ABRIDGED DATA SHEET

EVALUATION KIT AVAILABLE

Click here for production status of specific part numbers.

DS28C36

DeepCover Secure Authenticator

General Description

The DS28C36 is a DeepCover® secure authenticator that provides a core set of cryptographic tools derived from integrated asymmetric (ECC-P256) and symmetric (SHA-256) security functions. In addition to the security services provided by the hardware implemented crypto engines, the device integrates a FIPS/NIST true random number generator (RNG), 8Kb of secured EEPROM, a decrement-only counter, two pins of configurable GPIO, and a unique 64-bit ROM identification number (ROM ID).

The ECC public/private key capabilities operate from the NIST defined P-256 curve and include FIPS 186 compliant ECDSA signature generation and verification to support a bidirectional asymmetric key authentication model. The SHA-256 secret-key capabilities are compliant with FIPS 180 and are flexibly used either in conjunction with ECDSA operations or independently for multiple HMAC functions.

Two GPIO pins can be independently operated under command control and include configurability supporting authenticated and nonauthenticated operation including an ECDSA-based crypto-robust mode to support secure-boot of a host processor.

DeepCover embedded security solutions cloak sensitive data under multiple layers of advanced security to provide the most secure key storage possible. To protect against device-level security attacks, invasive and noninvasive countermeasures are implemented including active die shield, encrypted storage of keys, and algorithmic methods.

Applications

- IoT Node Crypto-Protection
- Accessory and Peripheral Secure Authentication
- Secure Storage of Cryptographic Keys for a Host Controller
- Secure Boot or Download of Firmware and/or System Parameters

DeepCover is a registered trademark of Maxim Integrated Products, Inc.

Benefits and Features

- ECC-256 Compute Engine
  - FIPS 186 ECDSA P256 Signature and Verification
  - ECDH Key Exchange with Authentication Prevents Man-in-the-Middle Attacks
  - ECDSA Authenticated R/W of Configurable Memory
- FIPS 180 SHA-256 Compute Engine
  - HMAC
- SHA-256 OTP (One-Time Pad) Encrypted R/W of Configurable Memory Through ECDH Established Key
- Two GPIO Pins with Optional Authentication Control
  - Open-Drain, 4mA/0.4V
  - Optional SHA-256 or ECDSA Authenticated On/Off and State Read
  - Optional ECDSA Certificate to Set On/Off after Multiblock Hash for Secure Boot
- RNG with NIST SP 800-90B Compliant Entropy Source with Function to Read Out
- Optional Chip Generated Pr/Pu Key Pairs for ECC Operations
- 17-Bit One-Time Settable, Nonvolatile Decrement-Only Counter with Authenticated Read
- 8Kbits of EEPROM for User Data, Keys, and Certificates
- Unique and Unalterable Factory Programmed 64-Bit Identification Number (ROM ID)
  - Optional Input Data Component to Crypto and Key Operations
- I^2C Communication Up to 1MHz
- Operating Range: 2.2V to 3.63V, -40°C to +85°C
- 6-Pin TDFN Package

***Ordering Information* appears at end of data sheet.**

***Typical Application Circuit* appears at end of data sheet.**

19-8564; Rev 2; 1/19

maxim integrated™

Absolute Maximum Ratings

Voltage Range on Any Pin Relative to GND .....-0.5V to 4.0V
Maximum Current into Any Pin.....20mA
Operating Temperature Range..... -40°C to +85°C
Junction Temperature.....+125°C
Storage Temperature Range..... -55°C to +125°C
Lead temperature (soldering, 10s).....+300°C
Soldering Temperature (reflow)..... +260°C

Stresses beyond those listed under "Absolute Maximum Ratings" may cause permanent damage to the device. These are stress ratings only, and functional operation of the device at these or any other conditions beyond those indicated in the operational sections of the specifications is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

Package Information

6 TDFN-EP

Package Code	X14400F+1
Outline Number	21-0137
Land Pattern Number	90-0058
Thermal Resistance, Single-Layer Board:	
Junction to Ambient (θ_{JA})	55°C/W
Junction to Case (θ_{JC})	9°C/W
Thermal Resistance, Four-Layer Board:	
Junction to Ambient (θ_{JA})	42°C/W
Junction to Case (θ_{JC})	9°C/W

For the latest package outline information and land patterns (footprints), go to www.maximintegrated.com/packages. Note that a "+", "#", or "-" in the package code indicates RoHS status only. Package drawings may show a different suffix character, but the drawing pertains to the package regardless of RoHS status.

Package thermal resistances were obtained using the method described in JEDEC specification JESD51-7, using a four-layer board. For detailed information on package thermal considerations, refer to www.maximintegrated.com/thermal-tutorial.

Electrical Characteristics

(T_A = -40°C to +85°C.) (Note 1)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
Supply Voltage	V_{CC}	DS28C36	2.97	3.3	3.63	V
		DS28C36B	2.2			
Active Supply Current	I_{CC}	(Note 2)			300	µA
Standby Supply Current	I_{CCS}				250	µA
Computation Current	I_{CMP}	(Note 3)			7.5	mA
GPIO						
Output Low	$PIOV_{OL}$				0.4	V
Input Low	$PIOV_{IL}$		-0.3		V_{CC} x 0.3	V
Input High	$PIOV_{IH}$		V_{CC} x 0.7		V_{CC} + 0.3	V
Leakage current	I_L	DS28C36	-10		+10	µA
		DS28C36B	-1		+1	
ECC ENGINE						
Generate ECDSA Signature Time	t_{GES}				50	ms
Generate ECC Key Pair	t_{GKP}				100	ms
Verify ECDSA Signature or Compute ECDH Time	t_{VES}				150	ms
SHA-256 ENGINE						
Computation Time (HMAC or RNG)	t_{CMP}				3	ms

Electrical Characteristics (continued)

(T_A = -40°C to +85°C.) (Note 1)

PARAMETER	SYMBOL	CONDITIONS		MIN	TYP	MAX	UNITS
EEPROM							
W/E Endurance	NCY	(Note 4)		100K			—
Read Memory Time	t_{RM}					1	ms
Write Memory Time	t_{WM}					15	ms
Data Retention	t_{DR}	T_A = +85°C (Note 5)		10			years
I²C SCL AND SDA PINS (Note 6)							
Low-Level Input Voltage	V_{IL}			-0.3		0.3 × V_{CC}	V
High-Level Input Voltage	V_{IH}			0.7 × V_{CC}		V_{CC} + 0.3	V
Hysteresis of Schmitt Trigger Inputs	V_{HYS}	(Note 7)			0.05 × V_{CC}		V
Low-Level Output Voltage at 4mA Sink Current	V_{OL}					0.4	V
Output Fall Time from $V_{IH(MIN)}$ to $V_{IL(MAX)}$ with a Bus Capacitance from 10pF to 400pF	t_{OF}	(Note 7)			30		ns
Pulse Width of Spikes that are Suppressed by the Input Filter	t_{SP}	(Note 7)				50	ns
Input Current with an Input Voltage Between 0.1VCCmax and 0.9VCCmax	II	DS28C36		-10		+10	µA
		DS28C36B (Note 8)		-1		+1	
Input Capacitance	CI	(Note 7)			10		pF
SCL Clock Frequency	f_{SCL}	(Note 9)	DS28C36	0		0.4	MHz
			DS28C36B	0		1	
Hold Time (Repeated) START Condition	$t_{HD:STA}$		DS28C36	0.6			µs
			DS28C36B	0.45			
Low Period of the SCL Clock	t_{LOW}	(Note 10)	DS28C36	1.3			µs
			DS28C36B	0.65			
High Period of the SCL Clock	t_{HIGH}		DS28C36	0.6			µs
			DS28C36B	0.35			
Setup Time for a Repeated START Condition	$t_{SU:STA}$		DS28C36	0.6			µs
			DS28C36B	0.35			
Data Hold Time	$t_{HD:DAT}$	(Notes 7, 10, 11)	DS28C36			0.9	µs
			DS28C36B			0.35	
Data Setup Time	$t_{SU:DAT}$	(Notes 10, 12)		100			ns
Setup Time for STOP Condition	$t_{SU:STO}$		DS28C36	0.6			µs
			DS28C36B	0.35			
Bus Free Time Between a STOP and START Condition	t_{BUF}		DS28C36	1.3			µs
			DS28C36B	0.6			
Capacitive Load for Each Bus Line	C_B	(Notes 9, 13)				400	pF
Warm-Up Time	t_{OSCWUP}	(Note 14)	DS28C36			0.25	ms
			DS28C36B			1.0	

Electrical Characteristics (continued)

(T_A = -40°C to +85°C.) (Note 1)

Note 1: Limits are 100% production tested at T_A = +25°C and/or T_A = +85°C. Limits over the operating temperature range and relevant supply voltage range are guaranteed by design and characterization. Typical values at +25°C.

Note 2: Operating current continuously reading memory at 400kHz with < 25ns rise and fall times on SDA and SCL.

Note 3: Average current drawn from V_{CC} during EEPROM read, EEPROM write, RNG calculation, SHA-256 calculation, or ECDSA calculation.

Note 4: Write-cycle endurance is tested in compliance with JESD47H.

Note 5: Data retention is rested in compliance with JESD47H.

Note 6: All I^2C timing values are referred to $V_{IH(MIN)}$ and $V_{IL(MAX)}$ levels.

Note 7: Guaranteed by design and/or characterization only. Not production tested.

Note 8: I/O pins of the DS28C36B do not obstruct the SDA and SCL lines if V_{CC} is switched off.

Note 9: System requirement.

Note 10: t_{LOW} min = $t_{HD:DAT}$ max + t_{EDGE} max + $t_{SU:DAT}$ min, where t_{EDGE} is rise or fall time. For the DS28C36, t_{EDGE} max = 300ns; for the DS28C36B, t_{EDGE} max = 200ns. Values greater than these can be accommodated by extending t_{LOW} accordingly.

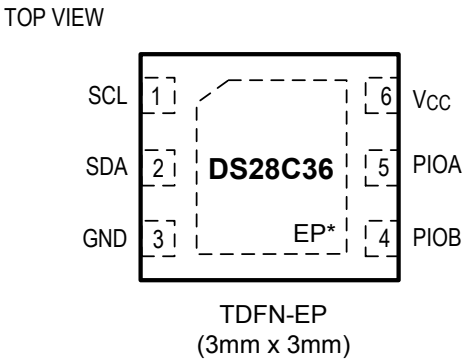
Note 11: The DS28C36 provides a hold time of at least 100ns for the SDA signal (referred to the $V_{IH(MIN)}$ of the SCL signal) to bridge the undefined region of the falling edge of SCL. The master can provide a hold time of 0ns when writing to the device.

Note 12: The DS28C36 can be used in a standard-mode I^2C bus system, but the requirement $t_{SU:DAT}$ ≥ 250ns must then be met (I^2C bus specification Rev. 03, 19 June 2007).

Note 13: C_B = total capacitance of one bus line in pF. The maximum bus capacitance allowable can vary from this value depending on the actual operating voltage and frequency of the application (I^2C bus specification Rev. 03, 19 June 2007).

Note 14: I^2C communication should not take place for max t_{OSCWUP} time following a power-on reset.

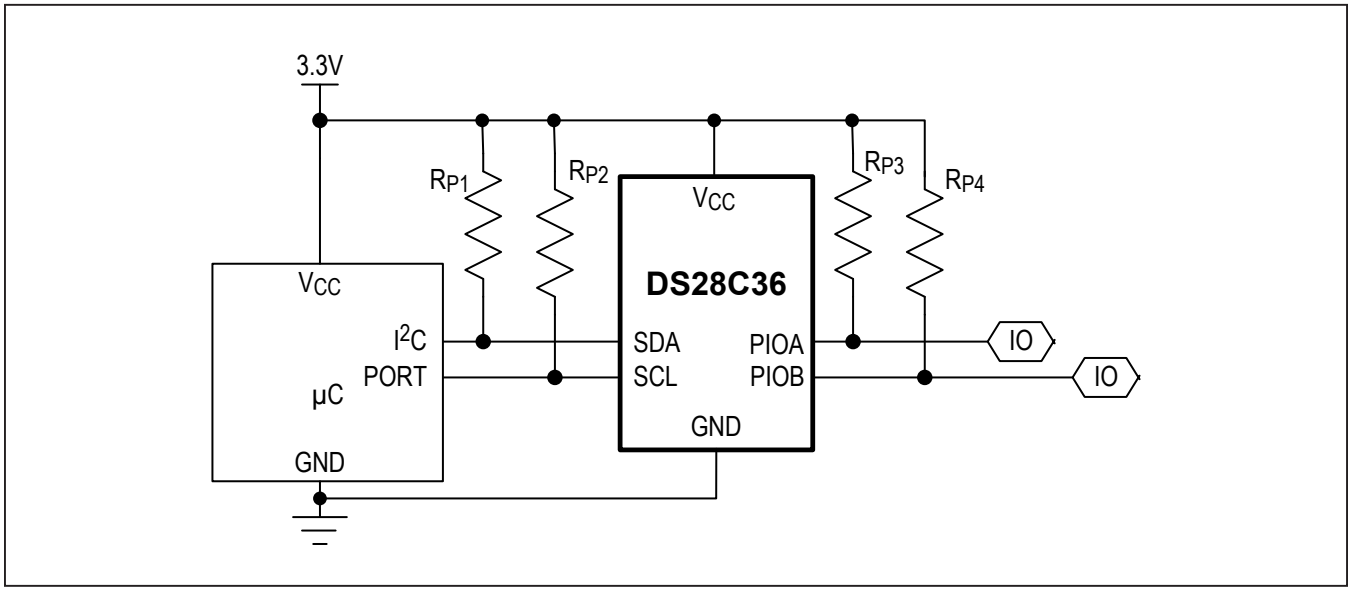
Pin Configuration



Pin Description

PIN	NAME	FUNCTION
1	SCL	I^2C CLK. Connect to V_{CC} with a pullup resistor.
2	SDA	I^2C Data. Connect to V_{CC} with a pullup resistor.
3	GND	Ground
4	PIOB	General-Purpose IO
5	PIOA	General-Purpose IO
6	V_{CC}	Supply Voltage
—	EP	Exposed Pad. Solder evenly to the board's ground plane for proper operation. Refer to Application Note 3273: Exposed Pads: *A Brief Introduction* for additional information.

Typical Application Circuit



Ordering Information

PART	TEMP RANGE	PIN-PACKAGE
DS28C36Q+T†	-40°C to +85°C	6 TDFN-EP* (2.5k pcs)
DS28C36BQ+T	-40°C to +85°C	6 TDFN-EP* (2.5k pcs)

+Denotes a lead(Pb)-free/RoHS-compliant package.

T= Tape and reel.

**EP = Exposed pad.*

†Not recommended for new designs.

For pricing, delivery, and ordering information, please visit Maxim Integrated's online storefront at https://www.maximintegrated.com/en/storefront/storefront.html.

Maxim Integrated cannot assume responsibility for use of any circuitry other than circuitry entirely embodied in a Maxim Integrated product. No circuit patent licenses are implied. Maxim Integrated reserves the right to change the circuitry and specifications without notice at any time. The parametric values (min and max limits) shown in the Electrical Characteristics table are guaranteed. Other parametric values quoted in this data sheet are provided for guidance.

