ISL6

January 17, 2007 FN9

FlexiHash™ For Battery Authentication

The ISL6296 is a highly cost-effective fixed-secret hash engine based on Intersil's FlexiHash™ technology. The device authentication is achieved through a challenge-response scheme customized for low-cost applications, where cloning via eavesdropping without knowledge of the device's secret code is not economically viable. When used for its intended applications, the ISL6296 offers the same level of effectiveness as other significantly more expensive high maintenance monetary-grade hash algorithm and authentication schemes.

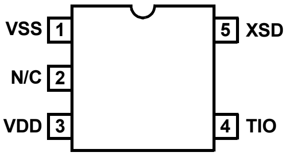
The ISL6296 has a wide operating voltage range, and is suitable for direct powering from a 1-cell Li-Ion/Li-Poly or a 3-cell series NiMH battery pack. The ISL6296 can also be powered by the XSD bus when the bus pull-up voltage is 3.3V or higher. The device connects directly to the cell terminals of a battery pack, and includes on-chip voltage regulation circuit, POR, and a non-crystal based oscillator for bus timing reference.

Communication with the host is achieved through a single-wire XSD interface - a light-weight subset of Intersil's ISD bus interface. The XSD bus is compatible for use with serial ports offered by all 8250 compatible UART's or a single GPIO (general purpose input and output) pin of a microprocessor.

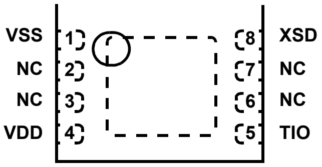
A clone prevention solution utilizing the ISL6296 offers safety and revenue protection at the lowest cost and power, and is suitable for protection against after-market replacement for a wide variety of low-cost applications.

Pinouts

ISL6296
(5 LD SOT-23)
TOP VIEW



ISL6296
(8 LD 2X3TDFN)
TOP VIEW



Features

- Challenge-response based authentication scheme using 32-Bit challenge code and 8-Bit authentication code.
- Fast and flexible authentication process. Multi-pass authentication can be used to achieve the highest security level if necessary.
- 16x8 OTP ROM stores up to three sets of 32-Bit host-selectable secrets with additional programmable memory for storage of up to 48 bits of ID code and/or pack information.
- FlexiHash engine uses two sets of 32-Bit secrets for authentication code generation.
- Non-unique mapping of the secret key to an 8-Bit authentication code maximizes hacking difficulty due to need for exhaustive key search (superior to SHA-1).
- Supports 1-cell Li-Ion/Li-Poly and 3-cell series NiMH battery packs (2.6V ~ 4.8V operation), or powered by the XSD bus.
- XSD single-wire host bus interface communicates with all 8250-compatible UART's or a single GPIO. Supports CRC on read data and transfer bit-rate up to 23kbps.
- True "Zero Power" Sleep mode - automatically entered after a bus inactivity time-out period
- 5 Ld SOT-23 and 8 Ld TDFN (2mm x 3mm) packages
- -20°C to +85°C operating temperature range
- Pb-free plus anneal available (RoHS compliant)

Applications

- Battery Pack Authentication
- Printer Cartridges
- Add-on Accessories
- Other Non-Monetary Authentication Applications

Related Literature

- Application Note AN1165 "ISL6296 Evaluation Kit"
- Application Note AN1166 "FlexiHash™ Engine Algorithm"
- Application Note AN1167 "Implementing XSD Host Using a GPIO"
- Technical Brief TB363 "Guidelines for Handling and Processing Moisture Sensitive Surface Mount Devices (SMDs)"

CAUTION: These devices are sensitive to electrostatic discharge; follow proper IC Handling Procedures.
1-888-INTERSIL or 1-888-468-3774 | Intersil (and design) is a registered trademark of Intersil Americas Inc.

FlexiHash is a trademark of Intersil Americas Inc. All other trademarks mentioned are the property of their respective owners.

Ordering Information

PART NUMBER (Note)	PART MARKING	TEMP. RANGE (°C)	PACKAGE (Pb-free)	PKG. DWG. #
ISL6296DHZ-T	296Z	-20 to +85	5 Ld SOT-23 Tape and Reel	P5.064
ISL6296DRZ-T	96Z	-20 to +85	8 Ld 2x3 TDFN Tape and Reel	L8.2X3A
ISL6296EVAL1	ISL6296 Evaluation Kit			

NOTE: Intersil Pb-free plus anneal products employ special Pb-free material sets; molding compounds/die attach materials and 100% matte tin plate termination finish, which are RoHS compliant and compatible with both SnPb and Pb-free soldering operations. Intersil Pb-free products are MSL classified at Pb-free peak reflow temperatures that meet or exceed the Pb-free requirements of IPC/JEDEC J STD-020.

Absolute Maximum Ratings (Reference to GND)

Supply Voltage (VDD) 5.5V
All Other Pins. . . . . -0.5 to VDD+0.5V
ESD Rating
Human Body Model (Per MIL-STD-883 Method 3015.7) . . .4000V
Machine Model (Per EIAJ ED-4701 Method C-111) 400V
CDM 1000V

Recommended Operating Conditions

Ambient Temperature Range . . . . -20°C to +85°C

Thermal Information

Thermal Resistance (Typical)	θ_{JA} (°C/W)	θ_{JC} (°C/W)
SOT-23 Package (Note 1)	200	N/A
2x3 TDFN Package (Notes 2, 3)	70	10.5

Maximum Junction Temperature (Plastic Package) . . . . +125°C
Maximum Storage Temperature Range . . . . -40°C to +125°C
Maximum Lead Temperature (Soldering 10s) . . . . +300°C

CAUTION: Stresses above those listed in “Absolute Maximum Ratings” may cause permanent damage to the device. This is a stress only rating and operation of the device at these or any other conditions above those indicated in the operational sections of this specification is not implied.

NOTE:

1. θ_{JA} is measured with the component mounted on a high effective thermal conductivity test board in free air. See Tech Brief TB379 for details.
2. θ_{JA} is measured in free air with the component mounted on a high effective thermal conductivity test board with “direct attach” features. See Tech Brief TB379.
3. For θ_{JC}, the “case temp” location is the center of the exposed metal pad on the package underside.

Electrical Specifications

Unless otherwise noted, all parameters are guaranteed over the operational supply voltage and temperature range of the device as follows: T_A = -20°C to +85°C; V_{DD} = 2.6V to 4.8V.

PARAMETER	SYMBOL	TEST CONDITIONS	MIN	TYP	MAX	UNITS
DC CHARACTERISTICS						
Supply Voltage	V_{DD}	During normal operation	2.6	-	4.8	V
		During OTP ROM programming	2.8	-	4.8	V
Run Mode Supply Current (exclude I/O current)	I_{DD}	V_{DD} = 4.2V	-	110	140	µA
		V_{DD} = 4.8V	-	120	160	µA
Sleep Mode Supply Current	I_{DDS}	V_{DD} = 4.2V, XSD pin floating	-	0.15	0.5	µA
OTP Programming Mode Supply Current	I_{DDP}	For ~ 1.8ms duration per write operation	-	250	500	µA
Internal Regulated Supply Voltage	V_{RG}	Observable only in test mode	2.3	2.5	2.7	V
Internal OTP ROM Programming Voltage	V_{PP}	Observable only in test mode	11	12	13	V
POR Release Threshold	V_{POR+}		1.9	2.2	2.4	V
POR Assertion Threshold	V_{POR-}		1.5	1.8	2.1	V
XSD PIN CHARACTERISTICS						
XSD Input Low Voltage	V_{IL}		-0.4	-	0.5	V
XSD Input High Voltage	V_{IH}		1.5	-	V_{DD}+ 0.4V	V
XSD Input Hysteresis	V_{HYS}		-	400	-	mV
XSD Internal Pull-Down Current	I_{PD}	V_{DD} = 2.6V	-	0.8	-	µA
		V_{DD} = 4.2V	-	1.2	2.0	µA
		V_{DD} = 4.8V	-	1.8	2.5	µA
XSD Output Low Voltage	V_{OL}	I_{OL} = 1mA	-	-	0.4	V
XSD Input Transition Time	t_X	10% to 90% transition time	-	-	2	µs
XSD Output Fall Time	t_F	90% to 10%, C_{LOAD} = 12pF	-	-	50	ns
XSD Pin Capacitance	C_{PIN}		-	6	-	pF
XSD BUS TIMING CHARACTERISTICS (Refer to XSD Bus Symbol Timing Definitions Tables)						
Programming Bit Rate		x = 0.5 to 4	2.89	-	23.12	kHz
XSD Input Deglitch Time	T_{WDG}	Pulse width narrower than the deglitch time will not cause the device to wake up	7	-	20	µs

Electrical Specifications Unless otherwise noted, all parameters are guaranteed over the operational supply voltage and tempe range of the device as follows: T_A = -20°C to +85°C; V_{DD} = 2.6V to 4.8V. (Continued)

PARAMETER	SYMBOL	TEST CONDITIONS	MIN	TYP	MAX	UNITS
Device Wake-Up Time	T_{WKE}	From falling-edge of break command issued by host to falling-edge of break command returned by device	35	60	100	µs
Device Sleep Wait Time	T_{SLP}	From when the ‘11’ Opcode is detected to the shut-off of the internal regulator	4	-	-	µs
Auto-Sleep Time-Out Period	T_{ASLP}	From the last transition detected on the XSD bus to the device going into sleep mode	0.9	-	1.1	s
OTP ROM Write Time	T_{EEW}	From the last BT of the 2nd write data frame to when device is ready to accept the next instruction	-	1.8	1.9	ms
Hash Calculation Time	T_{HASH}	From the last BT of the Challenge Code Word from the host to the Authentication Code being available for read	-	1	-	BT
Soft-Reset Time	T_{SRST}	From the last BT of the Soft-Reset instruction issued by the host to the falling-edge of break command returned by device	-	-	30	µs
AC CHARACTERISTICS						
Oscillator Clock Frequency	f_{OSC}	Internal bus reference clock	505	532	560	kHz
Charge Pump Clock Frequency	f_{CP}	Internal high speed clock (observable only in test mode)				
		Low-speed mode	3.6	5	6	MHz
		High-speed mode	16	20	24	MHz

Pin Descriptions

PIN NUMBER	PIN NAME	DESCRIPTION
1	VSS	System ground.
2	NC	No connection.
3	VDD	Supply voltage.
4	TIO	Production test I/O pin. Used only during production testing. Must be left floating during normal operation.
5	XSD	Communication bus with weak internal pull-down to VSS. This pin is a Schmitt-trigger input and an open-drain output. An appropriate pull-up resistor is required on the host side.

Typical Applications

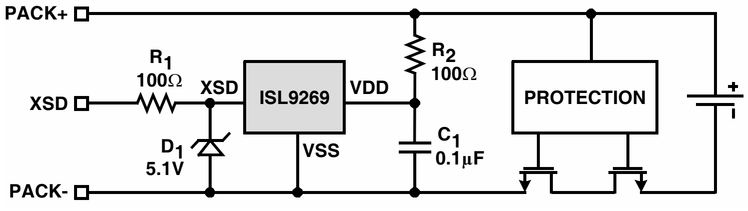


FIGURE 1. TYPICAL APPLICATION WITH THE ISL6296 POWERED BY THE BATTERY

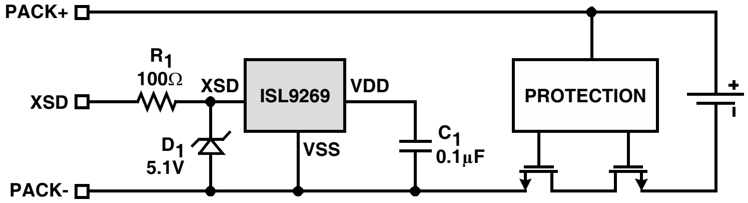


FIGURE 2. TYPICAL APPLICATION WITH THE ISL6296 POWERED BY THE XSD BUS

Block Diagram

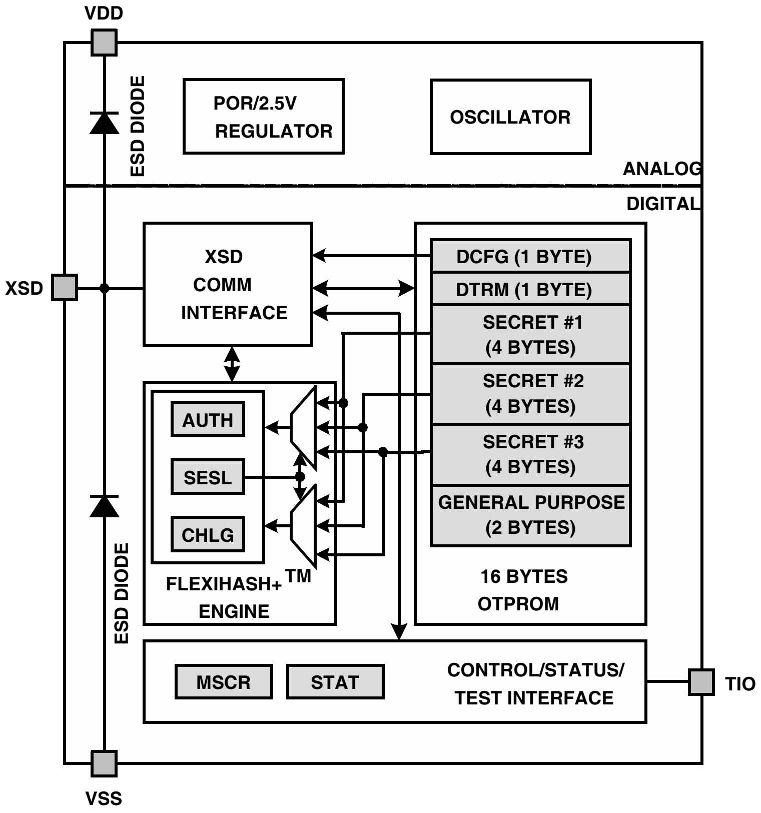


FIGURE 3. FUNCTIONAL BLOCK DIAGRAM

Theory of Operation

The ISL6296 contains all circuitry required to support battery pack authentication based on a challenge-response scheme. It provides a 16-Byte One-Time Programmable Read-Only Memory (OTPROM) space for the storage of up to 96-Bit of secret for the authentication and other user information. A 32-Bit CRC-based hash engine (FlexiHash™) calculates the authentication result immediately after receiving a 32-Bit random challenge code. The communication between the ISL6296 and the host is implemented through the XSD single-wire communication bus.

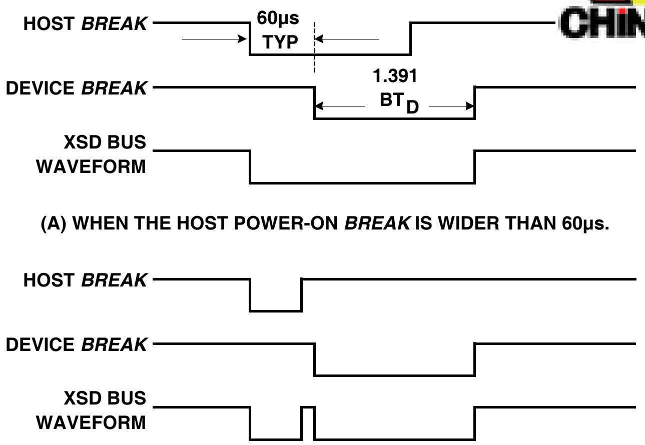
Major functions within the ISL6296 include the following, as shown in Figure 3.

- Power-on reset (POR) and a 2.5V regulator to power all internal logic circuits.
- 16 x 8-Bit (16-Byte) OTP ROM as shown in Table 8. The first part (two bytes) contains the device default configuration (DCFG) information (such as the device address and the XSD communication speed) and the default trimming (DTRM) information (such as the internal oscillator frequency trimming). The second part contains two groups (12-Byte) of memory that can be independently locked out for the storage of up to three sets of secret. The last part provides two additional bytes of space for general-purpose information.
- Control functions, including master control (MSCR) and status (STAT) registers (as shown in Table 9), interrupt generation, and the test-related interface.
- FlexiHash™ engine that includes the 32-Bit CRC-based hash engine, secret selection register, challenge code register, and the authentication result register. Table 10 shows all the registers.
- XSD communication bus Interface. The XSD device address and the communication speed are configured in the DCFG address in the OTPROM, as given in Table 8.
- Time Base Reference.

The following explain in detail the operation of the ISL6296.

Power-On Reset (POR)

The ISL6296 powers up in Sleep mode. It remains in Sleep mode until a power-on 'break' command is received from the host through the XSD bus. The initial power-on 'break' can be of any pulse width as long as it is wider than the XSD input deglitch time (20µs). Once the 'break' command is received, the internal regulator is powered up. About 20µs after the falling edge of the power-on 'break', an internal POR circuit releases the reset to the digital block, and a POR sequence is started. During the POR sequence, the ISL6296 initializes itself by loading the default device configuration information from pre-assigned locations within the OTP ROM memory. After initialization, a 'break' command is returned to the host to indicate that the ISL6296 is ready and waiting for a bus transaction from the host.



(A) WHEN THE HOST POWER-ON *BREAK* IS WIDER THAN 60µs.

(B) WHEN THE HOST POWER-ON *BREAK* IS NARROWER THAN 60µs.

FIGURE 4. POWER-ON BREAK SIGNAL TO WAKE-UP THE ISL6296 FROM SLEEP MODE

Note that the ISL6296 will initiate the power-on sequence without waiting for the power-on 'break' signal to return to the high state. If the host sends an initial 'break' pulse wider than 60µs, the device-ready 'break' returned by the ISL6296 will likely be merged with the pulse sent by the host and, therefore, may not be detectable. Figure 4 illustrates the waveforms during the Power-on Reset. Figure 4 (A) represents the case when the power-on 'break' rising edge occurs after the device starts sending the 'break'. Figure 4 (B) represents the case when the power-on 'break' finishes before the device sends its 'break'. The device break signal is always 1.391 times of the device bit-time (BT, see XSD Bus Interface section for more details). Either case in Figure 4 will wake up the device successfully if the device is in the sleep mode.

It is important to keep in mind that a narrow 'break' signal will be taken as a normal bit signal and cause errors, if the device is not in the sleep mode. For this reason, the narrow power-on 'break' signal should be used only if the user has to see the returned 'break' signal.

Auto-Sleep

While the ISL6296 is powered up and there is no bus activity for more than about 1 second, the device will automatically return to Sleep mode. Sleep mode can be entered independent of whether the XSD bus is held high or low. While the ISL6296 is in Sleep mode, it is recommended that the XSD bus be held low to eliminate current drain through the XSD-pin internal pull-down current.

Auto-Sleep mode can be disabled by clearing the ASLP bit in the MSCR register. By default, Auto-Sleep is always enabled at power-up and after a soft reset. Auto-sleep function can be permanently disabled by clearing the 0-00[2] bit (the ASLP bit in DCFG) during OTP ROM programming.