

FEATURES

- Demonstrates the capabilities of the DS2705 SHA-1 Authentication Master, including:
 - Initiating a Secure Challenge and Response Authentication using the SHA-1 Algorithm with a DS2703/DS2704
 - Dallas 1-Wire Master/Slave Interface at Standard and Overdrive speeds
 - Input and Output pins for Initiating Challenge and Reporting Authentication Pass/Fail
 - Programmable Configuration
- Interfaces to the USB Port of a PC running Windows OS that supports USB operation

INDEX

Evaluation Kit Contents
Equipment Needed
Introduction
Setup and Installation
 Board Connections
 Software Installation
Menus
DS2705 Interface
 Configuration Register
DS2704 Interface
DS2703 Interface

INTRODUCTION

The DS2705K Evaluation Kit makes performance evaluation, software development, and prototyping with the DS2705 SHA-1 Authentication Master easy. The evaluation board interfaces to a PC through a DS9123O USB Adapter and RJ-11 cable connection as well as to a DS2703K or DS2704K evaluation board. The provided CD ROM contains all related data sheets along with the evaluation software, which can be run under any Windows operating system that supports USB operation.

The DS2705K evaluation software allows the user to completely program and configure the DS2705. It also provides limited programmability of a DS2703 or DS2704.

The evaluation board circuit is designed to provide the DS2705 with a stable environment to perform a SHA-1 Authentication with a DS2703 or DS2704 and display a Pass/Fail on the result. Kit demonstration boards will vary as they are improved upon over time. For information on the demonstration board circuits refer to the documentation directory on the DS2705K CD ROM.

SETUP AND INSTALLATION

BOARD CONNECTIONS

Connections to the demonstration boards are best made either by soldering directly to the pads or by using cables with mini-grabber clips. The DS2705K has 2 RJ-11 Jacks labeled “← MASTER” and “SLAVE →” since the DS2705 can function as both a Master and a Slave.

EVALUATION KIT CONTENTS

- 1 pc. TSSOP Evaluation Board
- 1 pc. DS9123O USB Adapter
- 1 pc. RJ-11 Phone Cable
- 1 pc. DS2705K CD containing:
 - DS2705K Evaluation Software
 - DS2705 Related Data Sheets

REQUIRED EQUIPMENT

1. A PC running Windows 2000 or newer with a CD ROM drive and an available USB port.
2. A battery or power supply.
3. Cables with mini-grabber style clips or the ability to solder directly to connection pads.
4. A DS2703/DS2704 is required for Authentication.

Communication to the DS2705 with the DS2705K software can be accomplished through the RJ-11 jack labeled as "SLAVE →". Simply connect the provided standard six conductor RJ-11 cord from the "SLAVE →" jack to the DS9123O USB Adapter. Then attach the VDD/VSS terminals to a battery or power supply and the DS2705K software can communicate with the DS2705 for programming and configuring the device.

The DS2705 can operate as a Master by connecting the RJ-11 jack labeled as "←MASTER" to the RJ-11 jack of a DS2703K/DS2704K evaluation board with a RJ-11 cord. A DS2704K will require a battery or power supply. A DS2703K can be connected without any additional connections.

A 15V programming voltage is required on the High Voltage (HV) terminal in order to store the Challenge, Response and Configuration to EEPROM.

The Challenge (CH) terminal is used to initiate a SHA-1 Authentication.

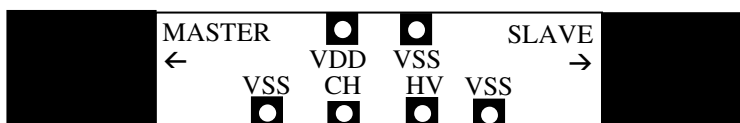


Figure 1: DS2705K Evaluation Board (PD102405) Connections

SOFTWARE INSTALLATION

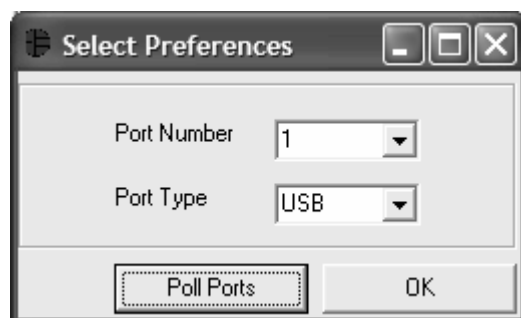
To install the DS2705K software, exit all programs currently running and insert the DS2705K software CD into your computer's CD ROM. The user can run SETUP.EXE from the setup directory and the installation process begins. Follow the prompts to complete the installation. The DS2705K software can be uninstalled in the Add/Remove Programs tool in the Control Panel. After the installation is complete, open the DS2705K folder and run DS2705K.EXE or select DS2705K from the program menu. A splash screen containing information about the evaluation kit appears as the program is being loaded.

The Documentation directory also located on the CD contains all relevant data sheets and application notes on the DS2705 and DS2705K. They are stored in Adobe Acrobat format for easy viewing.

SELECTING THE COM PORT

If the DS9123O is connected when the DS2705K is started, the software will start up automatically. If it is not connected, the Select Preferences window will open. This software will also operate with the DS9123 Serial Port Adapter.

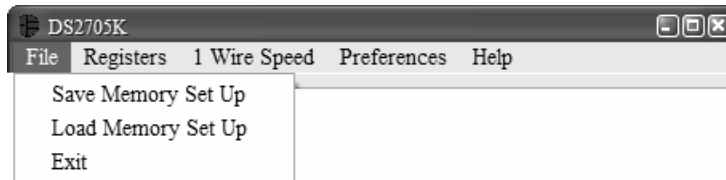
In this window, select either serial port or USB communication and the port number; then hit OK. The DS2705K software saves this port selection and automatically uses the selection each time the program starts. To change the port later, click the Preferences option on the menu bar, select Edit Preferences, and then select the appropriate port. To attempt to automatically locate the DS9123O or DS9123, click the Poll Ports button. Warning - automatically polling for the DS9123 can disrupt other devices connected to your computer's COM ports.



MENUS

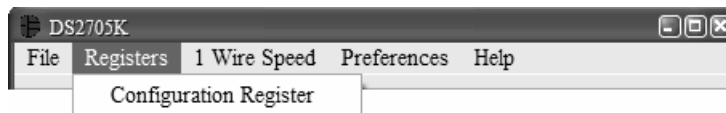
Several pull down menu options have been provided to simplify use of the DS2705K software for the user. Their functions are individually detailed below.

FILE MENU



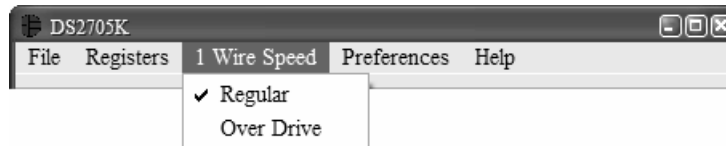
The File Menu allows the user to save the contents of the 30 bytes of EEPROM to a file so that other DS2705's can easily be programmed with the same data. The software copy of the Secret is also saved to the file. To save the values to a file, select Save Memory Set Up and enter a filename and select the location to store the file. This will store the contents of all of the text boxes to the selected file. To load the values from a file into the text boxes, select Load Memory Set Up and select the desired file.

REGISTER MENU



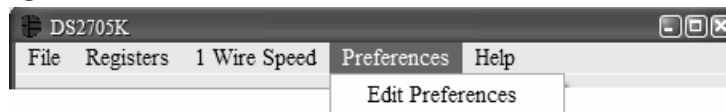
The Registers details of the Configuration Register can be viewed by using the Registers Menu or by clicking on the "View Configuration Register" button.

1 WIRE SPEED MENU



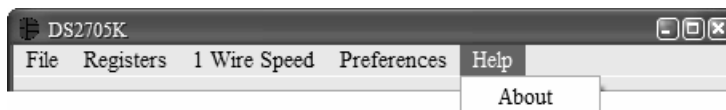
The 1 Wire Speed Menu allows the user to set the 1 Wire speed that the software uses. The DS2705 is capable of communicating at Regular and Over Drive speeds, so it is possible that the software will be communicating in one speed and the DS2705 will be in the other speed. This menu allows the user to specify which speed the software will use, but it will not make any changes to the device. The software will attempt to identify the correct speed of the device at startup, but in the event that the software and the device get out of sync, this Menu will allow the user to correct the problem. A check mark will be next to the speed that is currently in use by the software.

PREFERENCES MENU



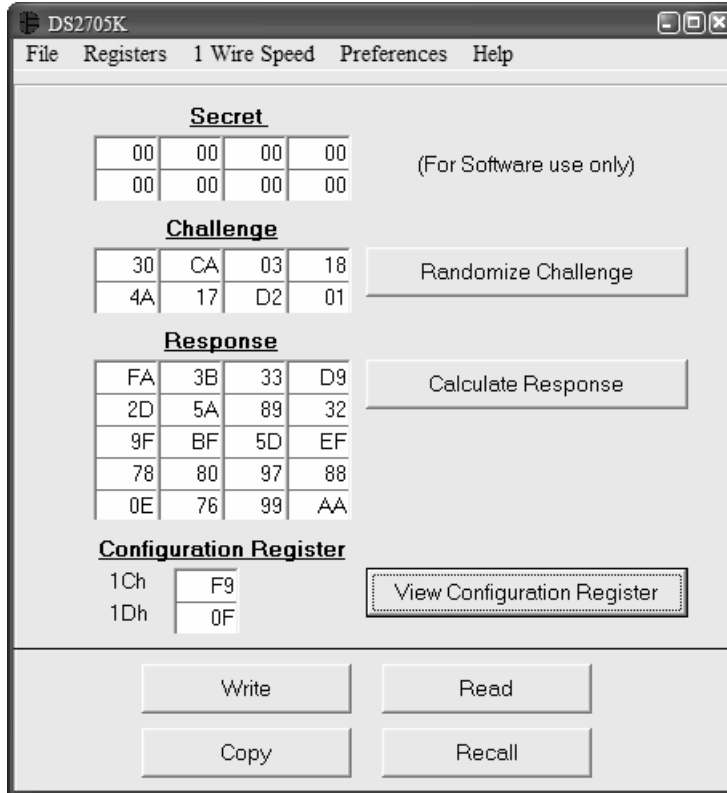
The Preferences Menu allows the user to change port settings at any time. Edit Preferences opens the Select Preferences window. See Selecting the COM Port above.

HELP MENU



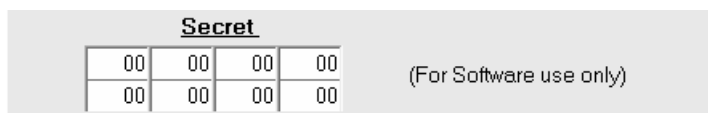
Selecting the About topic from the Help Menu will open a window containing information about this program and Dallas Semiconductor.

MAIN Interface



The DS2705 stores an 8 byte Challenge, a 20 byte Response, and a 2 byte Configuration Register in EEPROM. The Secret is only used by software to create the proper Response for any given Challenge and is never transmitted across the 1-Wire bus. The “Read” and “Write” buttons allow access to the Shadow RAM. The “Copy” and “Recall” buttons issue the commands to transfer the data between the Shadow RAM and EEPROM.

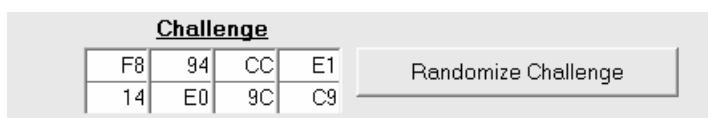
The Secret



The user is able to enter the 8 bytes of the Secret into the text boxes. The top-right text box is the LSB of the Secret, and the bottom-left text box is the MSB of the Secret. (All text boxes are displayed in this same format.)

The Secret is not stored in the DS2705; it is only used by the DS2705K software to calculate the appropriate Response for a given Challenge. It is important that the Secret entered here is the same secret that is stored in the DS2703/DS2704 that is being authenticated.

The Challenge



The Challenge is a random 8 byte block, stored in EEPROM of the DS2705, which is used by the Dallas SHA devices to perform the SHA-1 encryption algorithm. Each time an authentication attempt is made, the DS2705 sends the 8 byte Challenge.

The user can left-click on the Randomize Challenge button to load a random challenge into the Challenge text boxes. Left-clicking this button does not write the Challenge to the device. It is still required that the user left-click on the Write and Copy buttons, described in the Memory Access section below, to write the Challenge to the device.

The Response

Response			
1F	FE	98	05
42	3D	54	E9
2F	39	B4	27
A4	20	E6	52
FE	8E	39	B1

Calculate Response

The Response is the 20 byte message digest that is the result of the SHA-1 encryption algorithm. The Result is stored in EEPROM of the DS2705. Each time an authentication attempt is made, the DS2705 sends the 8 byte Challenge and then reads back the 20 byte Response. If the Response that is read back matches the Response that is stored in EEPROM, the slave passes the authentication attempt.

The user can left-click on the Calculate Response button to calculate the Response that is to be expected based on the Secret and Challenge text boxes. Left-clicking this button does not write the Response to the device. It is still required that the user left-click on the Write and Copy buttons, described in the Memory Access section below, to write the Response to the device.

The Configuration Register

Configuration Register	
1Ch	F9
1Dh	0F

View Configuration Register

Configuration Register			
Bits 1:0	RTA1:0	Re-Tries Per Authentication Attempt is :	0 Re-tries
Bits 3:2	PAA1:0	Periodic Authentication Attempt is :	Attempt every 8s
Bits 5:4	PPT1:0	The Periodic Presence Test is :	Attempt every 1.0s
Bit 6	APA	Asynchronous Presence Authentication :	Yes
Bit 7	CHP	The Challenge Polarity bit is :	Active High
Bit 8	FOM	The Fail Output Mode is :	Flash
Bit 9	OWS	The 1-Wire Speed is :	Overdrive
Bits 11:10	LOCK1:0	The Lock Bits are :	11b
Bit 13	FAILF	The Fail Flag is :	Clear
Bit 14	PASSF	The Pass Flag is :	Clear
Bit 15	LOCKF	The Lock Flag is :	Clear

Write Read Done

The present state of all of the Configuration Register bits are displayed immediately upon opening the register window by left-clicking on the View Configuration Register button. R/W locations contain a selection to allow the user to determine their state. Pressing the Write button will write the new value to the register and then read the register inside the DS2705 to verify the correct value was written. The Copy button, as described below in the Memory Access section, must still be left-clicked from the main window in order to store the new contents into EEPROM.

Memory Access



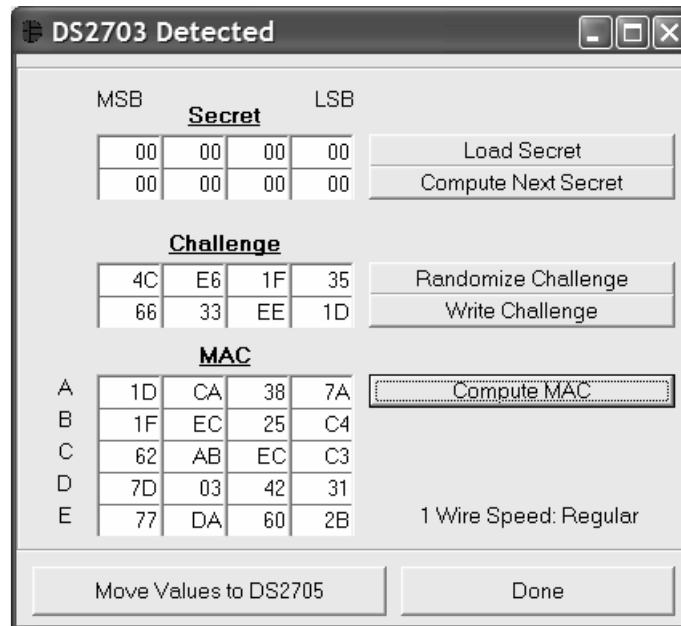
The 8 byte Challenge, the 20 byte Response and the 2 byte Configuration Register are all stored in EEPROM of the DS2705. Left-clicking on the Read or Write buttons transfers the values in the text boxes of the Challenge, Response and Configuration Register to and from the SRAM of the device. Left-clicking on the Copy and Recall buttons transfers the values between the SRAM and EEPROM of the device.

Authentication

Once the DS2705 has been configured appropriately, a DS2703 or DS2704 can be authenticated by connecting the RJ-11 jack labeled as “←MASTER” to the RJ-11 jack of a DS2703K/DS2704K evaluation board with a RJ-11 cord. A DS2704K will require a battery or power supply. A DS2703K can be connected without any additional connections.

An authentication attempt can be initiated in several methods depending on how the DS2705 is configured. When it is initiated, the DS2705 will send out the Challenge and if the Response from the slave device is what is expected, the DS2705K software will display PASS and the DS2705K evaluation board will turn on a green LED. If the authentication fails, FAIL will be displayed by the software and a red LED will be turned on.

DS2703 Interface



Connecting a DS2703K board to the DS912130 with the RJ-11 phone cable, will cause the DS2703 Detected Window to appear. This window allows the user to access some of the functionality of the DS2703.

The user can load a new Secret into the DS2703 by left-clicking on the Load Secret button. This will load the values in the Secret text boxes into the DS2703. The user can also send the Compute Next Secret command by left-clicking on the Compute Next Secret button. It is necessary to write the challenge prior to left-clicking the Compute Next Secret button. A 15 volt programming pulse is required to change the Secret of the DS2703.

Left-clicking on the Write Challenge button writes the 8 bytes of the Challenge text boxes to the DS2703. A random challenge can be generated into the Challenge text boxes by left-clicking the Randomize Challenge button. Left-clicking the Randomize Challenge button only changes the text boxes; it is still required to left-click the Write Challenge button to write the values to the DS2703.

Left-clicking the Compute MAC button will send the command to compute the 20 byte MAC (or Result) and read it back. The caption below the Compute MAC button indicates if the DS2703 is configured to communicate in Regular or Over Drive 1-Wire Speed.

The values in the Secret, Challenge and MAC text boxes can be transferred to the text boxes on the main DS2705K window by left-clicking the Move Values to DS2705 button. This will not write the values to the DS2705. It simply loads the text boxes with the values.

DS2704 Interface

The screenshot shows a window titled "DS2704 Detected" with standard window controls (minimize, maximize, close). The window is divided into three main sections: Secret, Challenge, and MAC. Each section has a grid of input boxes and associated buttons.

Secret Section: Labeled "MSB" on the left and "LSB" on the right. It contains a 2x4 grid of boxes, each containing "00". To the right of the grid are two buttons: "Clear Secret" and "Compute Next Secret".

Challenge Section: Contains a 2x4 grid of boxes. The top row contains "A7", "EA", "2A", "2B". The bottom row contains "20", "D9", "9B", "2E". To the right of the grid are two buttons: "Randomize Challenge" and "Write Challenge".

MAC Section: Labeled "MAC" in the center. It contains a 5x4 grid of boxes. The rows are labeled A through E on the left. The boxes contain: Row A: "46", "9C", "B7", "97"; Row B: "51", "CD", "15", "AF"; Row C: "3F", "25", "24", "37"; Row D: "81", "C8", "7F", "F0"; Row E: "4F", "F6", "A5", "4F". To the right of the grid is a button labeled "Compute MAC". Below the button, the text "1 Wire Speed: Regular" is displayed.

At the bottom of the window are two buttons: "Move Values to DS2705" and "Done".

Connecting a powered DS2704K board to the DS91213O with the RJ-11 phone cable, will cause the DS2704 Detected Window to appear. This window allows the user to access some of the functionality of the DS2704.

The user can clear the Secret into the DS2704 by left-clicking on the Clear Secret button. This will load 00h into the Secret text boxes, as well as in the DS2704. The user can also send the Compute Next Secret command by left-clicking on the Compute Next Secret button. It is necessary to write the challenge prior to left-clicking the Compute Next Secret button.

Left-clicking on the Write Challenge button writes the 8 bytes of the Challenge text boxes to the DS2704. A random challenge can be generated into the Challenge text boxes by left-clicking the Randomize Challenge button. Left-clicking the Randomize Challenge button only changes the text boxes; it is still required to left-click the Write Challenge button to write the values to the DS2704.

Left-clicking the Compute MAC button will send the command to compute the 20 byte MAC (or Result) and read it back. The caption below the Compute MAC button indicates if the DS2704 is configured to communicate in Regular or Over Drive 1-Wire Speed.

The values in the Secret, Challenge and MAC text boxes can be transferred to the text boxes on the main DS2705K window by left-clicking the Move Values to DS2705 button. This will not write the values to the DS2705. It simply loads the text boxes with the values.

