



DATA SHEET

PRELIMINARY 0.1

SGT1001

CyberRock-Token

Version 0.7

October 2025



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

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 cannot be tampered with.

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	PIN CONFIGURATION	
CSN	1	SPI Chip Select Not	CSN	1
MISO	2	SPI Main In Sub Out Device data output	MISO	2
NC	3	Not connected	NC	3
VSS	4	Negative supply voltage, Ground	VSS	4
MOSI	5	SPI Main Out Sub In Device data input	SGT1001	
CLK	6	SPI Clock input	8	VDD
NC	7	Not connected	7	NC
VDD	8	Positive supply voltage	6	CLK
PACKAGE INFORMATION			5 MOSI	
DEVICE MARKING			Top view	
			8-pin plastic Small Outline package SO8 Body dimension 3.8 x 4.9mm Pin spacing 1.27mm (0.005")	
			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	+/-2000	V
ESD Charge Device Model (CDM) following JS-002-2022	+/-500	V

CHARACTERISTICS

SYMBOL	PARAMETER	CONDITIONS	MIN	TYP	MAX	UNIT
SUPPLY (pin 8)						
V_{DD}	Operational supply voltage range	f=1MHz	1.8		5.5	V
		f=10MHz	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 $T_A = 25^\circ\text{C}$, $V_{DD} = 3.3\text{V}$ and MODE3 unless otherwise noted.

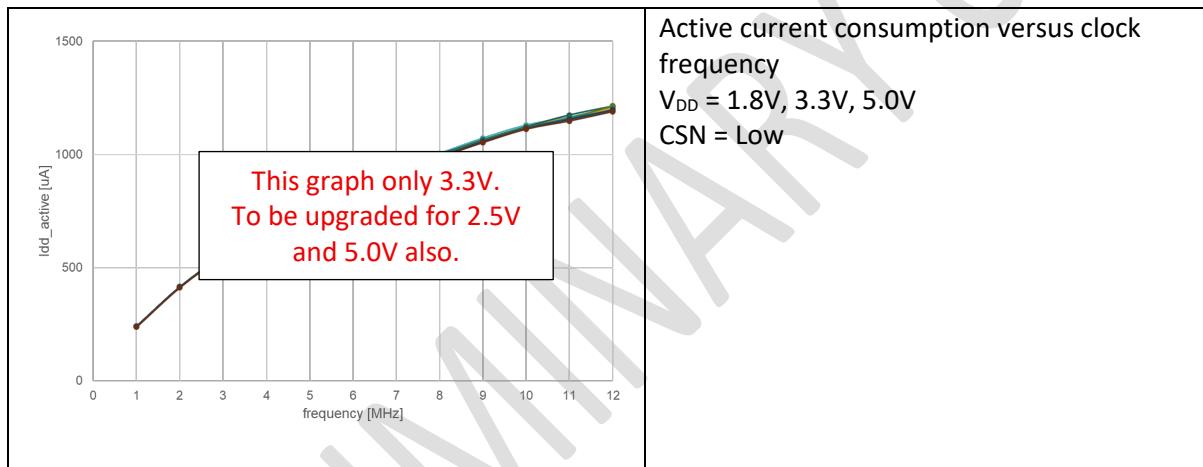
SYMBOL	PARAMETER	CONDITIONS	MIN	TYP	MAX	UNIT
SUPPLY (pin 8)						
I_{DD}	Supply current	CSN=Low, f=1MHz			5.0	mA
		CSN=Low, f=10MHz		2.5	5.0	mA
$I_{DD,Q}$	Quiescent current	CSN=High		1	5	nA
P_Q	Quiescent power consumption	CSN=High			20	nW
SPI INTERFACE (pin 1, 5, 6)						
f_{CLK}	Clock frequency	50% duty cycle			10	MHz
$I_{I/O}$	I/O current				100	μA



Typical characteristics measured at $T_A = 25^\circ\text{C}$, $V_{DD} = 5\text{V}$ and MODE3 unless otherwise noted.

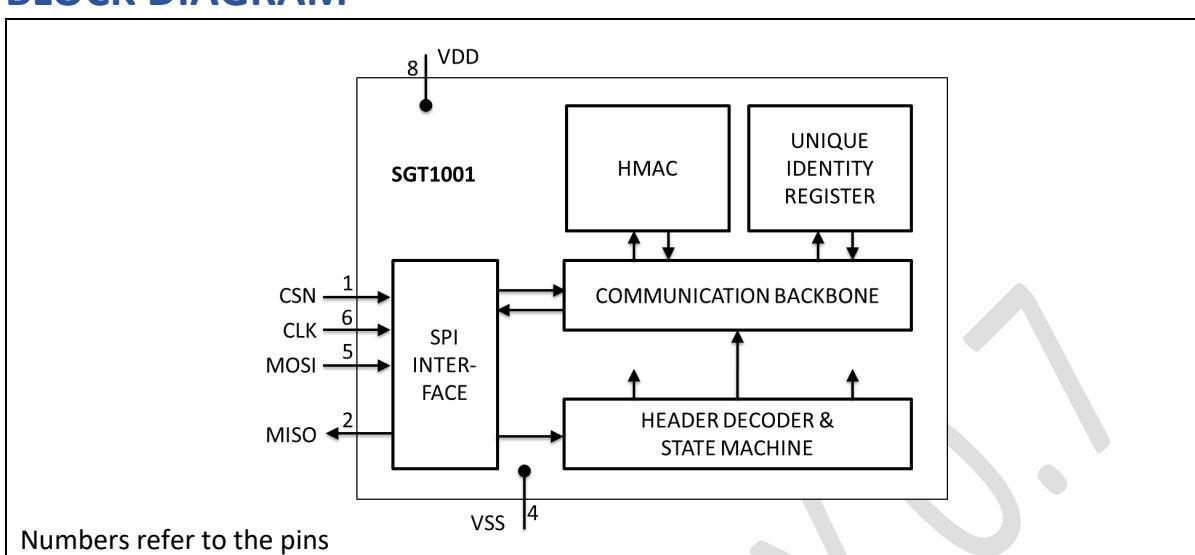
SYMBOL	PARAMETER	CONDITIONS	MIN	TYP	MAX	UNIT
SUPPLY (pin 8)						
I_{DD}	Supply current	CSN=Low, $f=1\text{MHz}$			7.0	mA
		CSN=Low, $f=10\text{MHz}$		3.5	7.0	mA
$I_{DD,Q}$	Quiescent current	CSN=High		10	20	nA
P_Q	Quiescent power consumption	CSN=High			100	nW
SPI INTERFACE (pin 1, 5, 6)						
f_{CLK}	Clock frequency	50% duty cycle			10	MHz
$I_{I/O}$	I/O current				100	μA

TYPICAL PERFORMANCE

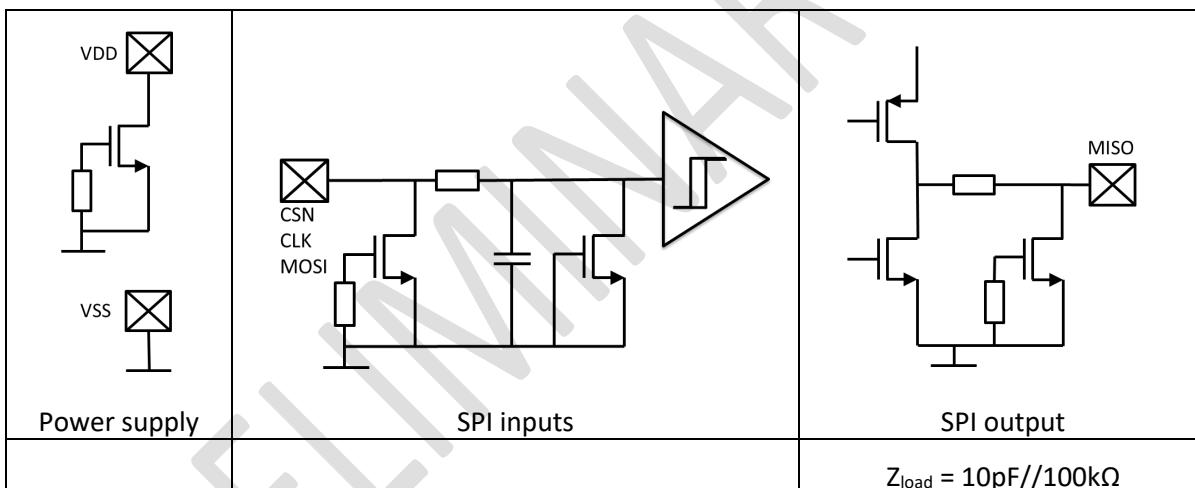




BLOCK DIAGRAM



IO CHARACTERISTICS



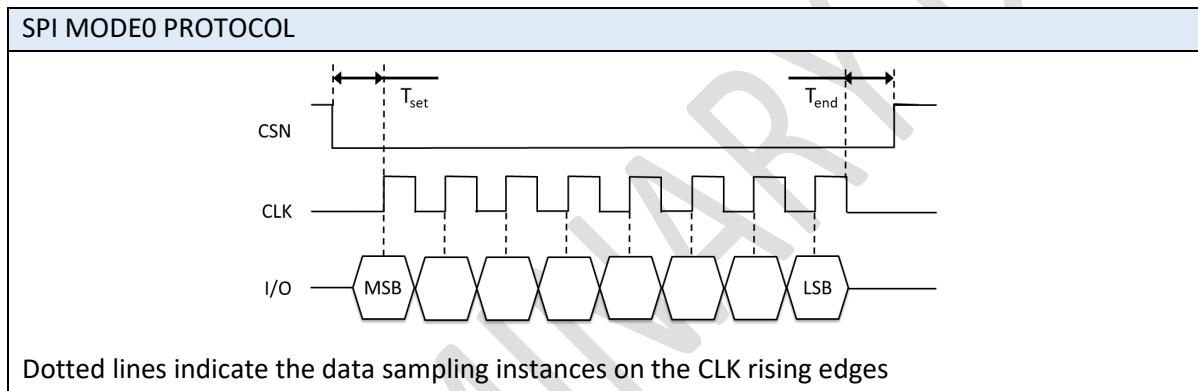


DATA STRUCTURE

SPI BUS

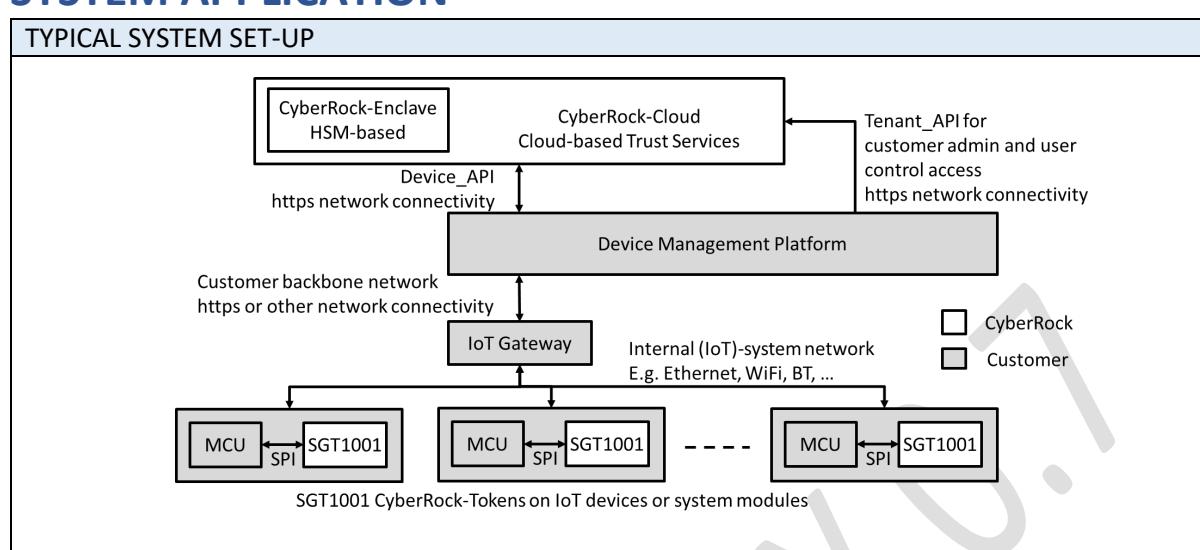
The SPI bus is used in MODE0 as defined in the SPI standard.

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





SYSTEM APPLICATION

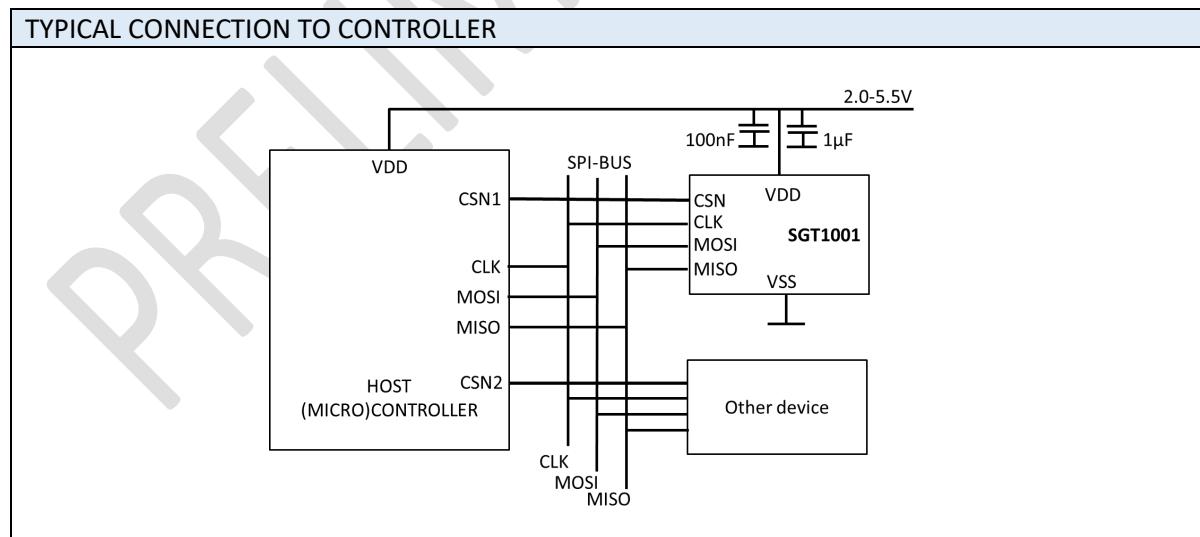


The SandGrain CyberRock system provides Trust Services out of the CyberRock-Cloud platform using two trust anchors:

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.



The SGT1001 can be connected to a mode0 SPI-bus, all that is needed is a free CSN port. In the absence of a bus, the SGT1001 can be connected directly to the (micro)controller SPI ports.



It is recommended that the SGT1001 uses the same power supply as the controller, under the condition that the VDD is between 2.0 and 5.0V for high-speed operation (clock frequency above 1MHz) and between 1.8V and 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, properly matched level shifters must be used between the two ICs.

Since the SGT1001 uses longer exchange sessions of up to 800 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	
		<i>Binary (32 bits)</i>	<i>Hex (8 digits)</i>
0,2,4, 8-254	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

All headers sent MSB first left to right.

ABBREVIATIONS

TID =	Token Identity
H =	Header
CW =	Challenge Word
HCW =	Host Challenge Word
RW =	Response Word
HRW =	Host Response Word
EK =	Ephemeral Key
BIST =	Built-in self-test
BRW =	BIST Response Word
BEK =	BIST Ephemeral Key
CLK =	Clock
LSB =	Least Significant Bit
MSB =	Most Significant Bit

GS1-SGTIN = Global Standards One - Serialized Global Trade Item Number



Mode0 GS1 SGTIN-198 Identification

MODE0 DATA FORMAT AND SEQUENCE				
CSN	8			
SGTIN-198 FORMAT				
TIN (64)				
H F P	GTIN	A	TID-LSB	0
8 3 3	44	6	128	6
Section	# bits	Code	Description	
Header	H	8	0x36	
Filter value	F	3	111	
Partitioning	P	3	000	
GTIN	GTIN	44	0xCB0C4807FF0	
Pre-amble	A	6	011000	
Total	TIN	64	0x36E32C31201FFC18	
Identity	TID-LSB	128	Unique per IC	
Empty	0	6	000000	
Total		198	Total SGTIN-198 for token with TID	

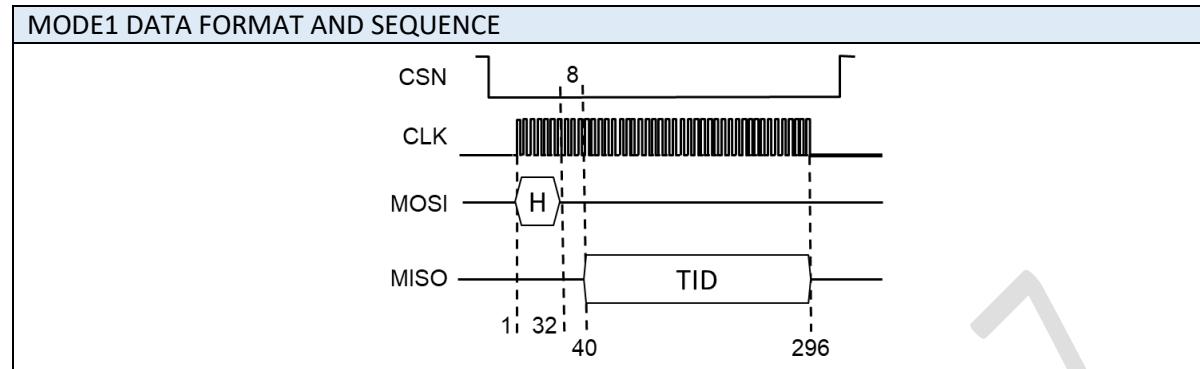
TIMING	PORT	ACTION
Start sequence	CSN	CSN low, wait T_{set}
At CLK 1	CLK	Start sending 238 CLK cycles
	MOSI	Start sending Mode0 Header (32 bits) MSB first
At CLK 40	MISO	Start receiving GS1 SGTIN198 header (58 bits) MSB first
At CLK 98	MISO	Start receiving chip Identity (128 bits) MSB first
After CLK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

Remarks:

- The Partitioning and GTIN parts of the SGTIN-198 code are SandGrain-specific
- The formal SGTIN header is mode0. However, any non-allocated header will also output the mode0 SGTIN code and identity.



Mode1 Token Identification



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

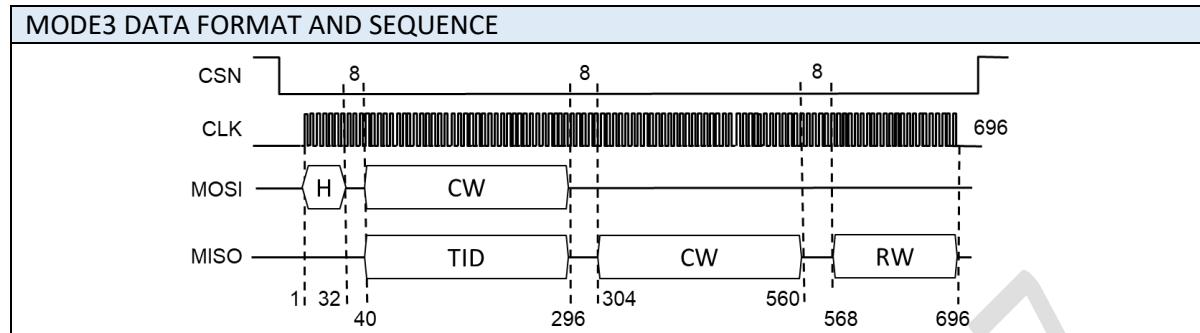
Remark:

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

PRELIMINARY



Mode3 Token Authentication



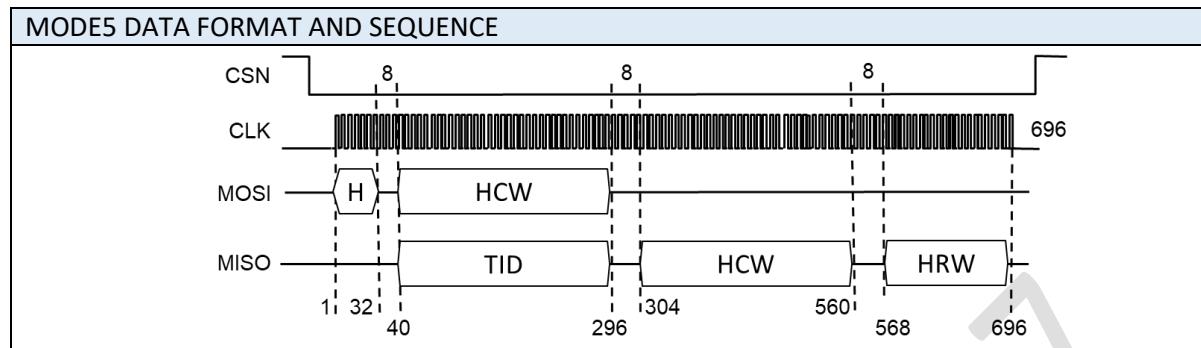
TIMING	PORT	ACTION
Start sequence	CSN	CSN low, wait T_{set}
At CLK 1	CLK	Start sending 296 CLK cycles
	MOSI	Start sending Mode3 Header (32 bits) MSB first
At CLK 40	MISO	Start receiving Token Identity (256 bits) MSB first
	MOSI	Start sending Challenge Word (256 bits) MSB first
At CLK 304	MISO	Start receiving 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. This data string should be sent to the SandGrain CyberRock-Cloud service for symmetrical authentication.
5. 8-bit gaps in the output data stream are inserted for clear separation between the different output elements.
6. Mode3 authentication only works in combination with the activated CyberRock-Cloud symmetrical functionality service.



Mode5 Host Authentication



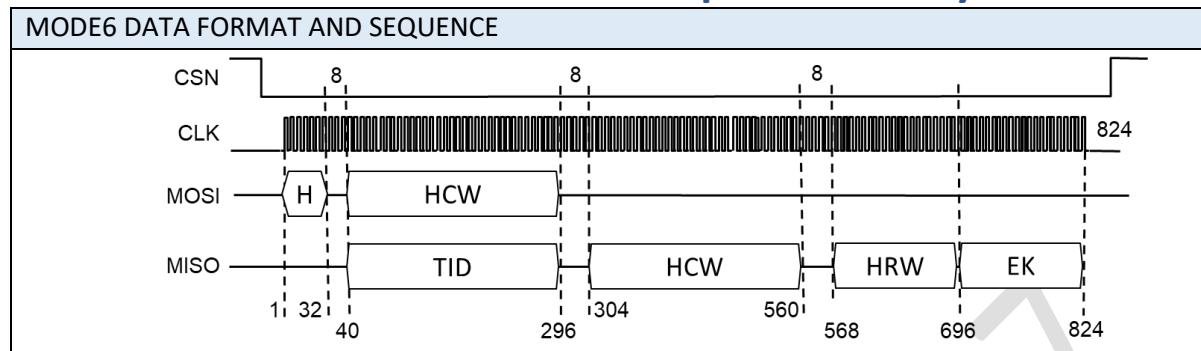
TIMING	PORT	ACTION
Start sequence	CSN	CSN low, wait T_{set}
At CLK 1	CLK	Start sending 296 CLK cycles
	MOSI	Start sending Mode5 Header (32 bits) MSB first
At CLK 40	MISO	Start receiving Token Identity (256 bits) MSB first
	MOSI	Start sending Host Challenge Word (256 bits) MSB first
At CLK 304	MISO	Start 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 locally generated 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. This data string should be used for symmetrical authentication.
5. 8-bit gaps in the output data stream are inserted for clear separation between the different output elements.
6. Mode5 host authentication only works in combination with the activated CyberRock-Cloud symmetrical functionality service.



Mode6 Host Authentication with Ephemeral Key



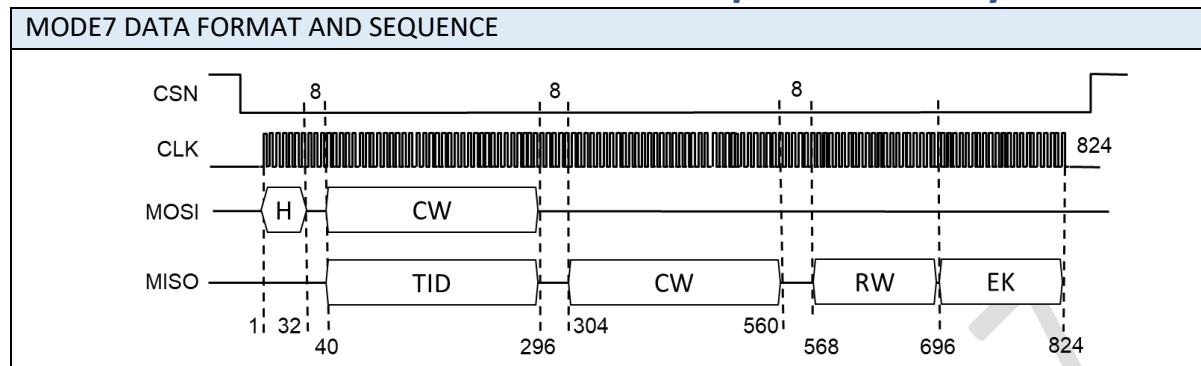
TIMING	PORT	ACTION
Start sequence	CSN	CSN low, wait T_{set}
At CLK 1	CLK	Start sending 296 CLK cycles
	MOSI	Start sending Mode6 Header (32 bits) MSB first
At CLK 40	MISO	Start receiving Token Identity (256 bits) MSB first
	MOSI	Start sending Host Challenge Word (256 bits) MSB first
At CLK 304	MISO	Start 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 locally generated 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. This data string minus the EK should be used for symmetrical authentication. The EK can be used locally in the device, for example for encryption. The EK will also be computed in the CyberRock-Cloud and can be sent to the destination for decryption.
6. 8-bit gaps in the output data stream have been inserted for clear separation between the different output elements.
7. Mode6 host authentication with EK generation only works in combination with the activated CyberRock-Cloud symmetrical functionality service.



Mode7 Token Authentication with Ephemeral Key



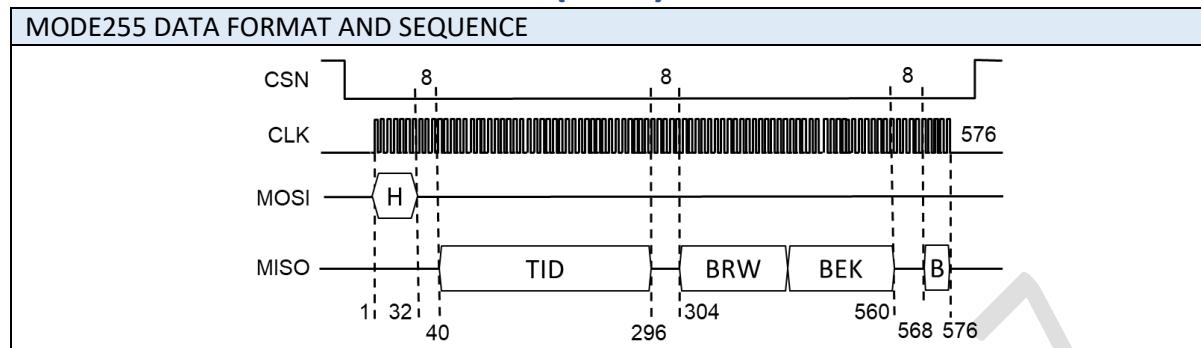
TIMING	PORT	ACTION
Start sequence	CSN	CSN low, wait T_{set}
At CLK 1	CLK	Start sending 296 CLK cycles
	MOSI	Start sending Mode7 Header (32 bits) MSB first
At CLK 40	MISO	Start receiving Token Identity (256 bits) MSB first
	MOSI	Start sending Challenge Word (256 bits) MSB first
At CLK 304	MISO	Start receiving 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. This data string minus the EK should be sent to the SandGrain CyberRock-Cloud service for symmetrical authentication. The EK can be used locally in the device, for example for encryption. The EK will also be computed in the CyberRock-Cloud and can be sent to the destination for decryption.
6. 8-bit gaps in the output data stream have been inserted for clear separation between the different output elements.
7. Mode7 authentication with EK generation only works in combination with the activated CyberRock-Cloud symmetrical functionality.



Mode255 Built-In Self-Test (BIST)



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 296 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:

- Where the device normally delivers a 128-bit Response Word (RW) in Mode3, in BIST Mode255 it provides a string BIST data of 256 bits for higher testing accuracy. The BIST data consists of two blocks:
 - BRW (128 bits) is the BIST-RW using the TID as CW (mode3)
 - BEK (128 bits) is the BIST-EK using the bit-inverted TID as HCW (mode6)
- 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.
- The BIST will be used in production for device testing but can also be used with the device in its application. When the BIST data output is stored in the device controller the BIST can be run at any desired moment. A quick check can be performed by ignoring the BIST data and just reading the BIST digit. A more extensive check can verify the received BRW and BEK using two additional Mode3 and Mode6 calls as explained in remark 1.



CyberRock-Token: Immutable IoT end node authentication IC

PACKAGING INFORMATION

PACKAGE DRAWING																																																																
					<table border="1"><thead><tr><th rowspan="2">SYMBOL</th><th colspan="4">DIMENSIONS</th></tr><tr><th>INCHES</th><th>MIN</th><th>MAX</th><th>MMILLIMETERS</th></tr></thead><tbody><tr><td>A</td><td>0.049</td><td>0.057</td><td>1.24</td><td>1.44</td></tr><tr><td>B</td><td>0.000</td><td>0.011</td><td>0.00</td><td>0.27</td></tr><tr><td>C</td><td>0.018</td><td>-</td><td>0.46</td><td>-</td></tr><tr><td>D</td><td>0.006</td><td>0.011</td><td>0.16</td><td>0.27</td></tr><tr><td>E</td><td>0.145</td><td>0.154</td><td>3.70</td><td>3.90</td></tr><tr><td>F</td><td>0.189</td><td>0.198</td><td>4.81</td><td>5.01</td></tr><tr><td>G</td><td></td><td>0.150</td><td></td><td>3.81</td></tr><tr><td>H</td><td>0.231</td><td>0.244</td><td>5.88</td><td>6.18</td></tr><tr><td>J</td><td>0.013</td><td>0.021</td><td>0.35</td><td>0.52</td></tr><tr><td>K</td><td></td><td>0.050</td><td></td><td>1.27</td></tr></tbody></table> <p>SOIC-8 (REV: R0)</p>	SYMBOL	DIMENSIONS				INCHES	MIN	MAX	MMILLIMETERS	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
SYMBOL	DIMENSIONS																																																															
	INCHES	MIN	MAX	MMILLIMETERS																																																												
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																																																												

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

Orderable Device	Status	Package Type	Product Marking	Package Quantity	Packaging Type
SGT1001	Design	SO8	SGB	-	-



REVISION HISTORY

Release version	Date	Content, changes	Status
0.1	February 2024	First version based on measured SandGrainA engineering samples	Preliminary
0.2	August 2024	Extended with 5V operation, SGTIN, FGCW and EK modes, ESD tests updated.	Preliminary
0.3	March 2025	Power supply specs, IO circuits, small additions & corrections.	Preliminary, based on design verification.
0.4	June 2025	Updated naming convention, small additions & corrections.	Preliminary
0.7	October 2025	Updated naming convention of CyberRock-Cloud Release 1.7, small additions & corrections.	Preliminary

NOTE

Please be aware that the SandGrainA Engineering Samples, marked SGA, and the SandGrainB Engineering Samples, marked SGB, have different functionality. SGA samples therefore do not exhibit all functionality as described in this Data Sheet v0.7. For SGA samples Data Sheet v0.1b should be used. For the common functions SGB samples are backward compatible with the SGA except for the BIST.

CONTACT INFORMATION

SandGrain application support

SandGrain B.V.

High Tech Campus 9

5656 AE Eindhoven

The Netherlands

productsupport@sandgrain.eu

PRELIMINARY