DATA SHEET

SGT1001
CyberRock-Token

Version 1.0	January 2026

FEATURES

- Immutable token with unique hard-coded 256-bit identity
- HMAC symmetrical authentication using SHA256
- Authentication using centrally or locally generated challenges
- Optional generation of Ephemeral Key for encryption
- Built-in Self-Test for in-application testing
- GS1 SGTIN198 RFID-compatible ID
- SPI mode0 interface
- Wide supply operating range
- Standard deep sleep mode
- Low power consumption

APPLICATIONS

All connected systems requiring remote asset and/or configuration management

- Complex and high-tech equipment
- Smart sensor and lighting networks
- Infrastructure and utility networks

DESCRIPTION

The SGT1001 CyberRock-Token is a monolithic IC acting as a “digital bar code” and local Trust Anchor for any connected electronic device. On request the device reads back the unique, hard-coded, embedded identity. Because the device does not use a microcontroller and memory it is well protected against tampering.

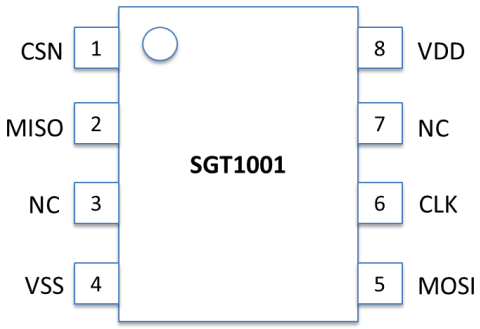
In combination with the SandGrain CyberRock-Cloud platform the device performs a symmetrical HMAC challenge/response authentication, which makes the solution post-quantum resilient (PQR) and robust to all known forms of hacking.

A standard SPI mode0 interface and single supply make it easy to apply in any controller-based end node. Because the device is mostly in deep sleep mode it has extremely low power consumption.

PINNING

SYMBOL	PIN	DESCRIPTION
CSN	1	SPI Chip Select Not
MISO	2	SPI Main In Sub Out Device data output
NC	3	Not connected
VSS	4	Negative supply voltage, Ground
MOSI	5	SPI Main Out Sub In Device data input
CLK	6	SPI Clock input
NC	7	Not connected
VDD	8	Positive supply voltage

PIN CONFIGURATION



Top view

PACKAGE INFORMATION	8-pin plastic Small Outline package SO8 Body dimension 3.8 x 4.9mm Pin spacing 1.27mm (0.05”)
DEVICE MARKING	SGB

LIMITING VALUES

Over operating free air temperature range.
Operating the device beyond these values may result in permanent damage.

SYMBOL	PARAMETER	MIN	MAX	UNIT
V_{DD}	Supply voltage		7.0	V
V_{pin}	Voltage on input ports	-0.5	V_{DD} +0.5	V
I_o	DC Output current		5	mA
T_{stg}	Storage temperature	-55	+150	°C
T_{amb}	Ambient operating temperature	-40	+125	°C
T_j	Junction temperature		+150	°C

ESD and HANDLING

		VALUE	UNIT
ESD Human Body Model (HBM)	following JS-001-2023	+/-2500	V
ESD Charge Device Model (CDM)	following JS-002-2022	+/-2000	V
Latch up	following JESD78	+/- 100	mA

CHARACTERISTICS

SYMBOL	PARAMETER	CONDITIONS	MIN	TYP	MAX	UNIT
SUPPLY (pin 8)						
V_{DD}	Operational supply voltage range	f ≤ 1 MHz	1.8		5.5	V
		1 < f ≤ 10 MHz	2.2		5.5	V
SPI INTERFACE (pin 1, 5, 6)						
V_{IH}	High-level input voltage		0.8*V_{DD}		V_{DD} +0.5	V
V_{IL}	Low-level input voltage		-0.5		0.2*V_{DD}	V
C_{IN}	Input capacitance	f=10MHz		2		pF
V_{OH}	High-level output voltage		V_{DD}-0.4		V_{DD}	V
V_{OL}	Low-level output voltage		0		0.4	V
T_{set}	Device settling time		1			Clock Cycles
T_{end}	Sequence end time		1			

Typical characteristics measured at T_A = 25°C, V_{DD} = 3.3V and MODE3 unless otherwise noted.

SYMBOL	PARAMETER	CONDITIONS	MIN	TYP	MAX	UNIT
SUPPLY (pin 8)						
I_{DD}	Supply current	CSN=Low, f=1MHz		1.1	3.5	mA
		CSN=Low, f=10MHz		3.5	8.0	mA
$I_{DD,Q}$	Quiescent current	CSN=High		1.0	5.0	nA
P_Q	Quiescent power consumption	CSN=High			16.5	nW
SPI INTERFACE (pin 1, 5, 6)						
f_{CLK}	Clock frequency	50% duty cycle			10	MHz

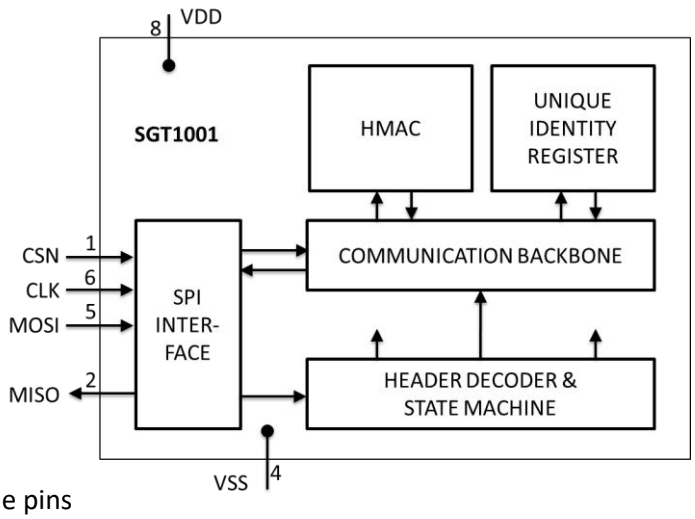
Typical characteristics measured at T_A = 25°C, V_{DD} = 5.0V and MODE3 unless otherwise noted.

SYMBOL	PARAMETER	CONDITIONS	MIN	TYP	MAX	UNIT
SUPPLY (pin 8)						
I_{DD}	Supply current	CSN=Low, f=1MHz		2.0	5.0	mA
		CSN=Low, f=10MHz		5.7	12.0	mA
$I_{DD,Q}$	Quiescent current	CSN=High		7.0	15.0	nA
P_Q	Quiescent power consumption	CSN=High			75.0	nW
SPI INTERFACE (pin 1, 5, 6)						
f_{CLK}	Clock frequency	50% duty cycle			10	MHz

Power considerations

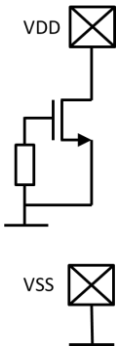
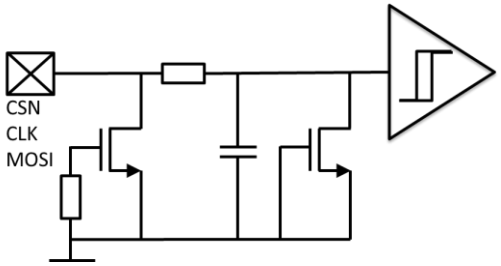
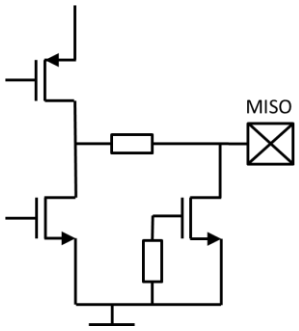
If minimum energy per authentication is required then we recommend using f=10Mhz at 1.8 V supply. The duration of the operating power consumption in mode 3 is 696 cycles or 70 us.
If minimum peak power is required, then use lower communication speeds.
As soon as CSN=High, quiescent current is consumed and alternatively the supply can also be removed completely in the application (without impacting start up times).

BLOCK DIAGRAM



Numbers refer to the pins

IO CHARACTERISTICS

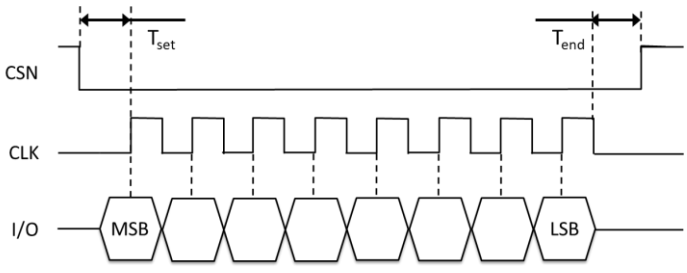
		
Power supply	SPI inputs	SPI output
		Z_{load} = 10pF//100kΩ

SPI BUS

The SPI bus is used in MODE0 as defined in the SPI standard.

PARAMETER	DEFINITION	SETTING
CPOL	Serial Clock polarisation	CPOL=0, CLK idle at Low level
CPHA	Serial Clock Phase	CPHA=0, sampling on CLK rising edge First data bit available immediately after CSN low
CSN	Chip Select Not	Chip select, goes Low to activate the SPI bus
MOSI	Main Out Sub In	Data input of the device, high-ohmic when not active
MISO	Main In Sub Out	Data output of the device, high-ohmic when not active
T_{set}	Setting time	At least one clock cycle
T_{end}	End-of-sequence time	At least one clock cycle

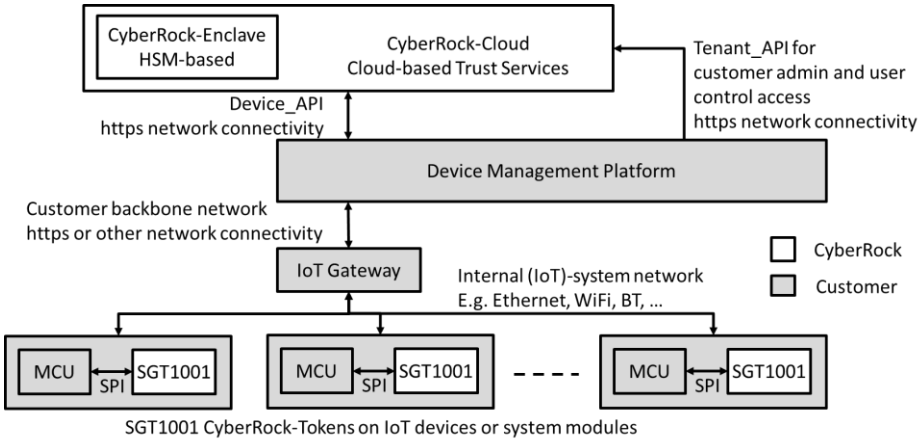
SPI MODE0 PROTOCOL



Dotted lines indicate the data sampling instances on the CLK rising edges

SYSTEM APPLICATION

TYPICAL SYSTEM SET-UP

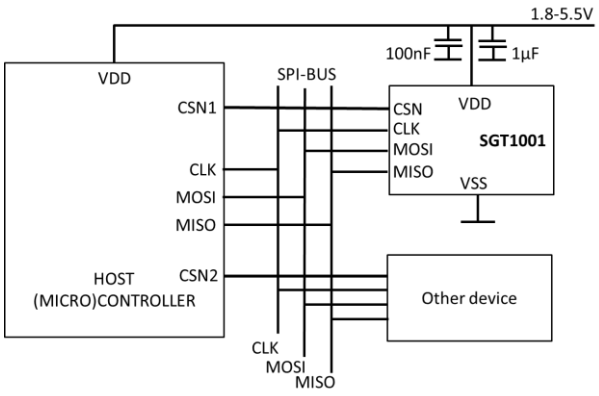


The SandGrain CyberRock system provides Trust Services out of the CyberRock-Cloud platform using two trust anchors:

1. The SGT1001 CyberRock-Token immutable hard-coded IC on the IoT devices and nodes
2. The CyberRock-Enclave HSM-based key vault.

The SGT1001 communicates through the SPI-bus with the local Microcontroller (MCU), the CyberRock-Cloud platform communicates using internet https connections through the two APIs. The picture above shows a typical network set-up and hierarchy.
All other communication and connections are customer defined and controlled and should take care that the required data going into the SGT1001 is properly delivered, while the output of the SGT1001 is sent to the appropriate destination.

TYPICAL CONNECTION TO CONTROLLER



The SGT1001 can be connected to a mode0 SPI-bus, with a dedicated CSN signal.

It is recommended that the SGT1001 uses the same power supply as the controller, under the condition that the VDD is between 2.2V and 5.5V for high-speed operation (clock frequency above 1MHz) and between 1.8V and 5.5V for low-speed operation (clock frequency 1MHz or below).

In case the controller and the SGT1001 use different supply voltages the SPI voltages and proper operation must be verified. If not, level shifters must be used between the two ICs.

Since the SGT1001 uses longer exchange sessions of up to 824 clock cycles, it must be verified that the SPI function of the controller supports these longer exchange sessions. Some controllers are limited to SPI exchanges of e.g. 256 clock cycles. In that case it is recommended to provide the CSN output of the controller through a GPIO port and not the standard MCU CSN port.

OPERATING MODES

MODE		HEADER	
		Binary (32 bits)	*Hex (8 digits)*
0	GS1 SGTIN-198	0000 0000 0000 0000 0000 0000 0000 0000	0x00000000
1	Token Identification	0000 0001 0000 0000 0000 0000 0000 0000	0x01000000
3	Token Authentication	0000 0011 0000 0000 0000 1000 0000 0000	0x03000800
5	Host Authentication	0000 0101 0000 0000 0000 1000 0000 0000	0x05000800
6	Host Authentication with Ephemeral Key	0000 0110 0000 0000 0000 1000 0000 0000	0x06000800
7	Token Authentication with Ephemeral Key	0000 0111 0000 0000 0000 1000 0000 0000	0x07000800
255	Built-in Self-Test	1111 1111 0000 0000 0000 0000 0000 0000	0xFF000000
2,4,8-254	Future use		

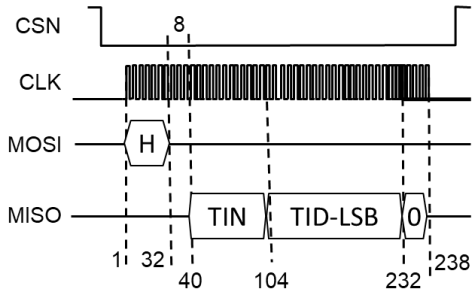
All headers sent MSB first left to right. Invalid headers result in mode 0 response.

ABBREVIATIONS

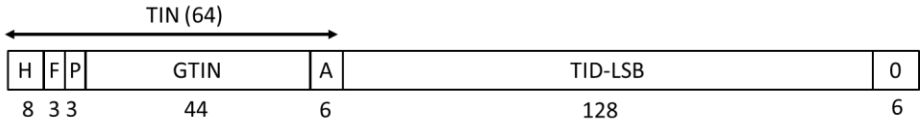
BEK	BIST Ephemeral Key
BIST	Built-in self-test
BRW	BIST Response Word
CLK	Clock
CW	Challenge Word
EK	Ephemeral Key
GS1-SGTIN	Global Standards One - Serialized Global Trade Item Number
H	Header
HCW	Host Challenge Word
HRW	Host Response Word
LSB	Least Significant Bit
MSB	Most Significant Bit
RW	Response Word
TID	Token Identity

Mode0 GS1 SGTIN-198 Identification

MODE0 DATA FORMAT AND SEQUENCE



SGTIN-198 FORMAT



Section		# bits	Value	Description
Header	H	8	0x36	Fixed per the standard
Filter value	F	3	111	Fixed per the standard
Partitioning	P	3	000	Part of SandGrain SGTIN code
GTIN	GTIN	44	0xCB0C4807FF0	Part of SandGrain SGTIN code
Pre-amble	A	6	011000	Part of the SandGrain SGTIN code
Total	TIN	64	0x36E32C31201FFC18	Full TIN code
Identity	TID-LSB	128	Unique per IC	The 128 LSB of the standard mode1 SandGrain Token ID
Empty	0	6	000000	Unused bits
Total		198		Total SGTIN-198 for token with TID

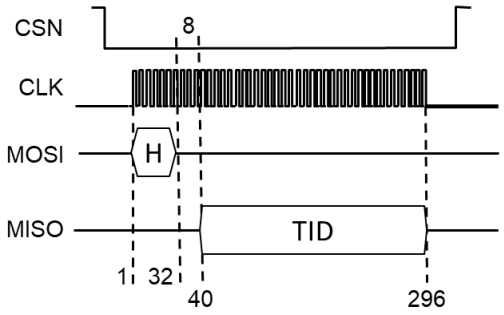
TIMING	PORT	ACTION
Start sequence	CSN	CSN low, wait T_{set}
At CLK 1	CLK	Start sending 238 CLK cycles
	MOSI	Start sending Mode0 Header (32 bits) MSB first
At CLK 40	MISO	Start receiving GS1 SGTIN198 header (58 bits) MSB first
At CLK 98	MISO	Start receiving chip Identity (128 bits) MSB first
After CLK 238	CLK	Stop sending CLK cycles, wait T_{end}
End sequence	CSN	CSN high, IC back to deep sleep mode

Remarks:

1. The Partitioning and GTIN parts of the SGTIN-198 code are a SandGrain-specific
2. The identity (TID-LSB) is a Sandgrain specific derivative

Mode1 Token Identification

MODE1 DATA FORMAT AND SEQUENCE



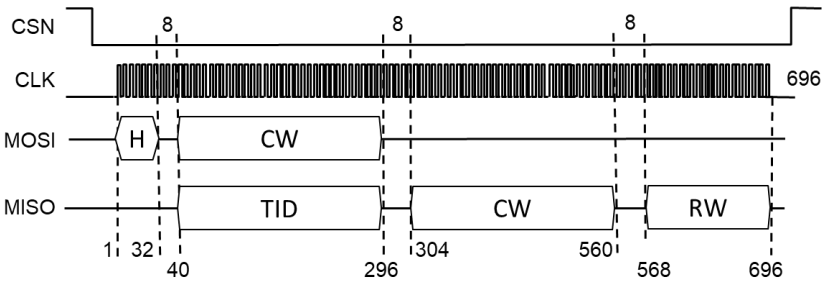
TIMING	PORT	ACTION
Start sequence	CSN	CSN low, wait T_{set}
At CLK 1	CLK	Start sending 296 CLK cycles
	MOSI	Start sending Mode1 Header (32 bits) MSB first
At CLK 40	MISO	Start receiving Token Identity (256 bits) MSB first
After CLK 296	CLK	Stop sending CLK cycles, wait T_{end}
End sequence	CSN	CSN high, IC back to deep sleep mode

Remark:

1. The Token Identity (TID) of every CyberRock-Token is globally unique, and hard coded into the IC during production. It cannot be modified.

Mode3 Token Authentication

MODE3 DATA FORMAT AND SEQUENCE



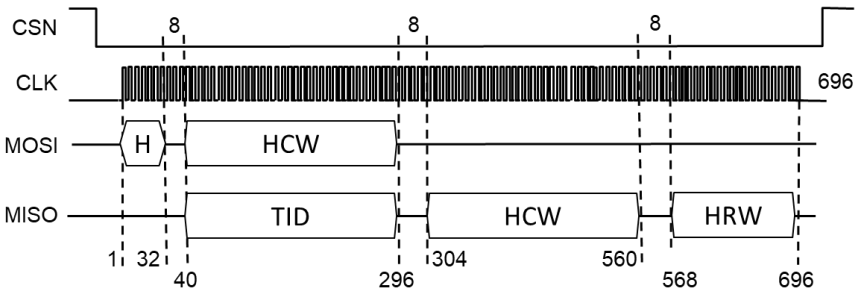
TIMING	PORT	ACTION
Start sequence	CSN	CSN low, wait T_{set}
At CLK 1	CLK	Start sending 696 CLK cycles
	MOSI	Start sending Mode3 Header (32 bits) MSB first
At CLK 40	MISO	Start receiving Token Identity (256 bits) MSB first
	MOSI	Start sending Challenge Word (256 bits) MSB first
At CLK 304	MISO	Start receiving Challenge Word (256 bits) MSB first
At CLK 568	MISO	Start receiving Response Word (128 bits) MSB first
After CLK 696	CLK	Stop sending CLK cycles, wait T_{end}
End sequence	CSN	CSN high, IC back to deep sleep mode

Remarks:

1. The Token Identity (TID) of every CyberRock-Token is globally unique, and hard coded into the IC during production. It cannot be modified.
2. In Mode3 (token authentication) the device uses the received Challenge Word (CW) as input to the HMAC authentication engine, delivering the Response Word (RW) as output.
3. The HMAC is compliant with FIPS198-1 and NIST SP800-107 and uses the SHA256 hash function compliant with FIPS180-4.
4. The output of the device, the data string TID-0-CW-0-RW contains all information for the authentication of the device with identity TID and the received CW.
5. 8-bit gaps in the output data stream are inserted for clear separation between the different output elements.

Mode5 Host Authentication using Host Challenge Word

MODE5 DATA FORMAT AND SEQUENCE



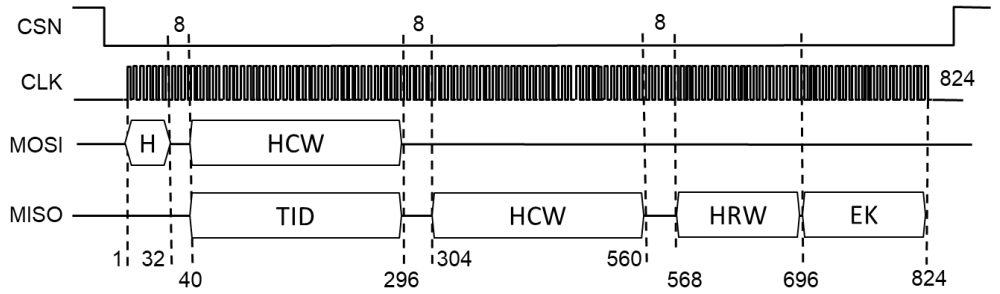
TIMING	PORT	ACTION
Start sequence	CSN	CSN low, wait T_{set}
At CLK 1	CLK	Start sending 696 CLK cycles
	MOSI	Start sending Mode5 Header (32 bits) MSB first
At CLK 40	MISO	Start receiving Token Identity (256 bits) MSB first
	MOSI	Start sending Host Challenge Word (256 bits) MSB first
At CLK 304	MISO	Start receiving Host Challenge Word (256 bits) MSB first
At CLK 568	MISO	Start receiving Host Response Word (128 bits) MSB first
After CLK 696	CLK	Stop sending CLK cycles, wait T_{end}
End sequence	CSN	CSN high, IC back to deep sleep mode

Remarks:

1. The Token Identity (TID) of every CyberRock-Token is globally unique, and hard coded into the IC during production. It cannot be modified.
2. In Mode5 (host authentication) the device uses a Host Challenge Word (HCW) as input to the HMAC authentication engine, delivering the Host Response Word (HRW) as output.
3. The HMAC is compliant with FIPS198-1 and NIST SP800-107 and uses the SHA256 hash function compliant with FIPS180-4.
4. The output of the device, the data string TID-0-HCW-0-HRW contains all information for the authentication of the device with identity TID and the HCW.
5. 8-bit gaps in the output data stream are inserted for clear separation between the different output elements.

Mode6 Host Authentication with Ephemeral Key

MODE6 DATA FORMAT AND SEQUENCE



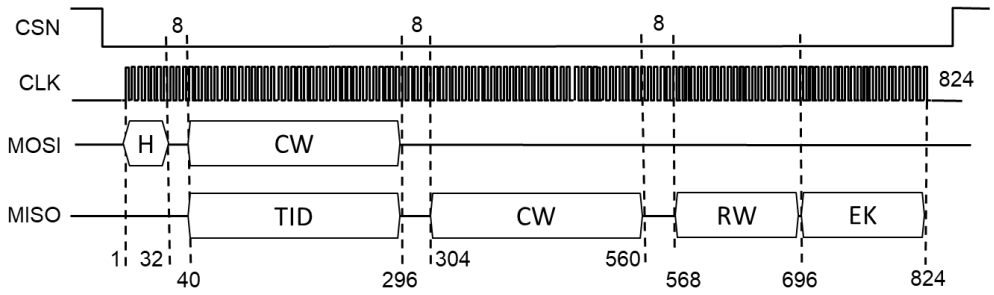
TIMING	PORT	ACTION
Start sequence	CSN	CSN low, wait T_{set}
At CLK 1	CLK	Start sending 824 CLK cycles
	MOSI	Start sending Mode6 Header (32 bits) MSB first
At CLK 40	MISO	Start receiving Token Identity (256 bits) MSB first
	MOSI	Start sending Host Challenge Word (256 bits) MSB first
At CLK 304	MISO	Start receiving Host Challenge Word (256 bits) MSB first
At CLK 568	MISO	Start receiving Host Response Word (128 bits) MSB first
At CLK 696	MISO	Start receiving Ephemeral Key (128 bits) MSB first
After CLK 824	CLK	Stop sending CLK cycles, wait T_{end}
End sequence	CSN	CSN high, IC back to deep sleep mode

Remarks:

1. The Token Identity (TID) of every CyberRock-Token is globally unique, and hard coded into the IC during production. It cannot be modified.
2. In Mode6 (host authentication with Ephemeral Key generation) the device uses a Host Challenge Word (HCW) as input to the HMAC authentication engine, delivering the Host Response Word (HRW) as output.
3. After sending the HRW the IC continues with sending a unique Ephemeral Key (EK). Given the TID and a unique HCW the EK is always unique. The EK will also be generated in CyberRock-Cloud.
4. The HMAC is compliant with FIPS198-1 and NIST SP800-107 and uses the SHA256 hash function compliant with FIPS180-4.
5. The output of the device, the data string TID-0-HCW-0-HRW-EK contains all information for the authentication of the device with identity TID and the HCW.
6. 8-bit gaps in the output data stream have been inserted for clear separation between the different output elements.

Mode7 Token Authentication with Ephemeral Key

MODE7 DATA FORMAT AND SEQUENCE



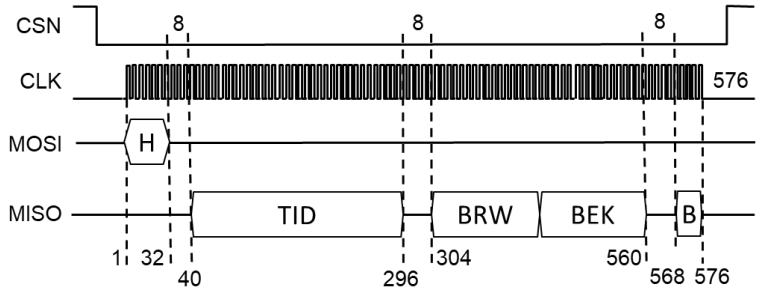
TIMING	PORT	ACTION
Start sequence	CSN	CSN low, wait T_{set}
At CLK 1	CLK	Start sending 824 CLK cycles
	MOSI	Start sending Mode7 Header (32 bits) MSB first
At CLK 40	MISO	Start receiving Token Identity (256 bits) MSB first
	MOSI	Start sending Challenge Word (256 bits) MSB first
At CLK 304	MISO	Start receiving Challenge Word (256 bits) MSB first
At CLK 568	MISO	Start receiving Response Word (128 bits) MSB first
At CLK 696	MISO	Start receiving Ephemeral Key (128 bits) MSB first
After CLK 824	CLK	Stop sending CLK cycles, wait T_{end}
End sequence	CSN	CSN high, IC back to deep sleep mode

Remarks:

1. The Token Identity (TID) of every CyberRock-Token is globally unique, and hard coded into the IC during production. It cannot be modified.
2. In Mode7 (authentication with Ephemeral Key generation) the device uses the received Challenge Word (CW) as input to the HMAC authentication engine, delivering the Response Word (RW) as output.
3. After sending the RW the IC continues with sending a unique Ephemeral Key (EK). Given the TID and a unique CW the EK is always unique. The EK will also be generated in CyberRock-Cloud.
4. The HMAC is compliant with FIPS198-1 and NIST SP800-107 and uses the SHA256 hash function compliant with FIPS180-4.
5. The output of the device, the data string TID-0-CW-0-RW-EK contains all information for the authentication of the device with identity TID and the CW.
6. 8-bit gaps in the output data stream have been inserted for clear separation between the different output elements.

Mode255 Built-In Self-Test (BIST)

MODE255 DATA FORMAT AND SEQUENCE



BIST Output B		DEFINITION
Binary (8 bits)	*Hex (1 byte)*	
0101 0000	0x50	Pass, Zero errors, BIST 100% successful
0111 0000	0x70	Fail, Errors

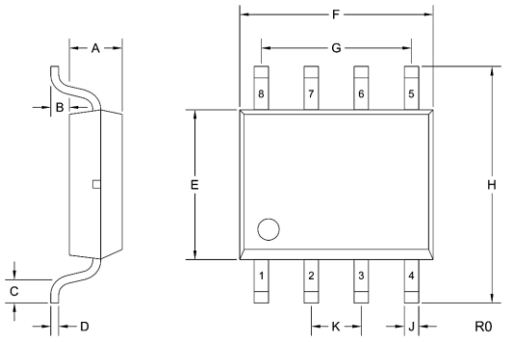
TIMING	PORT	ACTION
Start sequence	CSN	CSN low, wait T_{set}
At CLK 1	CLK	Start sending 576 CLK cycles
	MOSI	Start sending Mode255 Header (32 bits) MSB first
At CLK 40	MISO	Start receiving Token Identity (256 bits) MSB first
At CLK 304	MISO	Start receiving BRW and BEK (256 bits) MSB first
At CLK 568	MISO	Start receiving BIST Result Block B (8 bits) MSB first
After CLK 576	CLK	Stop sending CLK cycles, wait T_{end}
End sequence	CSN	CSN high, IC back to deep sleep mode

Remarks:

1. In BIST Mode255 the device provides BIST pass/fail result as well as extra test data. The BIST data consists of three blocks:
    a. BRW (128 bits) is the BIST-RW using the TID as CW (mode3)
    b. BEK (128 bits) is the BIST-EK using the bit-inverted TID as HCW (mode6)
    c. B (8 bits) which is 0X50 in case of PASS result
2. During BIST processing the device will use the internally stored unique TID of the device as CW for the HMAC authentication. The BIST data output (BRW+BEK) is therefore unique for every device.
3. The BIST will be used in production for device testing but can also be used with the device in its application. A check can be performed by reading the BIST result at any desired moment. A more extensive check can verify the received BRW and BEK using two additional Mode3 and Mode6 calls as explained in remark 1.

PACKAGING INFORMATION

PACKAGE DRAWING



DIMENSIONS				
	INCHES		MILLIMETERS	
SYMBOL	MIN	MAX	MIN	MAX
A	0.049	0.057	1.24	1.44
B	0.000	0.011	0.00	0.27
C	0.018	-	0.46	-
D	0.006	0.011	0.16	0.27
E	0.145	0.154	3.70	3.90
F	0.189	0.198	4.81	5.01
G	0.150		3.81	
H	0.231	0.244	5.88	6.18
J	0.013	0.021	0.35	0.52
K	0.050		1.27	

SOIC-8 (REV: R0)

SYMBOL	PARAMETER	MAX	UNIT
$R_{th,jc}$	Thermal resistance junction-to-case	52	°C/W
$R_{th,ja}$	Thermal resistance junction-to-ambient	204	°C/W

REVISION HISTORY

Release version	Date	Content, changes	Status
1.0	January 2026	SGT1001 first release	Released

CONTACT INFORMATION

Application support
SandGrain B.V.
High Tech Campus 9
5656 AE Eindhoven
The Netherlands
support@sandgrain.eu

Ordering
Sandgrain B.V.
High Tech Campus 9
5656 AE Eindhoven
The Netherlands
info@sandgrain.eu

Legal Disclaimer

No warranty

The information contained in this document is provided by SandGrain for general information purposes only and shall not be construed as a guarantee of any conditions, characteristics, or performance. SandGrain makes no representations or warranties, whether express or implied, including but not limited to warranties of accuracy, completeness, fitness for a particular purpose, or non-infringement of third-party intellectual property rights.

General terms and conditions

The general terms and conditions of sale of SandGrain ("Terms") apply to this datasheet and all products and services of SandGrain. The Terms can be downloaded here. By using and or accessing this document the user accepts the applicability of the Terms.

Limitation of liability

To the maximum extent permitted by applicable law, SandGrain shall not be liable for any indirect, incidental, special, punitive, or consequential damages, including without limitation loss of profits, business interruption, loss of data, or costs related to removal, replacement, or rework of products, arising out of or in connection with the use of this document or the products described herein. The additional terms regarding limitation of liability as set out in the Terms apply as well.

Intellectual property rights

All intellectual property rights, including but not limited to copyrights, trademarks, trade names, database rights, design rights, patents, know-how and any other proprietary rights, whether registered or unregistered, in and to this document and its contents are expressly reserved and shall remain vested exclusively in SandGrain. Nothing in this document shall be construed as granting, by implication, estoppel or otherwise, any license or right to use, reproduce, distribute or otherwise exploit any intellectual property rights, except as expressly permitted in writing by SandGrain. This document and all information contained herein are strictly confidential. Without the prior written consent of SandGrain, no part of this document may be disclosed, published, reproduced, duplicated, distributed, transmitted, made available to third parties, or otherwise used, in whole or in part, in any form or by any means, whether electronic, mechanical, photocopying, recording or otherwise. Any unauthorized use, disclosure or duplication of this document may result in civil and/or criminal liability and shall entitle SandGrain to seek injunctive relief, damages and any other remedies available under applicable law.

Changes and applications

SandGrain reserves the right to make changes to this document and the products described herein at any time without prior notice. Any applications, examples, or typical values are provided for illustrative purposes only and do not constitute a commitment or guarantee of suitability for any specific use.
Customers are solely responsible for the design, testing, and validation of their applications and for determining the suitability of SandGrain products for their intended use.

Life-support and safety-critical use

SandGrain products are not designed, authorized, or intended for use in life-support, life-critical, or safety-critical systems or applications. Use in such applications is prohibited unless expressly approved in writing by SandGrain.

Export control

This document and the products described herein may be subject to export control regulations. Export or transfer may require prior authorization from the competent authorities.