

# Unexpected Interaction Between the HCS08 Backdoor Key Sequence and Stop Mode

## 1 Problem Description

If KEYACC is set to 1 in a secure device to start the backdoor unlock sequence, and the device enters stop mode before the unlock sequence is completed, then security will be disengaged when the MCU wakes up from stop using an interrupt. If reset is used to wake up from stop, KEYACC is cleared and the MCU will remain secure. If the backdoor access feature is not enabled (nonvolatile KEYEN bit = 0), this unexpected operation cannot arise.

There is no known reason a user would enter stop mode after a backdoor unlock sequence has started but has not been completed. This stop instruction must be executed from within the (secure) user code and is not an occurrence that can be forced by actions external to the MCU. RAM is considered a secure resource when security is enabled, so a potential pirate cannot introduce code to force the MCU into stop mode.

## 2 Workaround

Avoid the conditions that lead to the unexpected security-unlock condition. You could choose to not allow the backdoor access mechanism by clearing the nonvolatile KEYEN bit in NVFOPT. If you plan to use the backdoor access mechanism, and your application also uses stop mode, you could choose to use reset instead of an interrupt to wake the MCU from stop. If you plan to use the backdoor access mechanism, and your application also uses stop mode with the possibility of an interrupt wakeup, then do not allow entry into stop during a backdoor access operation. Backdoor access is a rare operation so there should be no need to enter stop mode during the unlocking sequence.

### 3 Mask Sets Affected

- MC9S08AW60 — 0L16X, 0M75B, 1M75B, 3M75B, 5M75B
- PC9S08GT16A — 2M70C
- MC9S08JR12 — 0L95Y
- PC9S08LC60 — 0M78B
- MC9S08QG8/4 — 0M77B, 1M77B, 2M77B, 3M77B
- MC9S08RT16 — 0M14A

#### How to Reach Us:

**Home Page:**  
www.freescale.com

**E-mail:**  
support@freescale.com

**USA/Europe or Locations Not Listed:**  
Freescale Semiconductor  
Technical Information Center, CH370  
1300 N. Alma School Road  
Chandler, Arizona 85224  
+1-800-521-6274 or +1-480-768-2130  
support@freescale.com

**Europe, Middle East, and Africa:**  
Freescale Halbleiter Deutschland GmbH  
Technical Information Center  
Schatzbogen 7  
81829 Muenchen, Germany  
+44 1296 380 456 (English)  
+46 8 52200080 (English)  
+49 89 92103 559 (German)  
+33 1 69 35 48 48 (French)  
support@freescale.com

**Japan:**  
Freescale Semiconductor Japan Ltd.  
Headquarters  
ARCO Tower 15F  
1-8-1, Shimo-Meguro, Meguro-ku,  
Tokyo 153-0064  
Japan  
0120 191014 or +81 3 5437 9125  
support.japan@freescale.com

**Asia/Pacific:**  
Freescale Semiconductor Hong Kong Ltd.  
Technical Information Center  
2 Dai King Street  
Tai Po Industrial Estate  
Tai Po, N.T., Hong Kong  
+800 2666 8080  
support.asia@freescale.com

**For Literature Requests Only:**  
Freescale Semiconductor Literature Distribution Center  
P.O. Box 5405  
Denver, Colorado 80217  
1-800-441-2447 or 303-675-2140  
Fax: 303-675-2150  
LDCForFreescaleSemiconductor@hibbertgroup.com

Document Number: EB667  
Rev. 0  
4/2006

Information in this document is provided solely to enable system and software implementers to use Freescale Semiconductor products. There are no express or implied copyright licenses granted hereunder to design or fabricate any integrated circuits or integrated circuits based on the information in this document.

Freescale Semiconductor reserves the right to make changes without further notice to any products herein. Freescale Semiconductor makes no warranty, representation or guarantee regarding the suitability of its products for any particular purpose, nor does Freescale Semiconductor assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. "Typical" parameters that may be provided in Freescale Semiconductor data sheets and/or specifications can and do vary in different applications and actual performance may vary over time. All operating parameters, including "Typicals", must be validated for each customer application by customer's technical experts. Freescale Semiconductor does not convey any license under its patent rights nor the rights of others. Freescale Semiconductor products are not designed, intended, or authorized for use as components in systems intended for surgical implant into the body, or other applications intended to support or sustain life, or for any other application in which the failure of the Freescale Semiconductor product could create a situation where personal injury or death may occur. Should Buyer purchase or use Freescale Semiconductor products for any such unintended or unauthorized application, Buyer shall indemnify and hold Freescale Semiconductor and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that Freescale Semiconductor was negligent regarding the design or manufacture of the part.

Freescale™ and the Freescale logo are trademarks of Freescale Semiconductor, Inc. All other product or service names are the property of their respective owners.

© Freescale Semiconductor, Inc. 2006. All rights reserved.

RoHS-compliant and/or Pb-free versions of Freescale products have the functionality and electrical characteristics as their non-RoHS-compliant and/or non-Pb-free counterparts. For further information, see <http://www.freescale.com> or contact your Freescale sales representative.

For information on Freescale's Environmental Products program, go to <http://www.freescale.com/epp>.