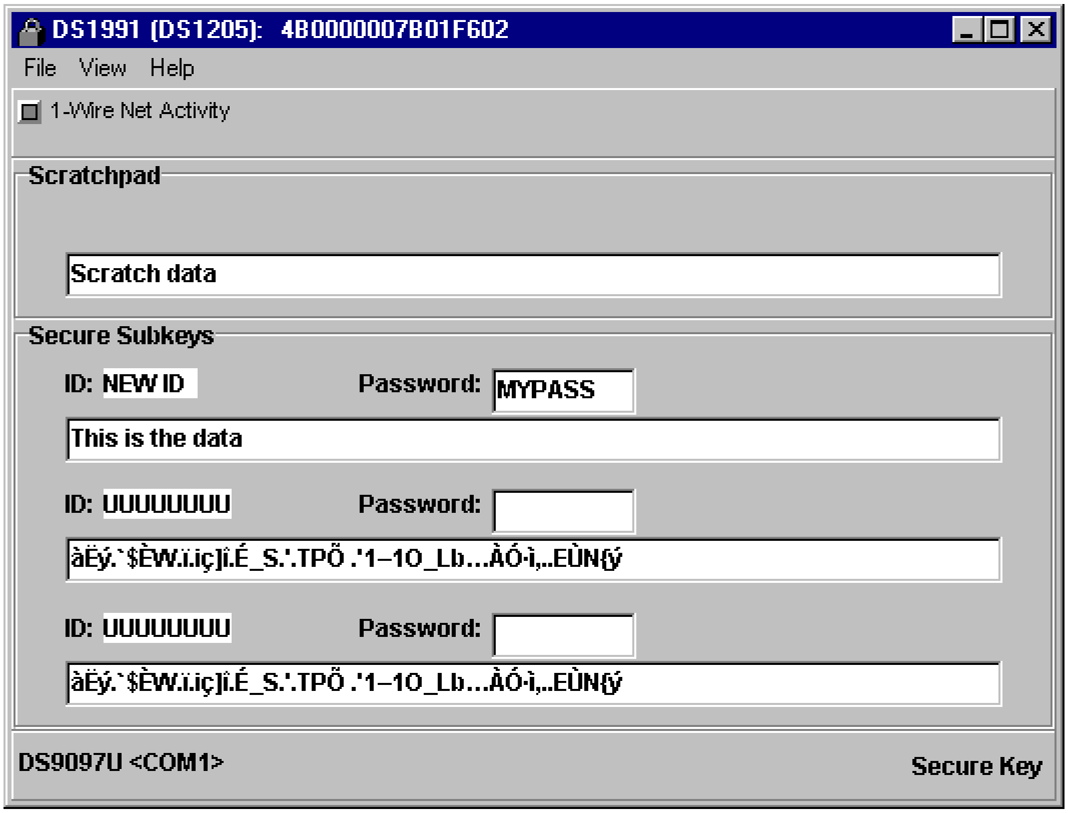
Secure Viewer

The Secure Viewer is used to read and write the DS1991 MultiKey iButton. In contrast to Memory iButtons, this device uses a file system that is implemented in hardware. The device is designed to store three files of 48 bytes each that are called Subkeys. Instead of 4 bytes with a numeric extension, the file name consists of 8 bytes and is called ID Field. In addition to the ID Field, each file has an 8-byte write-only password to protect its contents from unauthorized read access.

As with the other Memory iButtons, this device also includes a scratchpad. The scratchpad may be used to write data and read it back for verification before it is copied to its final destination in one of the Subkeys. With its 64 bytes, the scratchpad of the DS1991 can hold the ID Field, Password and all 48 data bytes of a Subkey. The usage of the scratchpad for intermediate storage is highly recommended for an environment where dwell time of the device at the 1-Wire network is short. Assuming that the dwell time is long enough, the iButton Viewer does not use the scratchpad and writes directly to the Subkey. As a consequence, the scratchpad becomes available as an additional publicly accessible memory space.

All of the memory areas of the DS1991 MultiKey iButton with the ID fields and password-entry boxes of the three Subkeys are laid-out in the window of the Secure Viewer in a straight-forward way, as shown below.

The three Subkeys combined into a block “Secure Subkeys” fill the lower three quarters of the window. To the left, above each Subkey’s data field there is a box labeled “ID” to display the contents of the key’s ID Field. Above the center of each Subkey’s data field is another box labeled “Password”. When reading a Subkey, one has to type the password into this box to give the program access to the secure data. Above the block of Subkeys there is a smaller block called “Scratchpad”. The scratchpad is represented as one line that displays the contents of the scratchpad in character form. As usual, the window is completed by a Status Bar that indicates the communication port in use and a short Menu Bar with the entries File (to exit the Secure Viewer) and View (to refresh the screen, in case a single device is viewed through multiple windows). This sample picture was generated using a device in the state as it is shipped from the factory. The “U”s are the ASCII representation of the character code 55 hex (= 85 decimal), a pattern that typically is written to the device before it leaves the factory.



Scratchpad

Scratch data

Secure Subkeys

ID: NEW ID Password: MYPASS

This is the data

ID: UUUUUUUU Password:

àËý.`$ÈW.ï.iç]î.É_S.'.TPŐ .'1–1O_Lb…ÀÓ·ì,..EÙN{ý

ID: UUUUUUUU Password:

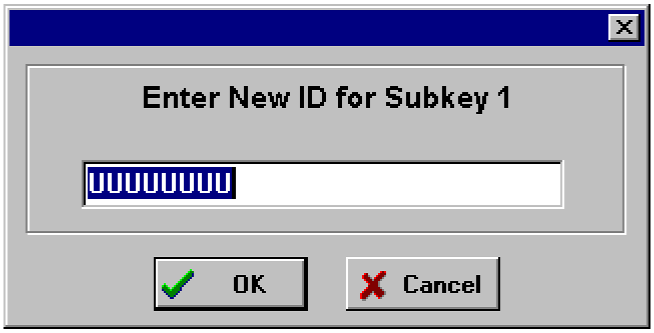
àËý.`$ÈW.ï.iç]î.É_S.'.TPŐ .'1–1O_Lb…ÀÓ·ì,..EÙN{ý

DS9097U <COM1> Secure Key

The Secure Viewer does not know or remember passwords. To meet the requirements of the communication protocol the viewer uses 8 spaces (code 20 hex or 32 decimal) as password when trying to read the Subkeys. Since this is usually different from the correct password, the device responds with “garbage” data, a pseudo-random pattern based on the provided password (not the stored one). The “garbage” is then checked for its printability. All non-printable codes, i. e., codes below 20 hex (32 decimal), are replaced by a “.” before data is displayed in character form as Subkey contents. Depending on national settings, the characters actually seen may be different from those shown in the sample window.

Writing Secure Data

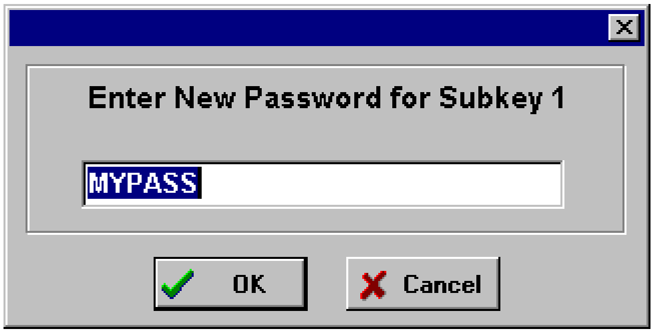
Before one can write secure data to a Subkey for the first time, one has to give the Subkey a name (optional) and specify a password (mandatory). To change the name of a Subkey, click on the box that displays the current contents of the key’s ID Field. This will open a child-window with the current name already selected for replacement, as shown below.



Enter New ID for Subkey 1

UUUUUUUU

Enter the new name and click OK. This will bring up a similar window for setting the password.



Enter New Password for Subkey 1

MYPASS

The default password of the Secure Viewer is 8 spaces. All but the first space are removed from the editing area of this child-window. The remaining single space is selected for replacement. Simply fill in the new password and click on OK. Clicking on “Cancel” will ignore the new name as well as the password. For both, the ID Field and the password, the program allows up to 8 characters, including embedded spaces, to be entered. Shorter names are padded with spaces to make the 8 characters necessary to meet the hardware requirements of the device.

After file name and password have been entered, the new names will be visible for the Subkey selected. Since writing a password erases the contents of the Subkey, the Subkey’s data field will now be filled with 48 dots, representing the non-printable code 00 hex. Now double-click on the dots to select them for replacement and type the new contents of the Subkey. With the first character entered, a “Write” button will appear above the right end of the Subkey’s data field. When finished typing, click on this temporary button to transfer the text to the secure Subkey. The text entered will be appended by spaces to fill the 48 bytes of the secure storage space of the key. To cancel the transfer without writing, exit the window of the Secure Viewer or click on “Refresh” in the view menu. After the data is written to the device, the “Write” button will disappear, but the file name, password and contents will remain visible. To make the password and the true contents of the Subkey invisible, overtype the password.

Reading Secure Data

To read secure data, click on the password-entry box of the key to be read and type the password. When the typing ends, the program assumes that the password is complete and will access the device. If the password is correct, the secure data will be displayed in its true length, with trailing spaces removed. Otherwise the display will show random data, based on the password entered. Note that the password is case-sensitive and must be entered exactly as it is stored in the device. Although the program fills short passwords with trailing spaces to make up the 8 bytes required by the DS1991, these trailing spaces need not be entered.

Modifying Secure Data

After secure data is read from one of the Subkeys of the DS1991 it can easily be modified and written back to the device. First access the Subkey as described in section “Reading Secure Data”. Now double-click on the word to be replaced and enter new text. To replace a selection, select the text to be replace with the mouse and type the new text. To replace the whole contents, select the full line. Alternatively, one can position the cursor anywhere in the data field and start erasing or typing, whatever is necessary. The program counts the characters and stops accepting more data as soon as the data field contains 48 characters. As described in section “Writing Secure Data”, a “Write” button will appear that needs to be clicked to finally write to the device.

Changing the ID Field And/Or Password

The Secure Viewer allows the user to change the ID Field of a Subkey and its password while keeping the Subkey’s contents. However, this is a multi-step procedure involving the Windows clipboard and keystroke commands. The procedure begins with displaying the contents of the subkey who’s ID or password is to be changed. See section “Reading Secure Data” for details. Next select all the contents of the Subkey’s data field with the mouse and copy it to the clipboard using the keystroke command Control + C.

Now click on the display area of the Subkey’s ID Field. This will pop up the child-window for entering the file name with the current name filled-in and selected. Make changes as desired or click on OK. This will transfer to the password child-window with the current valid password filled-in and selected. Make the desired changes and click on OK. This will write the new ID and password and erase the Subkey’s contents. Now double-click on the Subkey’s data field that is now filled with dots and paste in the contents of the clipboard using the keystroke command Control + V. Now click on the “Write” button to write the data to the device.

Trying to change the password by simply typing new text in the password field is not possible. The programs would assume that one is going to try another password for reading the Subkey’s contents. Changing the data field of the Subkey first and then the password before writing to the device will give the error message “Error writing the sub-key, password may be incorrect !”. This comes from the fact that the program tries to write to the device using the password shown on the screen. In the read-back cycle after writing the program will then see that the data does not match and therefore display the error message.

Reading/Writing The Scratchpad

With the Secure Viewer the scratchpad is treated as a Subkey without ID Field and password. The current contents therefore are displayed automatically. For editing and writing the scratchpad the same rules apply as for the data field of a secure Subkey. See section “Modifying Secure Data” for details. With the scratchpad, however, the program accepts up to 64 bytes.