Tech Note #013

SREDKey Tamper Detection

Rev. A

Revised 1/16/2017

International Technologies & Systems Corporation
10721 Walker Street, Cypress, CA 90630-4720; Tel: (714) 761-6368; Fax (714) 761-8880
www.idtechproducts.com

Introduction

ID TECH's SREDKey encrypted keypad is a PCI SRED device, which means (among other things) it incorporates tamper detection features. This document gives background on how the tamper detection functionality works and how units can be evaluated in the field as to their tamper status.

Tamper Trigger State

Once a unit's tamper detection functionality has been triggered in service, the SREDKey's LCD will display the trigger cause until power-down. Also, the unit will erase all sensitive data, including cryptographic keys, and enter a deactivated state.

Once deactivation has occurred, each time the unit powers up, its LCD will display the trigger cause for 5 seconds. Then "`Activating`…" displays on the LCD, and no "`Ready`" message will appear until the unit is repaired and reactivated by the manufacturer.

The trigger cause will appear in abbreviated form as one of: HTF LTF HVF3 HBF LBF SDI1 SDI2 HVF1 or VGF. These abbreviations are explained in the table further below.

Note:

- When powering on for the first time after triggering tamper, the LCD will display "`Init MSR, please wait...` " for several seconds, then display the trigger cause for 5 seconds (until that message is erased on purpose); then "`Activating`…" displays on the LCD. Because a tamper event causes all keys and secure data to be lost, the MAXQ processor needs to re-authenticate with SecureHead, internally. This needs to occur at the factory.

- If the battery is off, all of the tamper settings will be lost. So for the first time power on, the MAXQ will work in user-load mode to set tamper detection, and the LCD backlight is on but displays nothing. Please re-apply power to the unit.

- There may be one or more reasons for the triggering of a tamper condition; all appropriate display codes will display on the LCD. If multiple messages displayed on the LCD, it means *several* tamper conditions were triggered. (See below.) Contact your ID TECH representative.

Tamper Trigger Troubleshooting

Various conditions can lead to the triggering of a tamper event. Those conditions (and the associated abbreviations: HTF, LTF, HVF3, etc.) are outlined in the table below.

Abbreviations
BOR – Battery-on reset (battery attach).
DRS – Destructive reset (that is, reset involving zeroization of secure data).

LCD Display	Tamper Trigger Cause
HTF	*High Temperature Flag*. When set, this bit indicates that the enabled (TMPENH = 1) temperature sensor has detected the chip temperature above +125 C and caused a DRS. The bit is typically interrogated to determine if a DRS was caused by the chip's high temperature when the on-chip temperature sensor is enabled. (Normally, this is enabled when the security lock bit is locked by the ROM Loader.) This flag must be cleared by software once set, otherwise this bit is unaffected by any other resets except BOR. Setting of this bit by software will not generate a DRS.
LTF	*Low Temperature Flag*. When set, this bit indicates that the enabled (TMPENL = 1) temperature sensor has detected the chip temperature below -60 C and caused a DRS. It is typically interrogated to determine if a DRS was caused by the chip's low temperature when the on-chip temperature sensor is enabled. (Normally, this is enabled when the security lock bit is locked by the ROM Loader.) This flag must be cleared by software once set, otherwise this bit is unaffected by any other resets except BOR. Setting of this bit by software will not generate a DRS.
HVF3	*High VDDIO Flag*. When set, this bit indicates that the enabled (HIVOLEN = 1) voltage monitor has detected the VDDIO has reached above +4V and caused a reset. The flag is typically interrogated to determine if a reset was caused by the chip's high voltage when the voltage monitor is enabled. (Normally it is enabled when the security lock bit is locked by the ROM Loader.) This flag must be cleared by software once set, otherwise this bit is unaffected by any other resets except BOR. Setting of this bit by software will not generate a reset.

HBF	*High Battery Voltage Flag*. When set, this bit indicates that the enabled (TMPENH = 1) high battery voltage monitor has detected the battery voltage has reached above +4 V and caused a DRS. The flag is typically interrogated to determine if a DRS was caused by the battery voltage being too high.(Normally it is enabled when the security lock bit is locked by the ROM Loader.) This flag must be cleared by software once set, otherwise this bit is unaffected by any other resets except BOR. Setting of this bit by software will not generate a DRS.
LBF	*Low Battery Voltage Flag*. When set, this bit indicates that the enabled (TMPENL = 1) low battery voltage monitor has detected the battery voltage has reached below 2.2 V and caused a DRS. This bit is typically interrogated to determine if a DRS was caused by the battery voltage being too low. (Normally it is enabled when the security lock bit is locked by the ROM Loader.) This flag must be cleared by software once set, otherwise this bit is unaffected by any other resets except BOR. Setting of this bit by software will not generate a DRS.
SDI1	*SDI1 Flag*. When set, this bit indicates that the external tamper detection circuitry has been triggered and caused a DRS by activating SDI1. The flag is typically interrogated to determine if a DRS was caused by the SDI1. The SDI1 input can be configured to be a normally open connection (internal pull down resistor is in effect) or normally closed connection (internal pull-up resistor is in effect), based upon the SECNT.SDI1C configuration bit. This flag must be cleared by software once set, otherwise this bit is unaffected by any other resets except BOR. Setting of this bit by software will not generate a DRS or reset
SDI2	*SDI2 Flag*. When set, this bit indicates that the external tamper detection circuitry has been triggered and caused a DRS by activating SDI2. The bit is typically interrogated to determine if a DRS was caused by the SDI2. The SDI2 input can be configured to be a normally open connection (internal pull down resistor is in effect) or normally closed connection (internal pull-up resistor is in effect) based upon the SECNT.SDI2C configuration bit. This flag must be cleared by software once set, otherwise this bit is unaffected by any other resets except BOR. Setting of this bit by software will not generate a DRS or reset.
HVF1	*High VDDC Flag*. When set, this bit indicates that the enabled (HIVOLEN = 1) voltage monitor has detected the

	VDDC voltage has reached above +2.5V and caused a reset. The flag is typically interrogated to determine if a reset was caused by the chip's high voltage when the voltage monitor is enabled. (Normally enabled when the security lock bit is locked by the ROM Loader.) This flag must be cleared by software once set, otherwise this bit is unaffected by any other resets except BOR. Setting of this bit by software will not generate a reset.
VGF	*Voltage Glitch Failure*. When set, this bit indicates that the enabled (GLIEN = 1) voltage glitch monitor has detected a 1.5V negative/positive glitch from VDDIO or VDDC that exceeded 20 ns in duration and caused a reset. It is typically interrogated to determine if a reset was caused by voltage glitch when the glitch monitor is enabled. This flag must be cleared by software once set, otherwise this bit is unaffected by any other resets except BOR. Setting of this bit by software will not generate a reset.

Tamper Indication

The following photo shows what the LCD looks like when multiple tamper indications are present: