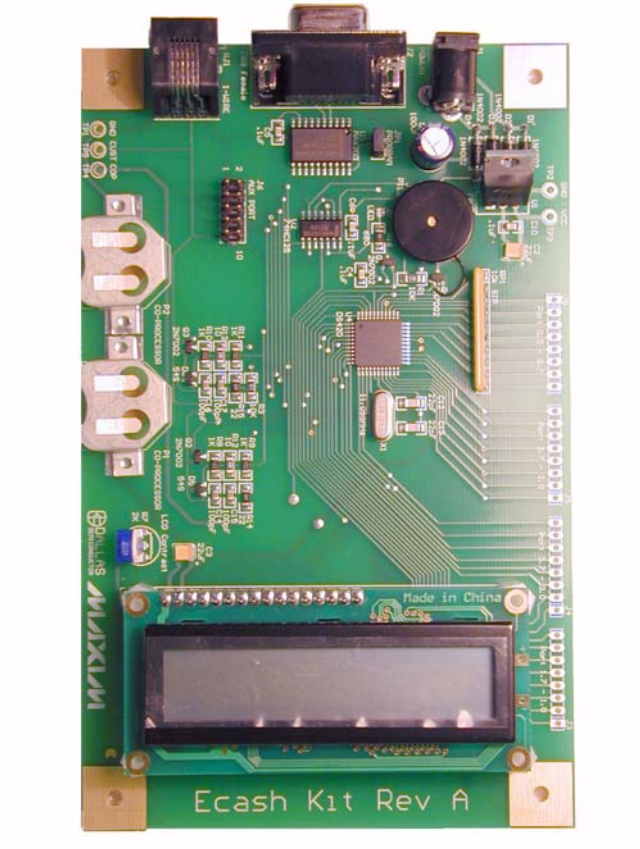
评估套件组成

(3) DS1963S – 协处理器或用户令牌
(2) DS1961S – 用户令牌
(4) DS9093A – (2) 黑色，(2) 蓝色
(1) DS1402-DR8 – iButton Blue Dot™接收器
(1) DS9097U-S09 – 1-Wire® PC 串口适配器，用于协处理器和用户令牌的 PC 初始化
(1) DB9 串口电缆 – 将评估板连接至计算机串口，监控评估板
(1) eCash 评估板
(1) 说明书

关键特性

- 单机 eCash 评估电路板，带有 LCD 显示屏和音频反馈信息
- 支持 DS1963S 和 DS1961S SHA-1 iButton 作为支付令牌
- 初始化后，支付板上的 DS1963S 协处理器使资金处于安全加密状态
- 100ms (大约)内完成 eCash 安全支付
- 提供 2 个 Java™程序(兼容于 Windows®和 Linux)供用户下载，以初始化 eCash 协处理器和令牌并监控评估板
- 评估板可组成规模更大的控制系统(服务控制单元)
- 提供简洁的‘C’程序固件
- 提供评估板原理图和元件清单
- 利用板上单指令周期、8051 兼容的 DS89C420，评估板可用于 eCash 代码开发

图1. eCash 评估板



定购信息

PART	DESCRIPTION
DSECASH	eCash Evaluation Kit

要求：

- 必须为 eCash 评估板提供外部电源。电源要求：交流/直流、9-20 V，最小 200mA。请参考下面*电源连接器*的建议。
- 初始化和软件监控需要互联网连接。

iButton 和 1-Wire 是 Dallas Semiconductor 的注册商标。
Blue Dot 是 Dallas Semiconductor 的商标。
Java 是 Sun Microsystems 的商标。
Windows 是 Microsoft Corp.的注册商标。

引言

eCash 评估套件的主要目的是演示 SHA-1 iButton，利用 Dallas Semiconductor 的其他应用笔记 (参见下表的白皮书 1)介绍的文件和安全标准，可在大约 100ms 内完成完全符合 SHA-1 认证的资金支付过程。该套件面向的应用包括：售货机、停车计费表、收费站、付费电话、公共交通、游戏等需要安全支付或者用户认证的应用。下面是和 iButton 以及 1-Wire 器件有关的应用笔记(建议从白皮书 8：“1-Wire SHA-1 概述”开始)：

表1. SHA-1 应用笔记

白皮书 8: 1-Wire SHA-1 概述
White Paper 4: Glossary of 1-Wire SHA-1 Terms
白皮书 3：为什么 1-Wire SHA-1 器件是安全的？
White Paper 1: SHA Devices Used in Small Cash Systems
App Note 150: Small Message Encryption using SHA Devices
App Note 151: Dallas Digital Monetary Certificates
App Note 152: SHA iButton Secrets and Challenges
App Note 154: Passwords in SHA Authentication
应用笔记 156：DS1963S SHA 1-Wire API用户指南
应用笔记 157：SHA iButton API概述

套件采用了一个 LCD 显示屏、两个协处理器(DS1963S 和 DS1961S)以及外部 1-Wire 和串口。协处理器和用户令牌初始化后，电路板可独立于 PC 工作。它还可以连接至 PC，以进行配置、监视和控制。开发人员利用已有的嵌入式系统，将 eCash 评估板作为大型系统的组件，加入部分简单的串行代码，来控制 eCash 电路板，迅速启动，运行基于 iButton 的支付系统。对此，演示板上提供串口和 IDC 连接器，以用于测试和试验开发。套件还提供了固件 C 源代码，因此，开发人员能够自由地扩展系统功能，或者定制系统功能。

可以从http://www.maxim-ic.com.cn/products/ibutton/ibuttons/ecashkit.cfm上下载套件工作指令和软件。软件下载中包括两个Java程序eCashInit.java和eCashMonitor.java。eCashInit程序对iButton进行初始化，用作处理器和用户令牌，eCashMonitor程序通过提供的串行电缆直接与评估板进行通信。

基本配置

为正确地设置和配置 eCash 评估板，第一步需要下载并配置软件。完成后，配置套件硬件，显示基本 SHA-1 资金支付。开发人员也可以对电路板固件进行扩展、增强或重写，装入到电路板处理器中。

软件配置

在第一次使用之前，建议首先安装并配置和套件相关的软件。然后，由软件对SHA-1 iButton进行初始化。至少需要将一个iButton设置为协处理器，一个设置为用户令牌。这可以利用PC上预先安装的Java运行环境(JRE)来完成。如果没有安装JRE，请访问http://java.sun.com，下载并安装它。

正确安装Java后，eCashInit和eCashMonitor程序都可以设置为Java “Web Start”程序。“Web Start”技术的优点之一是每次程序运行时，后台程序检查程序更新，从我们网站自动下载并安装这些更新程序。URL：http://www.maxim-ic.com.cn/products/ibutton/ibuttons/ecashjava.cfm上提供了所有程序的Java “Web Start”页面，该页面包含完整的安装和解决问题的方式。

手动安装软件

如果出于某种原因，需要手动安装 eCash 软件，可以按照以下说明进行。特别是，*RXTX 说明*、*eCashInit 设置说明*和*eCashMonitor 设置说明*等章节。

RXTX 说明

eCashInit和eCashMonitor都包含在Java程序中，需要在PC上安装RXTX 2.1。RXTX是eCashInit和eCashMonitor使用的交叉平台串行库，实现和DS9097U以及eCash评估板的通信。通过Java “Web Start”自动完成RXTX的安装，但是，在需要手动安装的情况下，Win32 构建二进制文件包含在下载的评估套件(从上述URL：http://www.maxim-ic.com.cn/products/ibutton/ibuttons/ecashkit.cfm下载)中。特别是，RXTX二进制文件在下载的software/rxtx文件夹中。如果没有采用 32 位Windows平台，可以从http://www.rxtx.org下载RXTX的二进制文件和源代码。

eCashInit 设置说明

在运行eCashInit程序之前，首先需要通过上面提到的“Web Start”(推荐使用)安装程序，也可以手动安装。重申一遍，可以从http://www.maxim-ic.com.cn/products/ibutton/ibuttons/ecashkit.cfm 下载“Web Start”。如果需要手动编译和运行，请按照以下说明进行。

编译 eCashInit：

```
javac -classpath "<path to 1-Wire API>/lib/OneWireAPI.jar;." *.java
```

运行 eCashInit：

```
java -classpath "<path to 1-Wire API>/lib/OneWireAPI.jar;." eCashInit
```

请注意，可以从eCash评估套件的Java Web Start网页http://www.maxim-ic.com.cn/products/ibutton/ibuttons/ecashjava.cfm下载OneWireAPI.jar。
也可以在网址http://www.maxim-ic.com.cn/products/ibutton/software/1wire/1wire_api.cfm提供的软件开发套件(SDK)的 1-Wire API中找到该文件。

安装并运行 Java “Web Start”程序后，自动完成对 RXTX 和 OneWireAPI.jar 的设置。

eCashMonitor 设置说明

和上面的 eCashInit 程序相似，可以通过上面提到的“Web Start” (推荐使用)来安装该程序，也可以手动安装。如果需要手动编译和运行，请按照下面的说明进行。

编译 eCashMonitor：

```
javac -classpath "<path to 1-Wire API>/lib/OneWireAPI.jar;." *.java
```

运行 eCashMonitor：

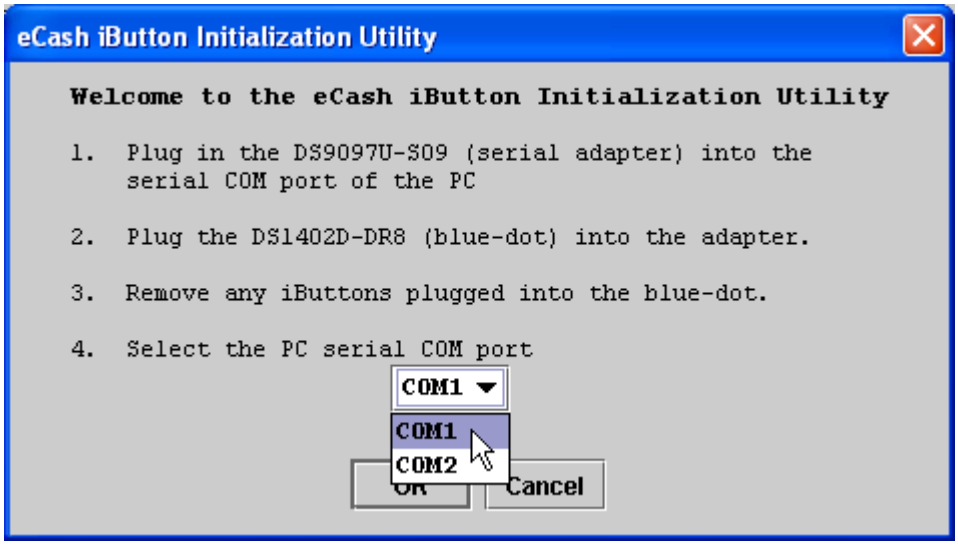
```
java -classpath "<path to 1-Wire API>/lib/OneWireAPI.jar;." eCashMonitor
```

请注意，eCashMonitor 程序还在开发中。它可以用于监控评估板及其任何 eCash 操作。它可以正确地译出所有'事件'，并以无格式英文输出(例如，发出令牌时，应正确显示该令牌的支付数量和货币平衡状况)。关于 eCash 电路板的所有命令列表，请参考*附录A：eCash 处理器*一节。

将 iButton 初始化为协处理器或用户令牌

DS9097U 1-Wire 适配器插入到串口，DS1402-DR8 Blue Dot 插入到适配器后，运行 eCashInit Java 程序，将出现以下窗口询问 DS9097U 使用哪一个 COM 端口：

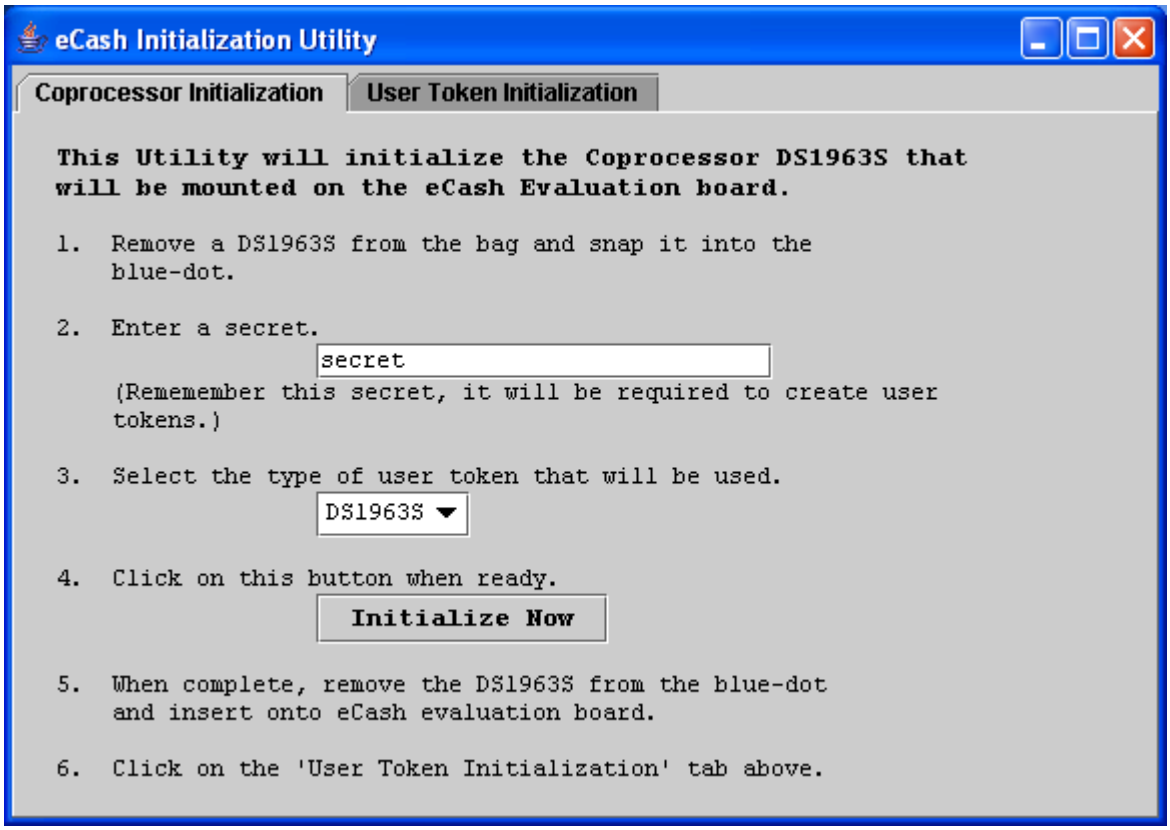
图2. eCashInit 启动屏幕



按照显示的步骤，选择合适的 COM 口。完成后，单击 OK。

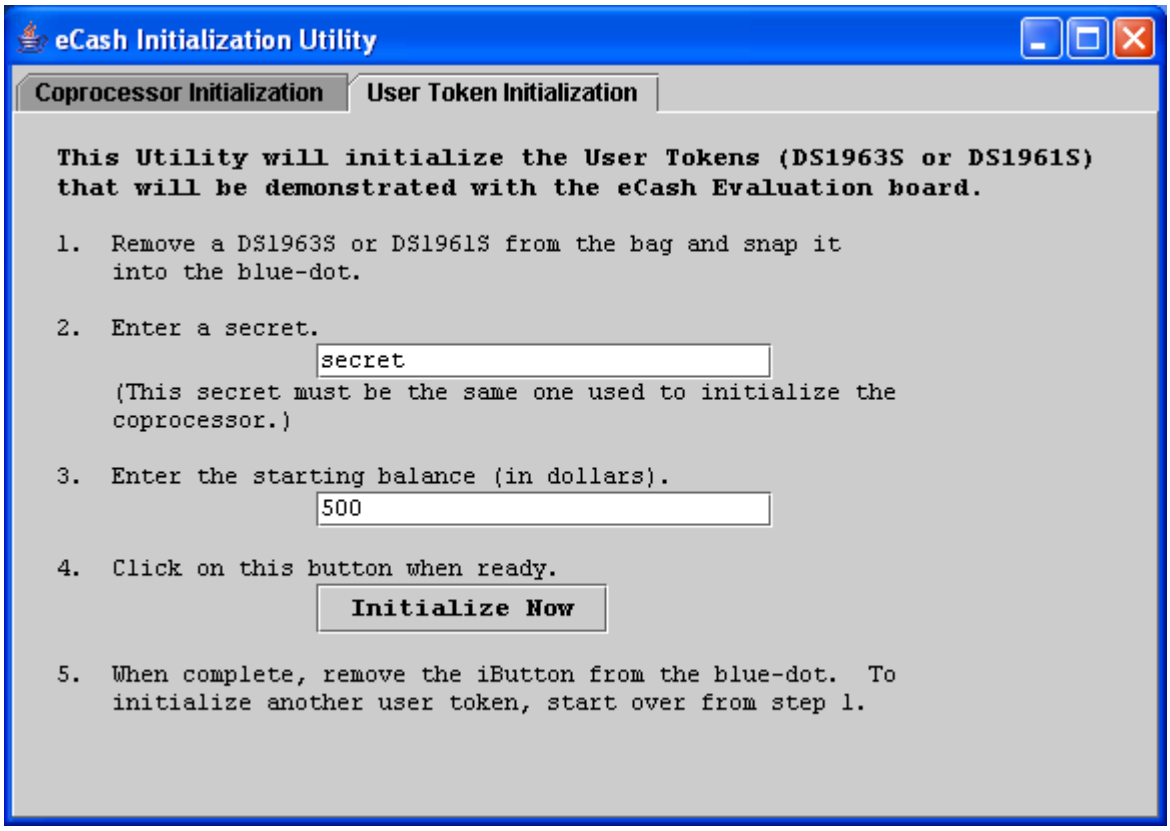
在随后出现的窗口中，可以选择两个标签。选择第一个标签，启动建立 SHA-1 协处理器的过程。按照说明，将 DS1963S iButton 插到 Blue Dot 上。完成后，将协处理器插到评估板的一个 iButton 夹上。请注意，需要指定用户令牌的类型(DS1961S 或 DS1963S)，请参考下面的截屏显示。

图3. eCashInit 协处理器初始化屏幕



eCashInit 程序的第二个标签启动用户令牌初始化过程。按照说明来建立用户令牌。用户令牌实际上承载了资金数量，需要在初始化过程中进行指定。用户令牌可以是 DS1961S 或者 DS1963S。单击“Initialize Now”按钮，完成用户令牌的建立，请参考下面的截屏显示。

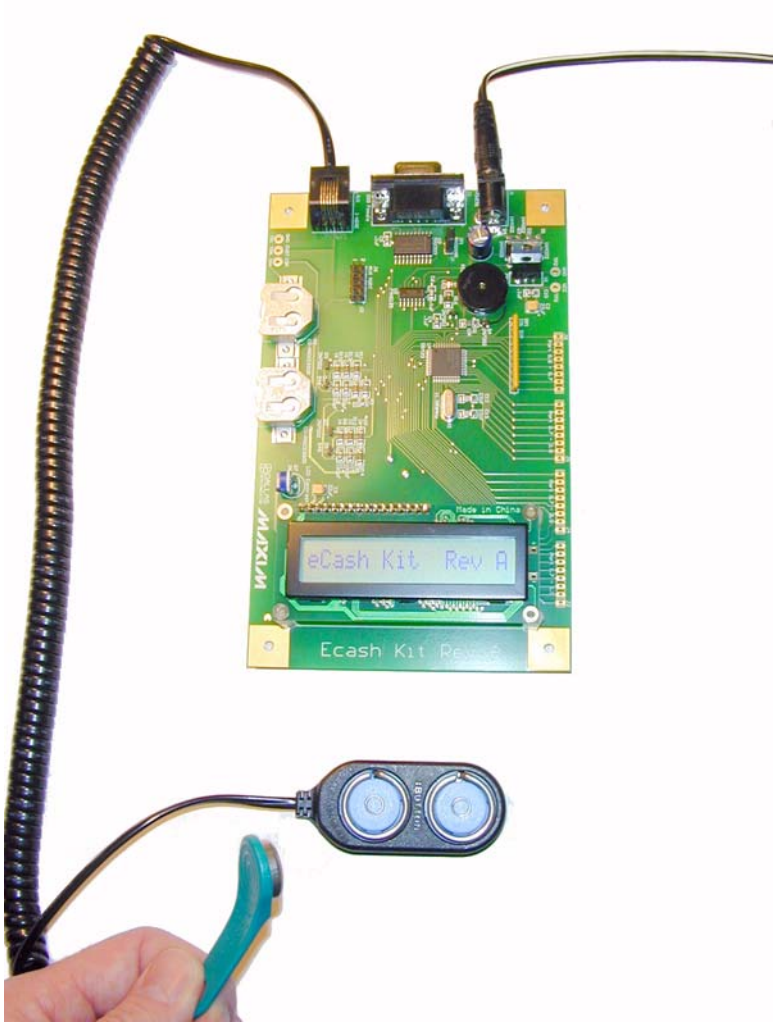
图4. eCashInit 用户令牌初始化屏幕



硬件配置

在开始 eCash 评估板的硬件设置前，至少需要建立一个协处理器和一个用户令牌(参见*软件配置*一节)。建立完成后，将协处理器插入到 eCash 评估板的 iButton 夹中。然后，从 1-Wire 适配器上拔出 DS1402-DR8 Blue Dot，将其插入到评估板的 RJ11 插槽中。最后，插上交流适配器，对 eCash 评估板进行供电，如下图所示。

图5. 硬件设置



请注意，很容易将用户令牌 iButton 插到钥匙扣上。套件提供 4 个钥匙扣。如果将 iButton 插到钥匙扣上时有困难，可以用热水浸泡钥匙扣的塑料部分，使其变软，以便容易插入 iButton。注意：请尽量不要将 iButton 浸入水中。

现在可以设置 eCash 系统。为实现系统支付，将用户令牌 iButton 按到蓝点，查看 LCD 屏上的支付显示。

快速启动

1. 将 DS9097U 插到 PC 上。Blue Dot 连接至 PC。
2. 选择 DS1963S 或者 DS1961S 作为用户令牌。
3. 将 DS1963S 初始化为令牌类专用协处理器。
4. 初始化上面第 2 步中选择的用户令牌。
5. 将协处理器放入 eCash 电路板的 iButton 夹中。
6. 将 Blue Dot 插到 eCash 电路板上。
7. eCash 电路板上电。
8. eCash 电路板上电默认状态是全自治支付。
9. 用户 iButton 支付，查看 LCD 上的结果。

评估套件用法

评估套件可以完成很多试验。以下是一些建议：

试验 1：
参见上面的安装简介。

试验 2：

1. 从 PC 上去掉 DS9097U。
2. PC 和 eCash 电路板之间连接直通串行电缆。
3. 运行 eCashMonitor 程序。
4. 改变并查看 eCash 电路板的不同工作模式。
5. 使用 eCash 电路板的各种模式，进行 iButton 支付，并监控状态。

试验 3：

1. 任意循环一个 DS1963S 用户令牌，获得所有类型的协处理器。将两个协处理夹到 eCash 电路板上，以支持所有用户令牌类型。
2. eCash 电路板进行单个 DS1963S 和 DS1961S 支付，在 LCD 上查看结果。

试验 4：
1. 利用 RS232 端口或者开发连接器，连接至其他主机/微机，实现 eCash 串行协议。

试验 5：
1. 增加固件装入跳接器，在 eCash 评估板上进行开发。

试验 6：
1. 使用固件源代码进行设计，将 eCash 功能集成到不同的电路板上。

固件

需要预先装载评估板运行的固件，我们在下载包中提供固件源代码，因此，开发人员可以扩展或者改进评估板的功能。采用 Keil C51 编译器构建固件，5.10 和 7.05 版的编译器均经过了测试。生成文件构建全部所需的文件，并进行链接。然而，Keil 链接器在链接后发出报警，返回错误状态(只是警告没有使用的部分)。执行带有'-i'选项的'make'命令，忽略这一错误，将二进制文件转换为'.hex'文件，准备装载到 DS89C420 eCash 电路中。

如果开发人员没有 Keil C51 编译器，还可以使用下载中提供的预构建 hex 文件。

装载程序说明

固件装载程序是简单的行命令串口装载器，它使用 Cygwin 核，在 Windows 上构建并进行测试。Cygwin 为串行 I/O 提供 POSIX 接口(与 Unix/Linux 相似)，因此，编译该应用程序需要 Cygwin 或另一 Unix。

可以从下面的网址下载 Cygwin：
http://www.cygwin.com.cn/

构建装载程序：
```
gcc -o load420 load420.c
```

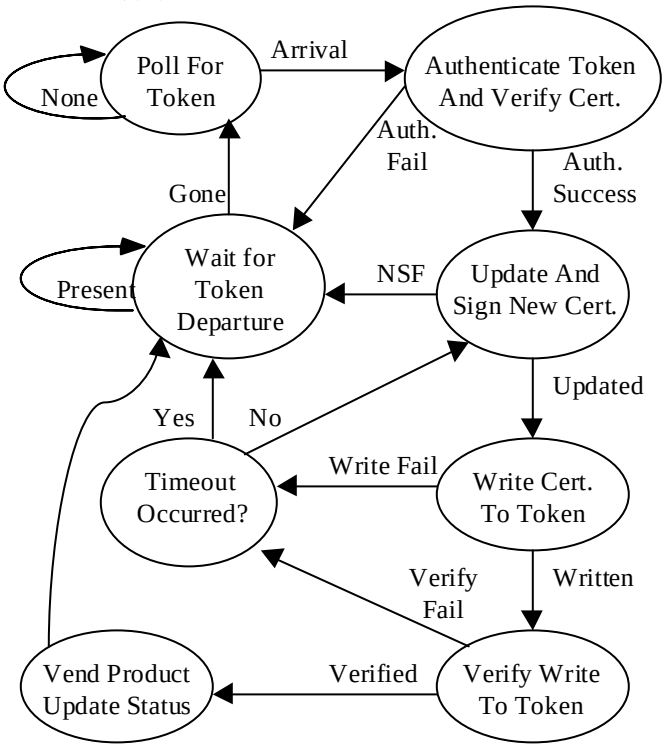
运行装载程序：
```
./load420 COM1 ../Firmware/ecash.hex
```

装载过程完成后，电路板具备了进行 eCash 支付的所有软件。

固件状态图

请参考图 6 固件状态图。

图6. 固件状态图



硬件规范

下面章节介绍评估板的硬件组成，涉及到的内容有开发板连接器、RJ11 “客户端”1-Wire 接口、DB9 串行接口、固件装载使能跳线和电源连接器等。

开发板连接器

IDC (绝缘置换连接器) 100mil 间隔。
开发连接器可用于远程监测并控制 eCash 评估板。

图7. IDC 连接器

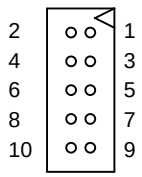


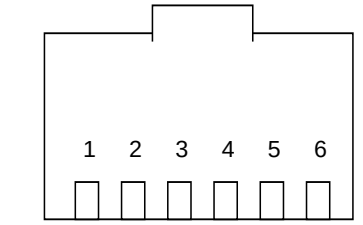
表2. IDC 连接器引脚

PIN	Signal	Description
1	VCC	5V power
2	RESET	reset to the micro
3	COP	coprocessor 1-Wire data
4	RX1	Serial port 1 receive TTL
5	TX1	Serial port 1 transmit TTL
6	INT0	Interrupt 0 on DS89C420
7	INT1	Interrupt 1 on DS89C420
8	P3.4	Port 3 bit 4 input/output
9	CUST	customer 1-Wire data
10	GND	signal ground

RJ11 1-Wire 接口

请参考下面图 8“客户端”1-Wire 接口，这是电路板外部 1-Wire 接口，用户或“客户”可以使用该接口。它提供了一个 DS1402-DR8 Blue Dot 插入位置，便于客户使用其用户令牌，完成支付。

图8. RJ11 “客户端” 1-Wire 接口



Looking into Female RJ11 Connector

表3. RJ11 “客户端” 1-Wire 接口引脚

Pin	Signal name	Description
1	VDD	+5 VDC output
2	GND	Power ground
3	OW	1-Wire Data
4	OW_GND	1-Wire ground return
5	no-connect	
6	no-connect	

DB9 串行接口

请参考下面图 9 和表 4 的 DB9 串口引脚。可采用标准直通串行电缆(套件提供)连接评估板和 PC 串口。然后利用上面提到的 eCashMonitor 程序实现与电路板的通信，请参考*附录 A：eCash 处理器*。这是电路板外部的 1-Wire 接口，用户或“客户”可以使用该接口。它为 DS1402-DR8 Blue Dot 插入提供位置，使客户能够轻松使用用户令牌，完成支付。

图9. DB9 串口

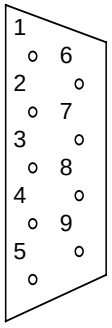


表4. DB9 串口引脚

Pin	Signal name	Description
1	no-connect	
2	RX12	RS232 Receive
3	TX12	RS232 Transmit
4	DTR	Data Terminal Ready
5	GND	Ground
6	no-connect	
7	no-connect	
8	no-connect	
9	no-connect	

图10. 固件装载使能跳线

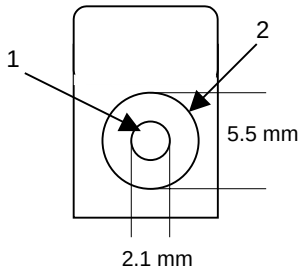
表5. 固件装载使能跳线

State	Description
JUMPER ON	Firmware loading is controlled by DTR on RS232 serial interface
JUMPER OFF	Firmware loading disabled (default)

电源连接器

电源供电要求：交流/直流、9-20 V、200mA
推荐：Stancor Model STA-300R
(Newark Electronics Stock No. 84F2081, Allied Electronics Stock No. 928-9895)

图11. 电源连接器



DSECASH 信息

关于DSECASH的详细信息，包括软件下载，请参考我们网站http://www.maxim-ic.com.cn/products/ibutton/ibuttons/ecashkit.cfm上的评估套件网页。

技术支持资源

Maxim 为开发人员提供丰富的技术支持。除了数据资料，我们还提供大量的应用笔记和白皮书、软件开发工具以及可以提交技术问题进行讨论的网络论坛。

iButton产品数据资料：http://para.maxim-ic.com/iButton.htm

1-Wire产品数据资料：http://para.maxim-ic.com/1Wire.htm

应用笔记和白皮书：http://www.maxim-ic.com.cn/appnotes10.cfm/ac_pk/1

软件开发工具和SDK：http://db.maxim-ic.com/ibutton/example/

在我们的网站论坛上提交技术问题：http://discuss.dalsemi.com/

原理图

请参考下面的电路板原理图。原理图包括：处理器 LCD 和 Piezo、协处理器和 1-Wire 客户端电路、电源以及 RS232 串口。

图12. 处理器 LCD 和 Piezo

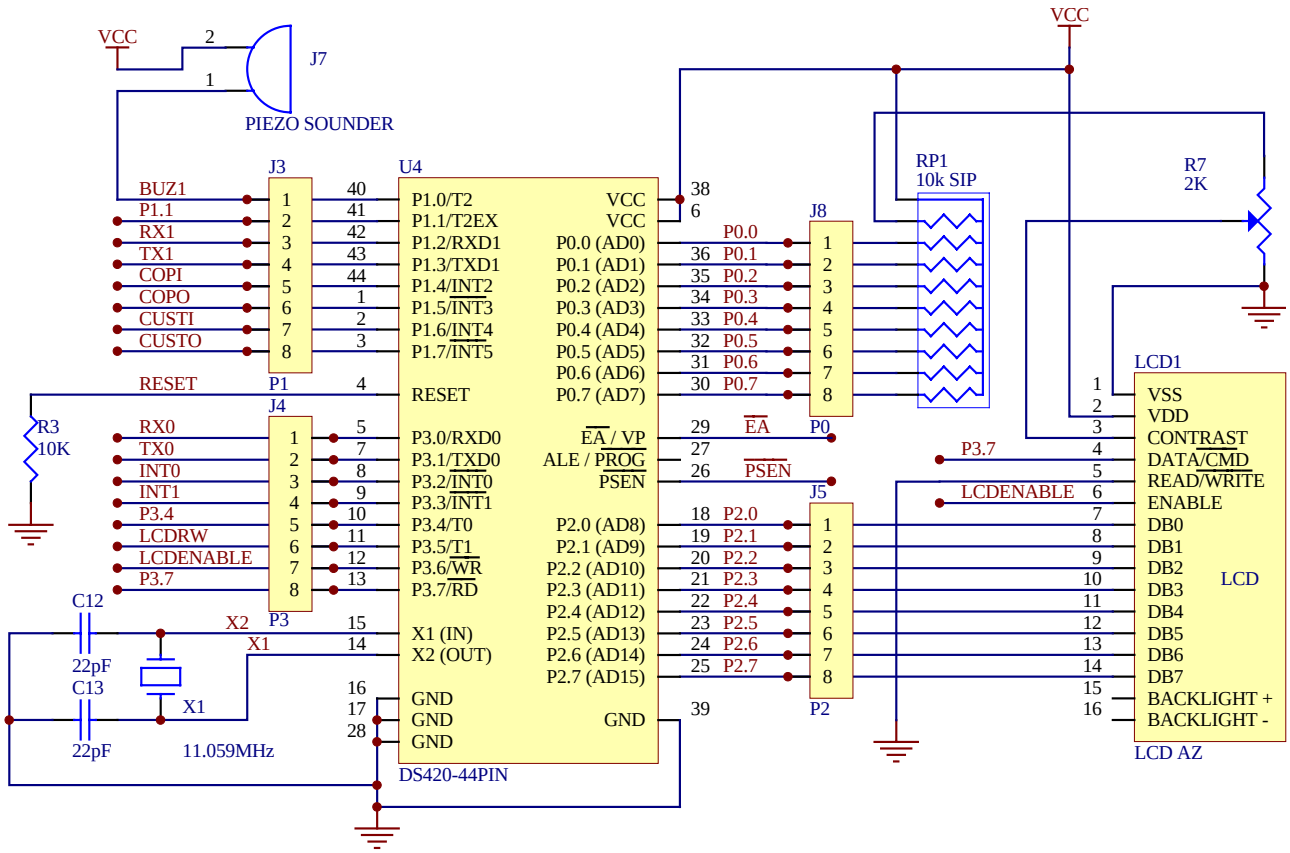


图13. 协处理器和 1-Wire 客户端电路

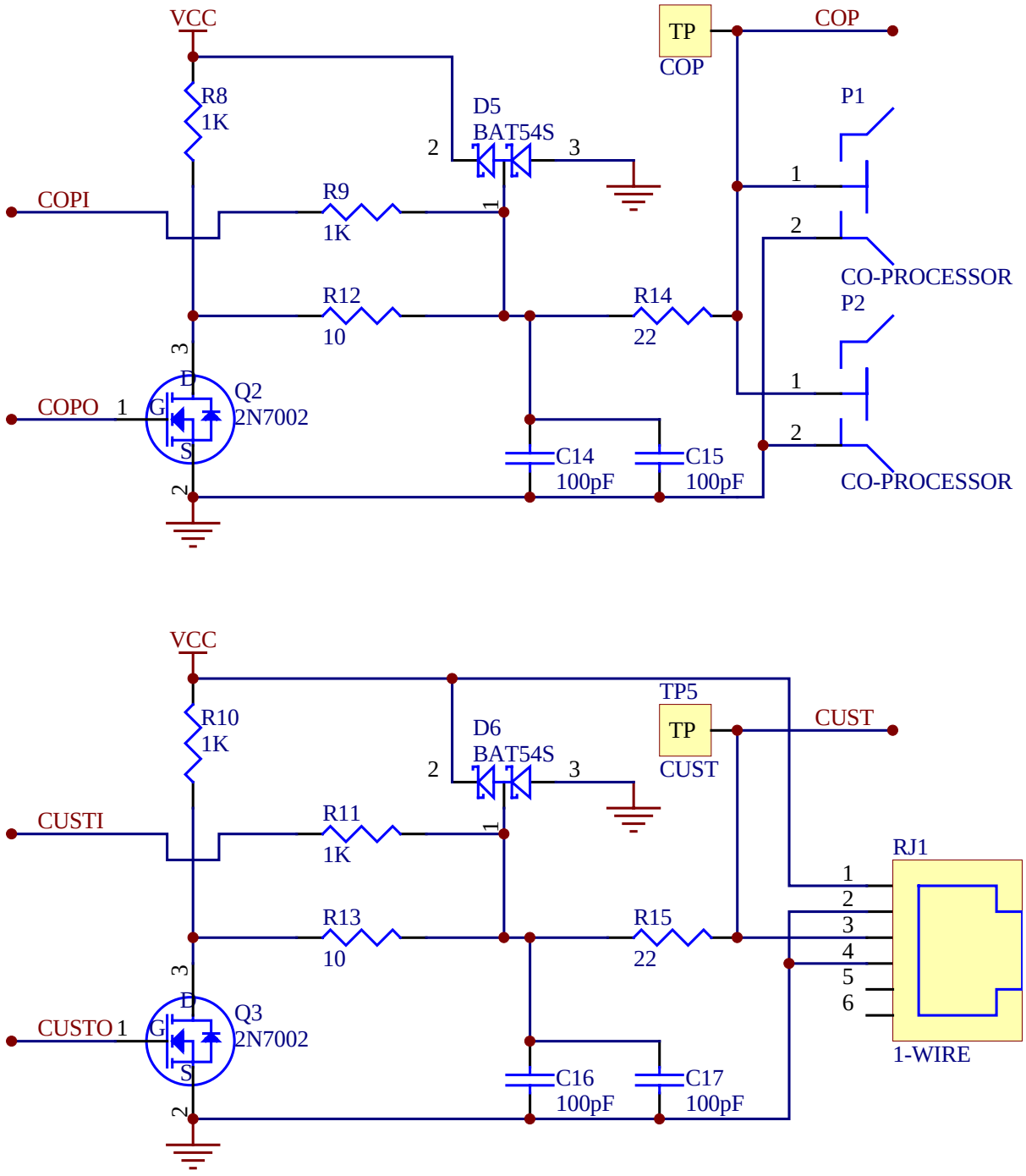


图14. 电源

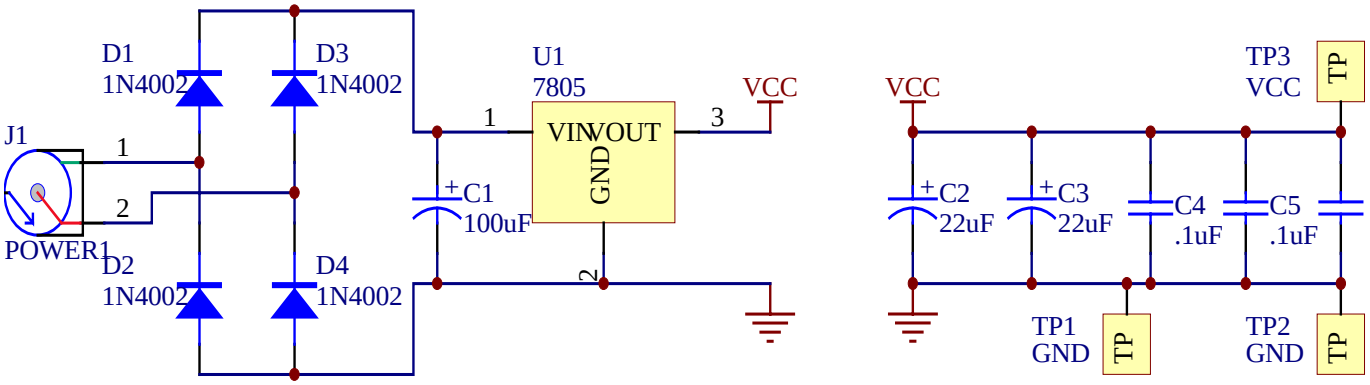
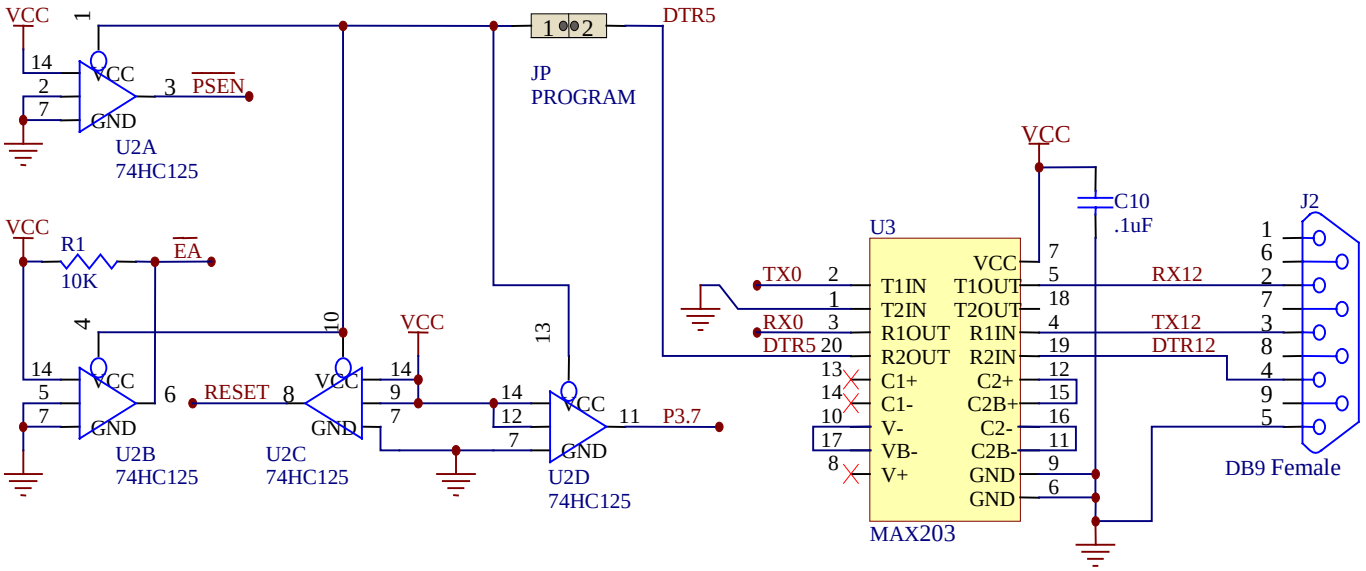


图15. RS232 串口

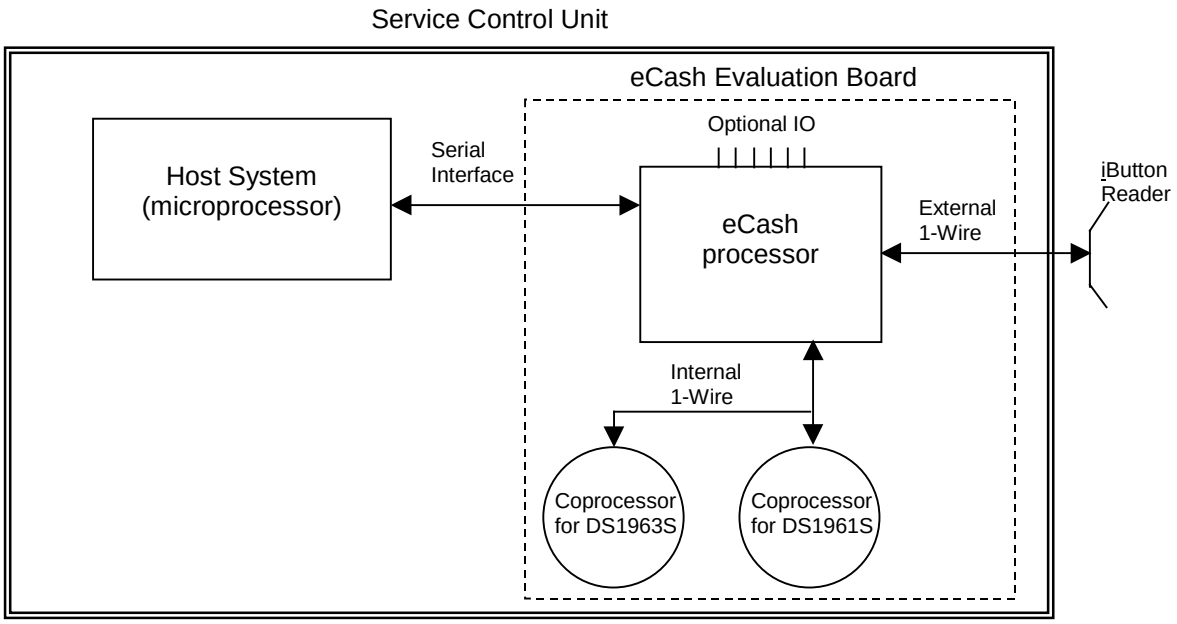


附录 A：eCash 处理器

eCash 处理器的目的之一是将较难的 1-Wire SHA 操作转移到专用微处理器。eCash 评估板上的 eCash 处理器利用内部 1-Wire 网络的 DS1963S 进行 SHA-1 认证，标记服务数据。这不但具有速度优势，而且还可以安全地保证不锈钢 iButton 封装内的加密信息。

另外，‘C’程序固件代码还可以导入到多种不同处理器中。eCash 处理器有三种基本工作模式：自治、标准和手动。自治模式下，eCash 处理器和主处理器没有任何联系。然而，当有事件发生时，从串口送出状态信息。标准模式下，eCash 处理器可以进行所有的 1-Wire 认证及支付工作，但由主机批准关键的过程。手动模式支持主机控制 eCash 处理器进行每一步操作。eCash 处理器在自治或标准模式下，也可以采用手动模式命令。

图16. eCash 处理器应用实例



速度考虑：自治模式是最快的，标准模式其次，手动模式最慢，因为每次 1-Wire 操作之前存在串行通信开销限制。

表6. 模式标志

Sequence (and bit #)	Operation Description
0	Automatic 1-Wire polling for user token
1	Automatic read and authentication
2	Automatic debit
3	Automatic Pulse of I/O bit
4	Automatic update of the LCD
5	Enable Overdrive operation
6	not used
7	not used

手动设置命令可以使能或禁止自治操作。
上载命令格式有两种不同的类型：‘get’或‘set’。Get 格式提供一个字符指示标志，Set 参数提供一个字符指示标志，并且，前面有字符长度数据域。

表7. 上载格式

Format	Description
GX	Get command where X is a one character designator
SX<D>	Set command where X is a one-character designator and <D> represents the data payload that the set command requires. If the length of the set command is inconsistent with the format then it will be disregarded.

例子：GF
获得 F 参数数据

例子：SQ3ABC
以 ABC 3 字符数据域来设置 Q 参数。

有两种类型的下载信息。第一类是 get 命令的结果，提供一个字节的指示标志和数据长度，然后是数据。第二类信息是异步事件。事件也有类型指示标志、长度和数据。

表8. 下载格式

Format	Description
RXhh<D>	Response of get command designator X with data following of hex length hh
EXhh<D>	Event type X occurred with data following of hex length hh

例子：EQ04ABCD
发生了 Q 类事件，提供‘ABCD’4 字符数据。

例子：RQ01Z
发生了 Q 类响应，提供‘Z’1 字符数据。

表 9 列出了所有‘get’和‘set’命令。

表9. Get 命令

Command + Format	Description
GD	Get time of last debit
GL	Get the last message sent (response or event).
GP	Read pages(specified by SP) of Coprocessor specified with SN and return
GS	Get status (dump of Memory State Table 6)
GU	Read pages(specified by SU) of user token
GV	Get firmware version
GW	Get ROM of coprocessor, if more then one coprocessor, use SN command to select

表10. Set 命令

Command + Format	Description
SAzy	Enables (y=1) or disables (y=0) mode flag (z=0 for AutoPolling, 1 for AutoReading, 2 for AutoDebiting, 3 for Pulsing IO bit, 4 for Update LCD, 5 for Use Overdrive Speed)
SBz	Abort the Lock-Step event (z=0 for Arrival, z=1 for read, z=2 for Debit)
SCy	Enable/Disable (y 1 enable, 0 disable) CRC16 of all packets sent from the eCash processor to the host. The inverted CRC16 is calculated over the entire packet and appended as a 4 character hex value.
SFaaaa	Set service filename aaa (ASCII file name, extension always 102 dec)
SGhhaaa…	Set the LCD to the text message (aaa…) of length hh (hex, max 16). If length N is 0 then clear display.
SIppx	Set the port pin ‘pp’ to the value ‘x’.
SKz	Acknowledge the Lock-Step event X so the next autonomous operation can be done (0 – poll, 1 – read, 2 – debit)
SLxy	Enable/Disable (y=1 enable, y=0 disable) a Lock-Step state. (x=0 for Arrival, 1 for Read, 2 for Debit). Will reset current Lock-Step status
SMhhhh	Set debit amount (hhhh hex number in hundredth of a unit)
SNx	Set the coprocessor number to read pages from (x=0 for DS1963S coprocessor or x=1 for DS1961S coprocessor)
SPhh	Set the coprocessor page to read with the GP command (hh hex page number)
SR	Soft Reset of eCash processor, will get a reset event when complete
SShh	Play beep (Sound) with (hh hex number of beeps)
STxb	Toggle port x bit b, where x and b are 4-bit ascii-encoded hex nibbles.
SUhh	Set the user token page to read (hh page hex number)
SYhh	Set the debit timeout value in hh seconds

注意，下面的状态说明没有包括所有的状态信息。忽略了可直接读取的状态信息(例如，获得版本的 GV)。

表11. 状态说明

Designator	Length (hex)	Example Data (hex)	Description
A	02	01	Autonomous operation mode flags (1 ASCII encoded hex byte) (See Table 1)
C	01	1	CRC16 enable flag (1 enabled, 0 disabled)
D	02	64	Time of last debit in milliseconds
F	04	ABCD	ASCII Service filename
G	10	eCash Demo V0.8	Current LCD text message
L	02	0102	Lock-step acknowledge flags (see Table 7)
M	06	020000	Amount to debit composed of 3 ASCII-encoded hex bytes, representing amount to debit (LSB first)
N	01	0	Coprocessor number selected (0=DS1963S or 1=DS1961S)
P	02	01	Page number to read from the current coprocessor
T	02	32	Port and bit number for the I/O pulse (1 ASCII encoded hex byte)
U	02	08	Page number to read from user Token
W	10	1800000000001122	Coprocessor ROM ID
Y	02	10	Debit timeout in seconds
Z	02	01	Status flags (see Table 8)

表12. 确认标志

Flag (bit position)	Description
0	Ack_PollEnabled
1	Ack_PollWaiting
2	Ack_ReadEnabled
3	Ack_ReadWaiting
4	Ack_DebitEnabled
5	Ack_DebitWaiting
6	Don't Care
7	Don't Care

表13. 状态标志

Flag (bit position)	Description
0	Stat_Poll
1	Stat_Read
2	Stat_DebitCert
3	Stat_UpdateToken
4	Stat_Verify
5	Stat_WaitUntilGone
6	Don't Care
7	Don't Care

表14. 事件

Code	Operation Description	Length + Data Payload Format
R	Soft reset complete	00
A	1-Wire arrival reporting, data is ROM	10RRRRRRRRRRRRRR
L	1-Wire departure reporting, data is ROM	10RRRRRRRRRRRRRR
U	Automatic read of select pages from user	40AA55AA55AA55AA55AA55AA55AA55AA55AA55AA55AA55AA55AA55AA55AA55AA55
S	Authenticated raw service data (8 bytes)	10CTCMCMMBMBMBIDID
M	Authenticated monetary balance service data	06MBMBMB
D	Debited final balance	06MBMBMB
I	IO bit pulse after completion of D. (If D is not set then pulse on completion of S or M).	00
C	Status displayed on LCD, length variable	0155
E	Error (see Table 10)	010A

表15. 故障代码

Code (hex)	Description
01	No valid token found during poll
02	Tear occurred, the device contents have not changed
03	Tear occurred, the device contents are in an unknown state
04	Tear occurred, but a fix has been applied. Retry verification.
05	Failed to erase coprocessor scratchpad.
06	Failed to find account file
07	Failed to get challenge from coprocessor
08	During Read: Failed to issue challenge to token
09	During Verify: Failed to issue challenge to token
0A	Failed to read token's account data, or data is bad
0B	Failed to compute the UTS
0C	Device failed authentication
0D	Money file signature failed validation
0E	Failed to update the device
0F	Insufficient funds for debit.
10	Failed to erase scratchpad.

响应实例：

GU:

RU200FAA008039070000444C534D660A0100BEED520001040094CE0000000000E3F

GP:

RP200FAA008063750000434F5052180104004AE1520001040094CEAAAAAAAAAAAAAA

GS: (CR's and spaces added for clarity)

RS63
A02 37
C01 0
D02 00
F04 DLSM
G0F iButton eCash
L02 00
M06 01000
N01 0
P02 00
T02 00
U02 00
W10 18F6AA0200000043
Y02 10
Z02 01

GD:

RD0268