

## DS28E15

# DeepCoverセキュア認証用IC、1-Wire SHA-256 および512ビットユーザー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、機密データを高度物理セキュリティの複数レイヤ下に隠し、最もセキュアなキーストレージを実現します。

DeepCoverセキュア認証用IC (DS28E15)は、高い暗号強度、双方向性、セキュリティを備えたチャレンジ/レスポンス認証機能と、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)に基づく実装を組み合わせています。512ビットのユーザー設定可能なEEPROMアレイはアプリケーションデータの揮発性ストレージを提供します。その他の保護されたメモリには、SHA-256処理用の読取り保護されたシークレットやメモリ保護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DS28E15の間での双方向の認証が可能で、スレーブからホストへの認証は、接続または内蔵されたDS28E15の正当性をセキュアな形で検証するために、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への認証は、不正なホストによる書換えからDS28E15のユーザーメモリを保護するために使用されます。DS28E15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

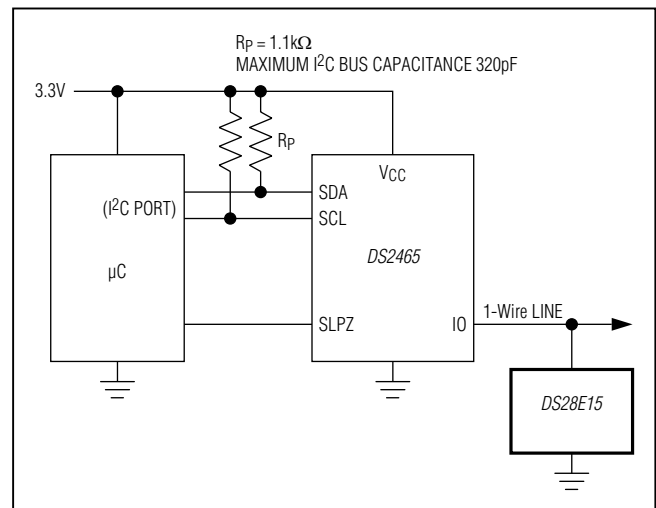
- 消耗品の認証
- セキュア機能制御

**型番**はデータシートの最後に記載されています。

### 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
- ◆ 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x2ページに分割された512ビットのユーザーEEPROM
- ◆ 認証/書き込み/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
- ◆ 出荷時に設定された固有の64ビットID番号
- ◆ 単一接点の1-Wireインタフェース
- ◆ 動作範囲：3.3V ±10%、-40°C ~ +85°C
- ◆ ESD保護：±8kV HBM (typ)
- ◆ パッケージ：2ピンSFN、6ピンTDFN-EP、6ピンTSOC

### 標準アプリケーション回路



DeepCoverおよび1-WireはMaxim Integrated Products, Inc.の登録商標です。

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/DS28E15.related](http://japan.maximintegrated.com/DS28E15.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](http://japan.maximintegrated.com))をご覧ください。

# DeepCoverセキュア認証用IC、1-Wire SHA-256 および512ビットユーザーEEPROM内蔵

### 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 (TDFN, TSOC only; soldering, 10s)..+300°C  
 Soldering Temperature (TDFN, TSOC only; reflow).....+260°C

**Note:** The SFN package is qualified for electro-mechanical contact applications only, not for soldering. For more information, refer to [Application Note 4132: Attachment Methods for the Electro-Mechanical SFN Package](#).

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

( $T_A = -40^\circ\text{C}$  to  $+85^\circ\text{C}$ , unless otherwise noted.) (Note 1)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
<b>IO PIN: GENERAL DATA</b>						
1-Wire Pullup Voltage	$V_{PUP}$	(Note 2)	2.97		3.63	V
1-Wire Pullup Resistance	$R_{PUP}$	$V_{PUP} = 3.3\text{V} \pm 10\%$ (Note 3)	300		1500	$\Omega$
Input Capacitance	$C_{IO}$	(Notes 4, 5)		1500		pF
Input Load Current	$I_L$	IO pin at $V_{PUP}$		5	19.5	$\mu\text{A}$
High-to-Low Switching Threshold	$V_{TL}$	(Notes 6, 7)		$0.65 \times V_{PUP}$		V
Input Low Voltage	$V_{IL}$	(Notes 2, 8)			0.3	V
Low-to-High Switching Threshold	$V_{TH}$	(Notes 6, 9)		$0.75 \times V_{PUP}$		V
Switching Hysteresis	$V_{HY}$	(Notes 6, 10)		0.3		V
Output Low Voltage	$V_{OL}$	$I_{OL} = 4\text{mA}$ (Note 11)			0.4	V
Recovery Time	$t_{REC}$	$R_{PUP} = 1500\Omega$ (Notes 2, 12)	5			$\mu\text{s}$
Time Slot Duration	$t_{SLOT}$	(Notes 2, 13)	13			$\mu\text{s}$
<b>IO PIN: 1-Wire RESET, PRESENCE-DETECT CYCLE</b>						
Reset Low Time	$t_{RSTL}$	(Note 2)	48		80	$\mu\text{s}$
Reset High Time	$t_{RSTH}$	(Note 14)	48			$\mu\text{s}$
Presence-Detect Sample Time	$t_{MSP}$	(Notes 2, 15)	8		10	$\mu\text{s}$
<b>IO PIN: 1-Wire WRITE</b>						
Write-Zero Low Time	$t_{W0L}$	(Notes 2, 16)	8		16	$\mu\text{s}$
Write-One Low Time	$t_{W1L}$	(Notes 2, 16)	1		2	$\mu\text{s}$
<b>IO PIN: 1-Wire READ</b>						
Read Low Time	$t_{RL}$	(Notes 2, 17)	1		$2 - \delta$	$\mu\text{s}$
Read Sample Time	$t_{MSR}$	(Notes 2, 17)	$t_{RL} + \delta$		2	$\mu\text{s}$

### DeepCoverセキュア認証用IC、1-Wire SHA-256 および512ビットユーザーEEPROM内蔵

#### ELECTRICAL CHARACTERISTICS (continued)

( $T_A = -40^{\circ}\text{C}$  to  $+85^{\circ}\text{C}$ , unless otherwise noted.) (Note 1)

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
<b>EEPROM</b>						
Programming Current	$I_{\text{PROG}}$	$V_{\text{PUP}} = 3.63\text{V}$ (Notes 5, 18)			1	mA
Programming Time for a 32-Bit Segment or Page Protection	$t_{\text{PRD}}$	<b>Refer to the full data sheet.</b>				ms
Programming Time for the Secret	$t_{\text{PRS}}$		ms			
Write/Erase Cycling Endurance	$N_{\text{CY}}$	$T_A = +85^{\circ}\text{C}$ (Notes 21, 22)	100k			—
Data Retention	$t_{\text{DR}}$	$T_A = +85^{\circ}\text{C}$ (Notes 23, 24, 25)	10			Years
<b>SHA-256 ENGINE</b>						
Computation Current	$I_{\text{CSHA}}$	<b>Refer to the full data sheet.</b>				mA
Computation Time	$t_{\text{CSHA}}$		ms			

- Note 1:** Limits are 100% production tested at  $T_A = +25^{\circ}\text{C}$  and/or  $T_A = +85^{\circ}\text{C}$ . 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  $V_{\text{PUP}}$  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:**  $V_{\text{TL}}$ ,  $V_{\text{TH}}$ , and  $V_{\text{HY}}$  are a function of the internal supply voltage, which is a function of  $V_{\text{PUP}}$ ,  $R_{\text{PUP}}$ , 1-Wire timing, and capacitive loading on IO. Lower  $V_{\text{PUP}}$ , higher  $R_{\text{PUP}}$ , shorter  $t_{\text{REC}}$ , and heavier capacitive loading all lead to lower values of  $V_{\text{TL}}$ ,  $V_{\text{TH}}$ , and  $V_{\text{HY}}$ .
- Note 7:** Voltage below which, during a falling edge on IO, a logic 0 is detected.
- Note 8:** The voltage on IO must be less than or equal to  $V_{\text{IL}(\text{MAX})}$  at all times the master is driving IO to a logic 0 level.
- Note 9:** Voltage above which, during a rising edge on IO, a logic 1 is detected.
- Note 10:** After  $V_{\text{TH}}$  is crossed during a rising edge on IO, the voltage on IO must drop by at least  $V_{\text{HY}}$  to be detected as logic 0.
- 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  $1/(t_{\text{WOL}(\text{MIN})} + t_{\text{REC}(\text{MIN})})$ .
- Note 14:** An additional reset or communication sequence cannot begin until the reset high time has expired.
- Note 15:** Interval after  $t_{\text{RSTL}}$  during which a bus master can read a logic 0 on IO if there is a DS28E15 present. The power-up presence detect pulse could be outside this interval but will be complete within 2ms after power-up.
- Note 16:**  $\epsilon$  in [Figure 11](#) represents the time required for the pullup circuitry to pull the voltage on IO up from  $V_{\text{IL}}$  to  $V_{\text{TH}}$ . The actual maximum duration for the master to pull the line low is  $t_{\text{W1L}(\text{MAX})} + t_{\text{F}} - \epsilon$  and  $t_{\text{W0L}(\text{MAX})} + t_{\text{F}} - \epsilon$ , respectively.
- Note 17:**  $\delta$  in [Figure 11](#) represents the time required for the pullup circuitry to pull the voltage on IO up from  $V_{\text{IL}}$  to the input-high threshold of the bus master. The actual maximum duration for the master to pull the line low is  $t_{\text{RL}(\text{MAX})} + t_{\text{F}}$ .
- Note 18:** Current drawn from IO during the EEPROM programming interval or SHA-256 computation. The pullup circuit on IO during the programming interval and SHA-256 computation should be such that the voltage at IO is greater than or equal to 2.0V.
- 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.

### DeepCoverセキュア認証用IC、1-Wire SHA-256 および512ビットユーザーEEPROM内蔵

#### ELECTRICAL CHARACTERISTICS (continued)

( $T_A = -40^{\circ}\text{C}$  to  $+85^{\circ}\text{C}$ , unless otherwise noted.) (Note 1)

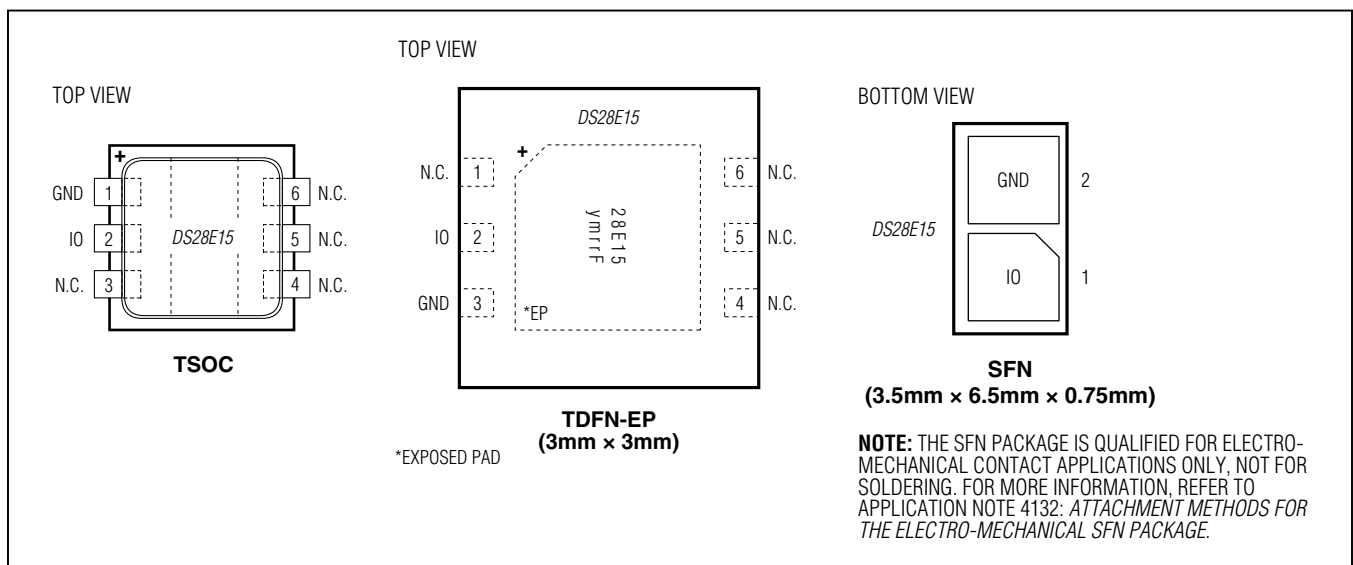
**Note 23:** Data retention is tested in compliance with JESD47G.

**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.

**Note 26:** Refer to the full data sheet.

#### ピン配置



#### 端子説明

SFN	端子		名称	機能
	TDFN-EP	TSOC		
—	1, 4, 5, 6	3-6	N.C.	接続されていません
1	2	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。
2	3	1	GND	グラウンド基準
—	—	—	EP	エクスポーズドパッド(TDFNのみ)。正しく動作させるため、基板のグラウンドプレーンに均等にはんだ付けします。詳細については、アプリケーションノート3273「Exposed Pads: A Brief Introduction」(英文)を参照してください。

# DeepCoverセキュア認証用IC、1-Wire SHA-256 および512ビットユーザー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/DS28E15](http://japan.maximintegrated.com/DS28E15)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
DS28E15G+	-40°C to +85°C	2 SFN
DS28E15G+T	-40°C to +85°C	2 SFN (2.5k pcs)
DS28E15Q+T	-40°C to +85°C	6 TDFN-EP* (2.5k pcs)
DS28E15P+	-40°C to +85°C	6 TSOC
DS28E15P+T	-40°C to +85°C	6 TSOC (4k 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 = エクスポートパッド

## 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](http://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に注意してください。

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.
2 SFN	T23A6N+1	<a href="#">21-0575</a>	—
6 TDFN-EP	T633+2	<a href="#">21-0137</a>	<a href="#">90-0058</a>
6 TSOC	D6+1	<a href="#">21-0382</a>	<a href="#">90-0321</a>



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

Maxim Integratedは完全にMaxim Integrated製品に組み込まれた回路以外の回路の使用について一切責任を負いかねます。回路特許ライセンスは明言されていません。Maxim Integratedは随時予告なく回路及び仕様を変更する権利を留保します。「Electrical Characteristics (電気的特性)」の表に示すパラメータ値(min、maxの各制限値)は、このデータシートの他の場所で引用している値より優先されます。

**Maxim Integrated 160 Rio Robles, San Jose, CA 95134 USA 1-408-601-1000**

42