maxim integrated™

要約版データシート

EVALUATION KIT AVAILABLE

219-0022; Rev 0; 12/12

DS28EL25

DeepCoverセキュア認証用IC、1-Wire SHA-256および4KbユーザーEEPROM内蔵

概要

DeepCover®エンベデッドセキュリティソリューションは、複数層の高度物理セキュリティによって機密データを秘匿し、可能な限り業界で最もセキュアなキーストレージを提供します。Deepcoverセキュア認証用IC (DS28EL25)は、高い暗号強度、双方向性、FIPS 180-3で規定されたセキュアハッシュアルゴリズム(SHA-256)に基づくセキュアなチャレンジ/レスポンス認証の機能性を兼ね備えています。4KbのユーザーEEPROMアレイはアプリケーションデータの不揮発性ストレージを提供し、その他の保護されたメモリにはSHA-256の動作用の読取り保護されたシークレットおよびユーザーメモリ制御用の設定が保持されます。各デバイスは、出荷時にチップにプログラムされる保証された固有の64ビットROM識別番号(ROM ID)を備えています。この固有のROM IDは、暗号操作用の基本的な入力パラメータとして使用されるとともに、アプリケーション内での電子的なシリアルナンバーとしても機能します。双方向のセキュリティモデルによって、ホストシステムとスレーブに内蔵されたDS28EL25の間での双方向の認証が可能です。スレーブからホストの認証は、接続または内蔵されたDS28EL25の正当性を完全に認証するために、ホストシステムによって使用されます。ホストからスレーブの認証は、不正なホストによる書換えからDS28EL25のユーザーメモリを保護するために使用されます。SHA-256メッセージ認証コード(MAC)はDS28EL25が生成し、ユーザーメモリ内のデータ、チップ内蔵のシークレット、ホストのランダムなチャレンジ、および64ビットROM IDを用いて計算します。DS28EL25は、単一接点の1-Wire®バス上で、オーバードライブ速度で通信を行います。通信は1-Wireプロトコルに従い、複数のデバイスの1-Wireネットワークの場合はROM IDがノードアドレスの役割を果たします。

アプリケーション

ネットワーク接続機器の認証

プリンタカートリッジの識別/認証

リファレンス設計のライセンス管理

システムの知的所有権保護

センサー/アクセサリの認証および較正

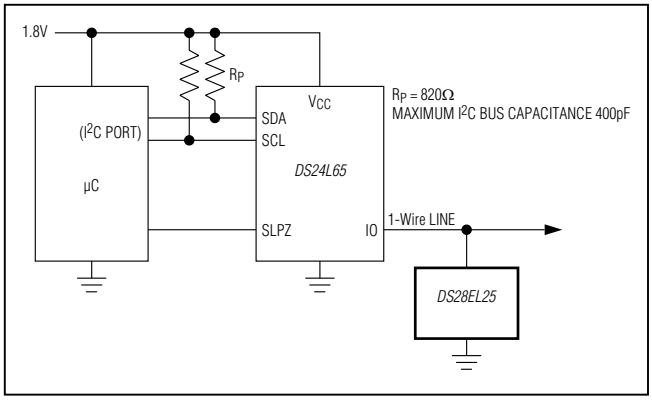
設定可能なシステム用のセキュアな機能設定

暗号システムの鍵生成および交換

特長

- SHA-256に基づく対称鍵ベースの双方向セキュア認証モデル
- SHA-256 MAC生成のための専用のハードウェア高速化SHAエンジン
- 高ビット数、ユーザー設定可能なシークレット、および入力チャレンジを使用した強力な認証
- 256ビットx 16ページに分割された4096ビットのユーザーEEPROM
- 認証/書込み/読取り保護、およびOTP/EPROMエミュレーションを含む、ユーザー設定可能で不可逆なEEPROMの保護モード
- 出荷時設定される固有の64ビットID
- 最大76.9kbpsでホストと通信する単一接点の1-Wireインタフェース
- 動作範囲：1.8V ±5%、-40℃～+85℃
- 低電力スタンバイ：5µA (typ)
- ±8kVヒューマンボディモデルESD保護(typ)
- 6ピンTDFNパッケージ

標準アプリケーション回路



型番はデータシートの最後に記載されています。

関連部品およびこの製品とともに使用可能な推奨製品については、japan.maximintegrated.com/DS28EL25.related を参照してください。

本データシートは日本語翻訳であり、相違及び誤りのある可能性があります。設計の際は英語版データシートを参照してください。

価格、納期、発注情報についてはMaxim Direct (0120-551056)にお問い合わせいただくか、Maximのウェブサイト(japan.maximintegrated.com)をご覧ください。

ABSOLUTE MAXIMUM RATINGS

IO Voltage Range to GND..... -0.5V to 4.0V
IO Sink Current.....20mA
Operating Temperature Range ..... -40°C to +85°C
Junction Temperature .....+150°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.

ELECTRICAL CHARACTERISTICS

(T_A = -40°C to +85°C, unless otherwise noted.) (Note 1)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
IO PIN: GENERAL DATA						
1-Wire Pullup Voltage	V_{PUP}	(Note 2)	1.71		1.89	V
1-Wire Pullup Resistance	R_{PUP}	V_{PUP} = 1.8V ±5% (Note 3)	300		750	Ω
Input Capacitance	C_{IO}	(Notes 4, 5)		1500		pF
Input Load Current	I_L	IO pin at V_{PUP}		5	19.5	µA
High-to-Low Switching Threshold	V_{TL}	(Notes 6, 7)		0.65 x V_{PUP}		V
Input Low Voltage	V_{IL}	(Notes 2, 8)			0.3	V
Low-to-High Switching Threshold	V_{TH}	(Notes 6, 9)		0.75 x V_{PUP}		V
Switching Hysteresis	V_{HY}	(Notes 6, 10)		0.3		V
Output Low Voltage	V_{OL}	I_{OL} = 4mA (Note 11)			0.4	V
Recovery Time	t_{REC}	R_{PUP} = 750Ω (Notes 2, 12)	5			µs
Time-Slot Duration	t_{SLOT}	(Notes 2, 13)	13			µs
IO PIN: 1-Wire RESET, PRESENCE-DETECT CYCLE						
Reset Low Time	t_{RSTL}	(Note 2)	48		80	µs
Reset High Time	t_{RSTH}	(Note 14)	48			µs
Presence-Detect Sample Time	t_{MSP}	(Notes 2, 15)	8		10	µs
IO PIN: 1-Wire WRITE						
Write-Zero Low Time	t_{W0L}	(Notes 2, 16)	8		16	µs
Write-One Low Time	t_{W1L}	(Notes 2, 16)	1		2	µs
IO PIN: 1-Wire READ						
Read Low Time	t_{RL}	(Notes 2, 17)	1		2 - δ	µs
Read Sample Time	t_{MSR}	(Notes 2, 17)	t_{RL} + δ		2	µs
EEPROM						
Programming Current	I_{PROG}	V_{PUP} = 1.89V (Notes 5, 18)			1	mA
Programming Time for a 32-Bit Segment or Page Protection	t_{PRD}	(Note 19)			10	ms
Programming Time for the Secret	t_{PRS}	**Refer to the full data sheet.**				ms
Write/Erase Cycling Endurance	N_{CY}	T_A = +85°C (Notes 21, 22)	100k			—
Data Retention	t_{DR}	T_A = +85°C (Notes 23, 24, 25)	10			Years

ELECTRICAL CHARACTERISTICS (continued)

(T_A = -40°C to +85°C, unless otherwise noted.) (Note 1)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
SHA-256 ENGINE						
Computation Current	I_{CSHA}	**Refer to the full data sheet.**				mA
Computation Time	t_{CSHA}					ms

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 are not guaranteed.
Note 2: System requirement.
Note 3: Maximum allowable pullup resistance is a function of the number of 1-Wire devices in the system and 1-Wire recovery times. The specified value here applies to systems with only one device and with the minimum 1-Wire recovery times.
Note 4: Typical value represents the internal parasite capacitance when V_{PUP} is first applied. Once the parasite capacitance is charged, it does not affect normal communication.
Note 5: Guaranteed by design and/or characterization only; not production tested.
Note 6: V_{TL}, V_{TH}, and V_{HY} are a function of the internal supply voltage, which is a function of V_{PUP}, R_{PUP}, 1-Wire timing, and capacitive loading on IO. Lower V_{PUP}, higher R_{PUP}, shorter t_{REC}, and heavier capacitive loading all lead to lower values of V_{TL}, V_{TH}, and V_{HY}.
Note 7: Voltage below which, during a falling edge on IO, a logic-zero is detected.
Note 8: The voltage on IO must be less than or equal to V_{ILMAX} at all times when the master is driving IO to a logic-zero level.
Note 9: Voltage above which, during a rising edge on IO, a logic-one is detected.
Note 10: After V_{TH} is crossed during a rising edge on IO, the voltage on IO must drop by at least V_{HY} to be detected as logic-zero.
Note 11: The I-V characteristic is linear for voltages less than 1V.
Note 12: Applies to a single device attached to a 1-Wire line.
Note 13: Defines maximum possible bit rate. Equal to $1/(t_{W0LMIN} + t_{RECMIN})$.
Note 14: An additional reset or communication sequence cannot begin until the reset high time has expired.
Note 15: Interval after t_{RSTL} during which a bus master can read a logic 0 on IO if there is a DS28EL25 present. The power-up presence detect pulse could be outside this interval. See the *Typical Operating Characteristics* for details.
Note 16: ε in Figure 11 represents the time required for the pullup circuitry to pull the voltage on IO up from V_{IL} to V_{TH}. The actual maximum duration for the master to pull the line low is $t_{W1LMAX} + t_F - \varepsilon$ and $t_{W0LMAX} + t_F - \varepsilon$, respectively.
Note 17: δ in Figure 11 represents the time required for the pullup circuitry to pull the voltage on IO up from V_{IL} to the input-high threshold of the bus master. The actual maximum duration for the master to pull the line low is $t_{RLMAX} + t_F$.
Note 18: Current drawn from IO during the EEPROM programming interval or SHA-256 computation. The pullup circuit on IO during the programming and computation interval should be such that the voltage at IO is greater than or equal to V_{PUPMIN}. A low-impedence bypass of R_{PUP} activated during programming and computation is the recommended way to meet this requirement.
Note 19: Refer to the full data sheet.

Note 20: Refer to the full data sheet.

Note 21: Write-cycle endurance is tested in compliance with JESD47G.
Note 22: Not 100% production tested; guaranteed by reliability monitor sampling.
Note 23: Data retention is tested in compliance with JESD47G.
Note 24: Guaranteed by 100% production test at elevated temperature for a shorter time; equivalence of this production test to the data sheet limit at operating temperature range is established by reliability testing.
Note 25: EEPROM writes can become nonfunctional after the data retention time is exceeded. Long-term storage at elevated temperatures is not recommended.

DS28EL25

DeepCoverセキュア認証用IC、1-Wire SHA-256および4KbユーザーEEPROM内蔵

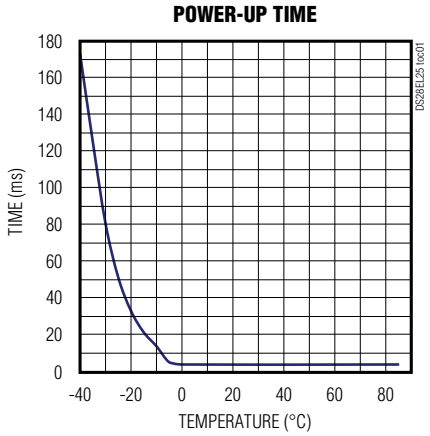
ELECTRICAL CHARACTERISTICS (continued)

(T_A = -40°C to +85°C, unless otherwise noted.) (Note 1)

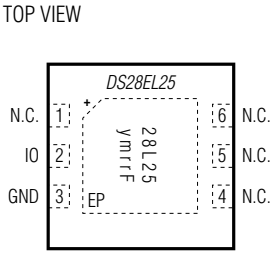
Note 26: Refer to the full data sheet.

標準動作特性

(V_{PUP} = 1.71V, V_{IL} = 0.3V)



ピン配置



TDFN
(3mm × 3mm)

端子説明

端子	名称	機能
3	GND	グランド基準
2	IO	1-Wireバスインタフェース。外付けのプルアップ抵抗を必要とするオープンドレイン信号です。
1, 4, 5, 6	N.C.	接続されていません
—	EP	エクスポーズドパッド。適切な動作のために、PCBのグランドプレーンに均等にはんだ付けしてください。詳細については、アプリケーションノート3273「Exposed Pads: A Brief Introduction」を参照してください。

DS28EL25

DeepCoverセキュア認証用IC、1-Wire SHA-256および4KbユーザーEEPROM内蔵

注：この資料はフルデータシートの要約版です。デバイスの詳細情報はフルデータシートでのみご覧いただけます。フルデータシートは**japan.maximintegrated.com/DS28EL25**からご請求ください。「**フルデータシートを請求する**」をクリックしてください。

型番

PART	TEMP RANGE	PIN-PACKAGE
DS28EL25Q+T	-40°C to +85°C	6 TDFN-EP* (2.5k pcs)

+は鉛(Pb)フリー/RoHS準拠パッケージを表します。
T = テープ&リール。
*EP = エクスポーズドパッド

パッケージ

最新のパッケージ図面情報およびランドパターン(フットプリント)は**japan.maximintegrated.com/packages**を参照してください。なお、パッケージコードに含まれる「+」、「#」、または「-」はRoHS対応状況を表したものでしかありません。パッケージ図面はパッケージそのものに関するものでRoHS対応状況とは関係がなく、図面によってパッケージコードが異なることがある点を注意してください。

パッケージタイプ	パッケージコード	外形図No.	ランドパターンNo.
6 TDFN-EP	T633+2	21-0137	90-0058

DS28EL25

DeepCoverセキュア認証用IC、1-Wire SHA-256および4KbユーザーEEPROM内蔵

改訂履歴

版数	改訂日	説明	改訂ページ
0	12/12	初版	—

maxim integrated™

マキシム･ジャパン株式会社　〒141-0032　東京都品川区大崎1-6-4 大崎ニューシティ 4号館 20F　TEL: 03-6893-6600