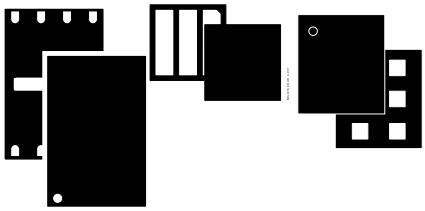
STSAFE-L010

Datasheet

Authentication, security for consumables and peripherals



UFDFPN8 XDFN3 X2F-PSON6

Product status
STSAFE-L010

Features

- Authentication of consumables and peripherals
- Usage monitoring with secure counters
- Nonvolatile memory zones with user-defined access rights

Security features

- Secure system solution
  - Secure *MCU*
  - Secure STSAFE-L010 operating system for authentication and data management
  - Unique serial number on each die
  - Monitoring of environmental parameters
  - Protection mechanism against faults
  - Protection against side-channel attacks
- Advanced asymmetric cryptography
  - Advanced asymmetric cryptography relying on *ECC* with 256 bits key length (Edwards curves Ed25519)

Hardware features

- 32 Kbytes of secure nonvolatile memory
  - Flash memory
  - 10 years data retention at 25°C
  - 100 000 erase/program cycles endurance at 25°C
- Supply voltage
  - 1.62 V to 5.5 V
- Operating temperature:
  - −25°C to 85°C

Protocol

- ST1Wire communication interface on one I/O
  - Up to 100 kbps communication speed
- *I²C* communication interface
  - Up to 100 kHz communication speed
  - 7-bit addressing mode

Packages

- ECOPACK-compliant UFDFPN 8-lead ultrathin profile fine pitch dual flat packages
- X2F-PSON6 package (under commercial conditions)
- XDFN3 package for direct contact (under commercial conditions)

1 Description

The STSAFE-L010 system-on-chip is a secure element providing authentication and data management services to a local host.

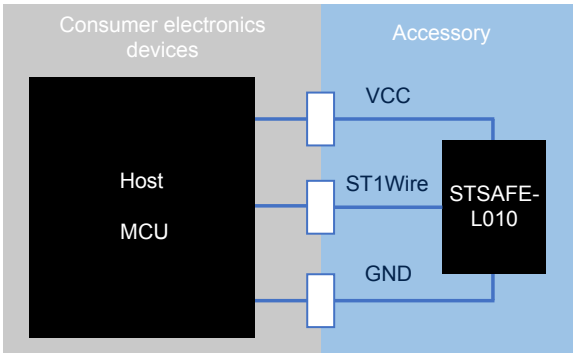
The primary function of the STSAFE-L010 is to allow the peripheral or consumable to which it is attached to be authenticated by a host for the latter to discriminate between wanted and unwanted peripheral or consumable.

The STSAFE-L010 authentication is performed by generating a digital signature over a challenge sent by the host (traceability data or zone data can be added to the challenge to authenticate it). It uses an Ed25519 signature private key that is unique for each chip and loaded at ST secure personalization center.

On top of authentication, STSAFE-L010 comes with a unique ID and offers a usage monitoring service with decrement-only counters.

A 32 Kbytes nonvolatile memory can be configured in memory zones with different access rights, so that a given zone can always be read but not modified, like manufacturing data, or can freely be modified during the life of the product, to track the way it is used for instance.

Figure 1. STSAFE-L010 connection diagram



1.1 Pin and signal description

Figure 2. **UFDFPN8 pinout - Top view**

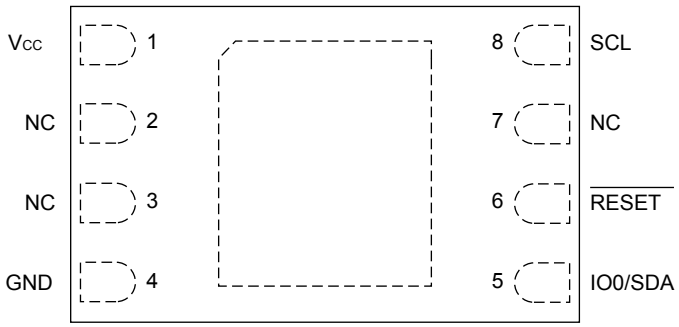
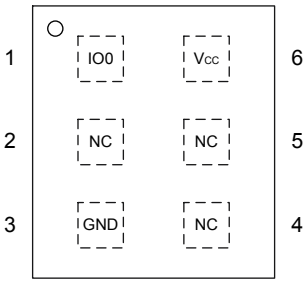
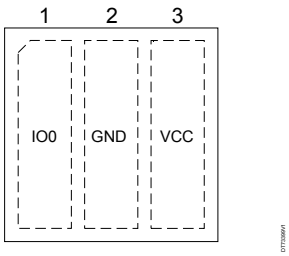


Figure 3. **X2F-PSON6 pinout - Top view**



Note: For the X2F-PSON6 package, V_{CC} and $\overline{RESET}$ are internally wired to pin 6

Figure 4. **DFN3 pinout - Top view**



Note: For the DFN3 package, V_{CC} and $\overline{RESET}$ are internally wired to pin 3 (V_{CC})

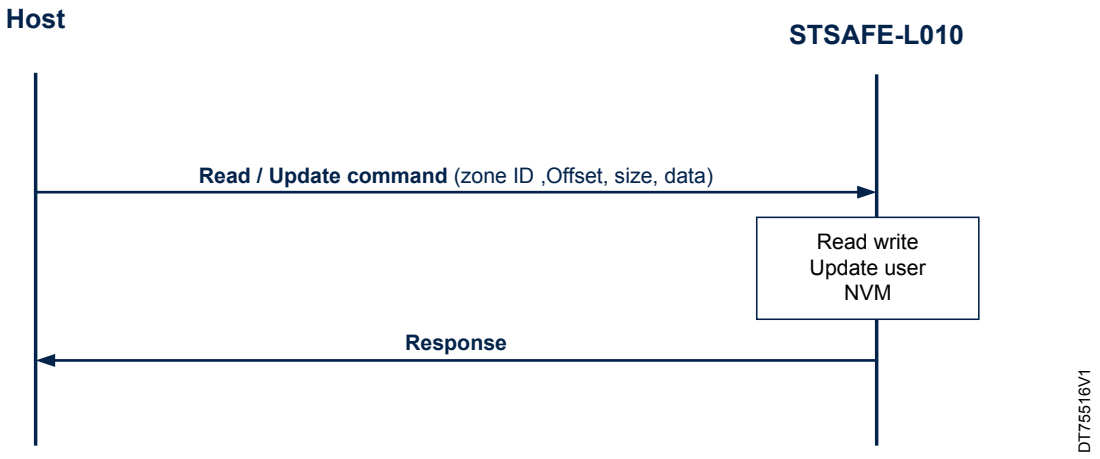
Table 1. **Signal descriptions**

Signal	Name	Description
V_{CC}	Power supply	The 1.62 V to 5.5 V supply voltage is supported for powering all internal STSAFE-L010 functions.
GND	Supply and signals ground	Ground reference pin for power and all *I/O* signals.
$\overline{\text{RESET}}$	Reset	This input signal is used to reset STSAFE-L010. The $\overline{\text{RESET}}$ pin is pull-down by default meaning that the device is reset if connected to ground or if the pin is floating. The device is active if the $\overline{\text{RESET}}$ pin is tied high.
IO0/SDA	Serial input/ output	This *I/O* signal is used to transfer data into and out of STSAFE-L010.
SCL	Serial clock	Serial clock for I2C data flow synchronization.
NC	-	Not connected internally.

1.2 Data management and usage monitoring

The STSAFE-L010 includes a secure memory storage intended for storage and device usage monitoring. The user memory region consists of up to 64 partitions (zones) with one-way counter. Each zone can be individually written, read, and updated. The following sequence diagram illustrate the use of read, write, and update commands.

Figure 5. **STSAFE-L010 data read/update sequence**



The data partition is set during chip manufacturing and can be customized on specific demand. Access to each zone can be restricted and locked using a set of attributes.

Overview of zone attributes:

- **Type**: indicating whether the zone has a one-way counter or not.
- **Data segment**: the zone data excluding the one-way counter (if any). The data segment can be absent (length is 0) when the zone type indicates that there is a one-way counter. When there is no one-way counter, the data segment cannot be absent.
- **One-way counter value**: 3-bytes unsigned integer. Absent if zone type indicates that there is no one-way counter.
- **Read access conditions (AC)**: in increasing order of strictness
  - Always.
  - Never.
- **Read AC change right**: A boolean indicating whether the *read access* conditions and read AC change right can be changed to a stricter value.

- **Update access conditions**: in increasing order of strictness
  - Always.
  - Never.
- **Update AC changes the right flag**: A boolean indicating whether the update access conditions, and the *update change right flag* can be updated to stricter conditions.

1.2.1 Device authentication

The *ECC* authentication is one of the primary services offered by the STSAFE-L010. This service provides a standardized approach to protect the brand ecosystem and the device against cloning. The device authentication relies on two factors:

- The verification of a unique identity composed of a unique *ECC* key pair and a pre-provisioned certificate in the STSAFE-L010.
- On the capabilities of the STSAFE-L010 to protect and never expose the *ECC* private key used during identity verification.

As illustrated in Figure 6, the pre-provisioned leaf-public key, is shared in a certificate signed by STMicroelectronics where STMicroelectronics acts as a certificate authority (*CA*). Any entity that needs to authenticate the device must first ensure the integrity and authenticity of the certificate by verifying the STSAFE-L010 certificate using a root *CA* self-signed certificate provided by STMicroelectronics. This confirms that the device certificate has been issued by STMicroelectronics and that its content is not altered. When the certificate is verified, the authenticity of the device is confirmed by sending a challenge to be signed by the device unique private key and verified using the public key shared within the device leaf-certificate.

Figure 6. STSAFE-L010 ECC authentication diagram

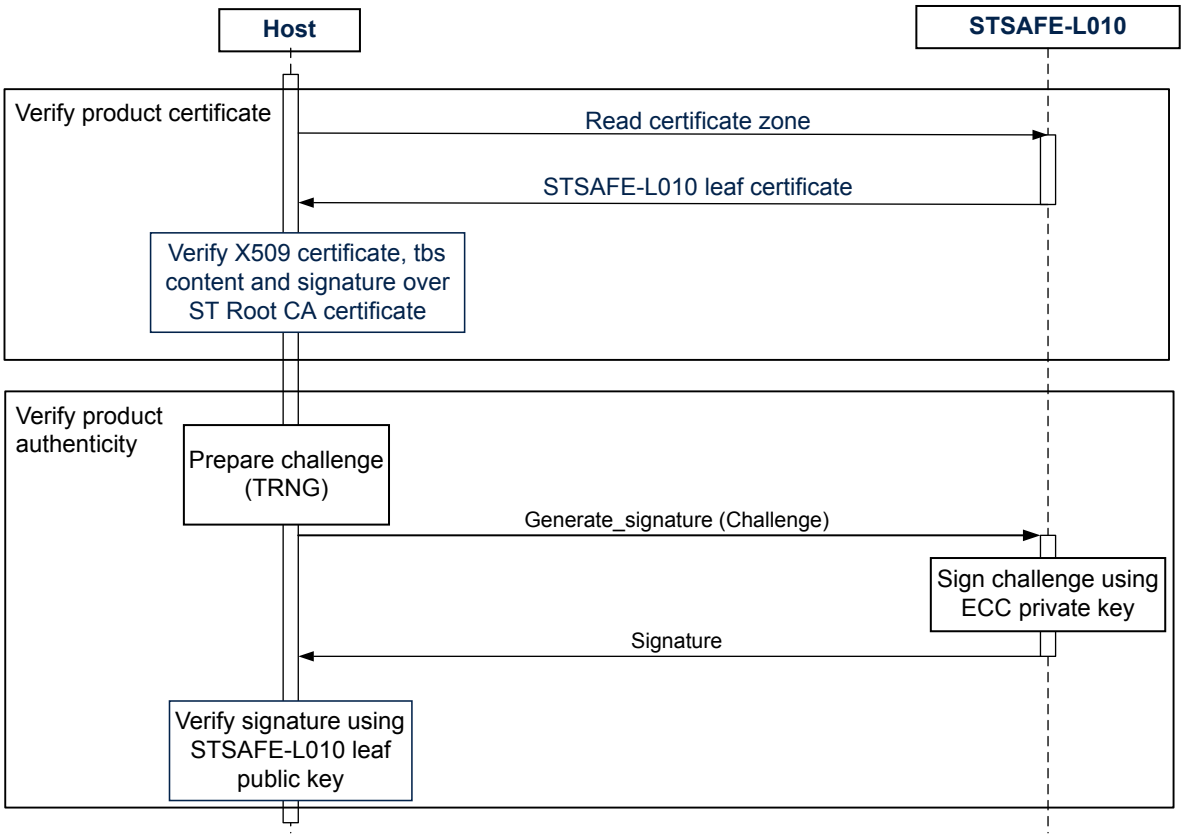
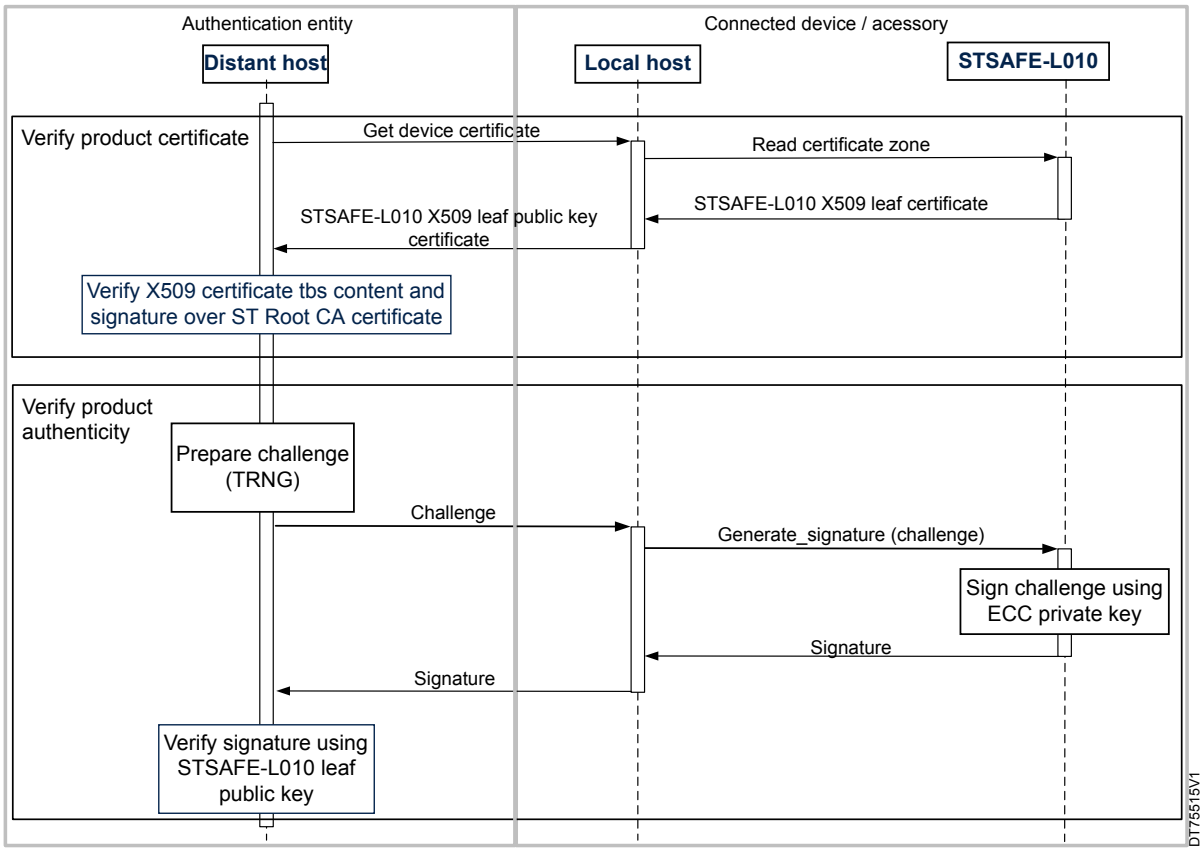


Figure 7 , illustrates the STSAFE-L010 authentication process on distant/external entity.

Figure 7. **STSAFE-L010 ECC Authentication diagram on distant entity**



1.2.2 User NVM data authentication

In complement to standard usage of the STSAFE-L010 *NVM* space as a storage area, the STSAFE-L010 offers developers with the possibility to enforce integrity and authenticity of the information coming from the secure element. It also protects against unwanted data manipulation on the bus.

As illustrated in Figure 8, the STSAFE-L010 unique key pair can be used to sign/verify the data exchanged on the communication bus from an STSAFE-L010 to the host . As for the standard authentication process, a two-step approach is to be followed to guarantee the authenticity of the data:

- Verification of the device certificate using the STMicroelectronics root *CA* to guarantee the leaf-public key authenticity.
- Verifying the signature generated by the STSAFE-L010 using its *ECC* private key over specific user-NVM zone content and the leaf certificate public-key.

Figure 8. **STSAFE-L010 user NVM data authentication**

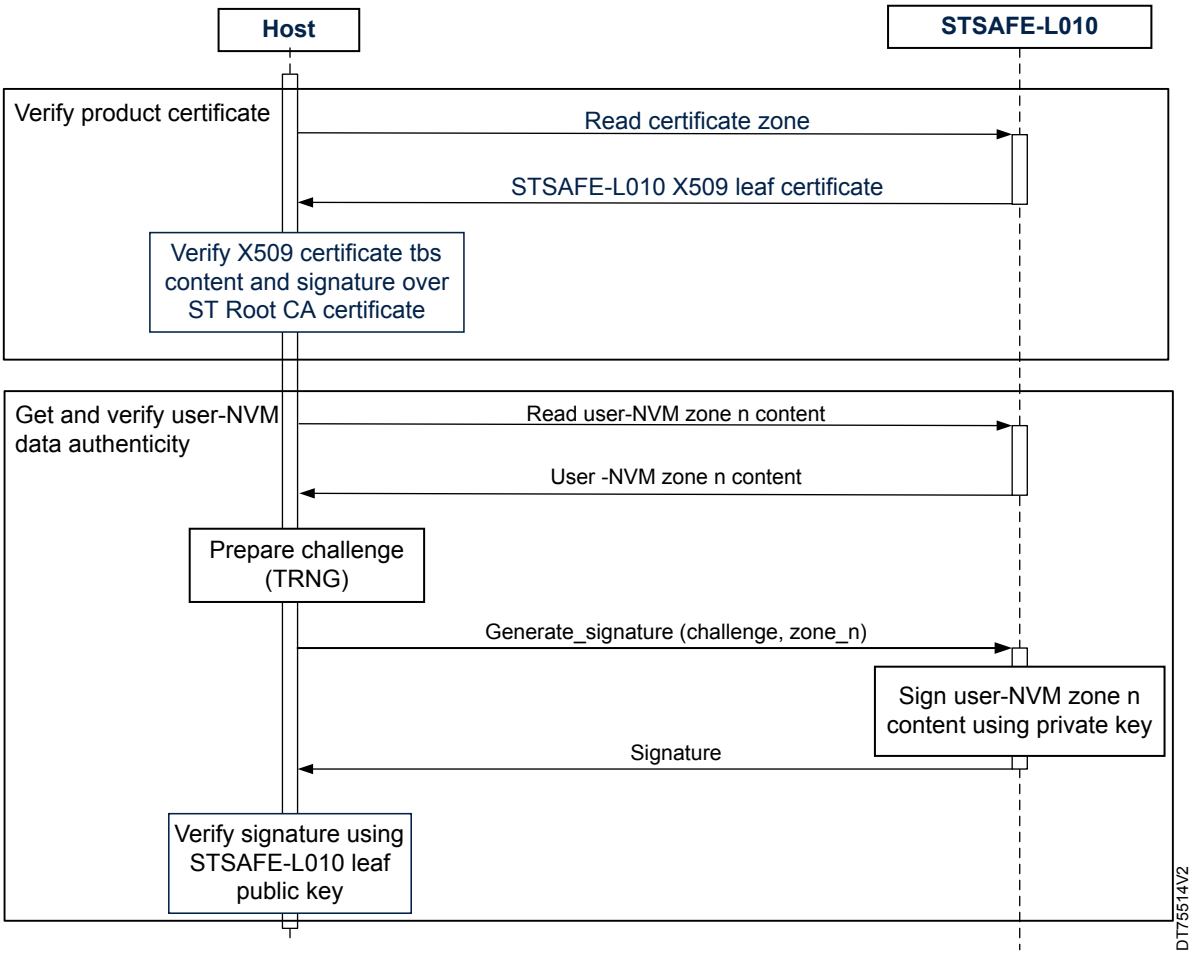
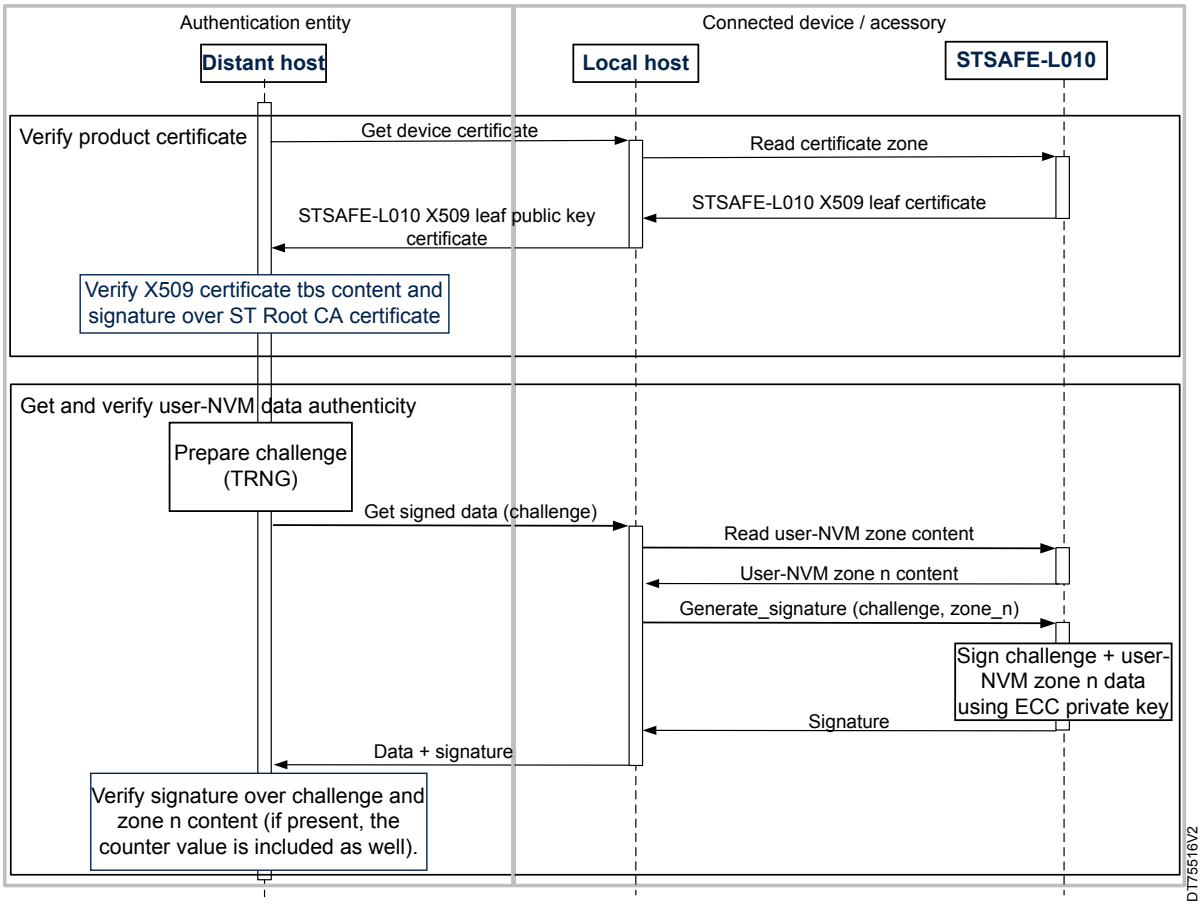


Figure 9 illustrates the STSAFE-L010 authenticated data exchange process with distant/external entity.

Figure 9. STSAFE-L010 user NVM data authentication on distant/external entity



2 Ecosystem

2.1 Services

The STSAFE-L010 comes ready to use, with pre-provisioned keys.

STMicroelectronics offers key provisioning services for storage of customer credentials in a secure, certified environment.

2.2 Software

The STSAFE-L010 is provided with a host software library that can be ported to a wide range of general-purpose microcontrollers or microprocessors. This library includes a command wrapper, cryptographic library as well as authentication and NVM update services.

2.3 Hardware

An STM32 Nucleo-64 extension is available as a reference design, and to accelerate the development of a secure solution with STSAFE-L010. This hardware allows the developer to benefit from the full STM32 Cube/Nucleo ecosystem.

3 STSAFE-L010 command set

ECHO

Returns as response the data received as command.

RESET

Closes any on-going secure session between host and STSAFE-L010 device then reboots the STSAFE-L010.

HIBERNATE

Sets the product in low-power consumption mode. In hibernate state, the device remains powered but loses its session context. Exiting from hibernate state can be performed by triggering the Reset pin or toggling data I/O. The device restart is equivalent to a restart after a reset or power on reset (POR).

DECREMENT

Decrements the one-way counter in a counter zone. When the counter reaches zero, the command is refused. In complement to the counter, the command can update the associated data segment with provided data.

It is also possible to change the access conditions (AC) to the counter/segment to a stricter value than the current one.

READ

Used to read data from a data partition zone. It reads the data starting from the specified offset within the zone and with the requested length. It checks the access conditions and only return the data starting from the specified offset up to the zone boundary.

This command can also be used to change the read access conditions of the zone to a stricter value.

UPDATE

Used to update data in a zone. It checks if the written data exceeds the zone boundary. When this occurs, it does not perform the operation.

This command can also be used to change the update access conditions of the zone to a stricter value; for example, when writing data only once. This command is applicable only on User-NVM zones without counter. For zone with counter the update is done through dedicated decrement command.

GENERATE SIGNATURE

This command generates an EdDSA signature over challenge, with the following optional data to sign :

- User *NVM* zone content
- STSAFE-L010 traceability information

REPEAT RESPONSE

Request STSAFE-L010 device to send again the last response frame.

PUT DATA

Used to modify specific device configuration attributes.

GET DATA

Used to get status on device configuration attributes.

4 Communication interfaces

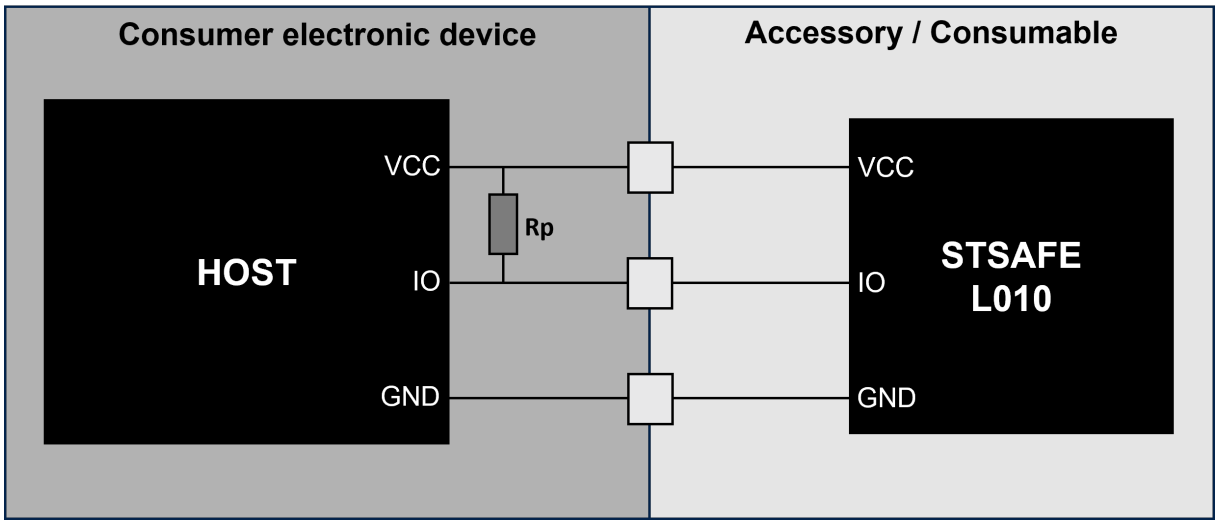
The STSAFE-L010 device supports ST1Wire and *I²C* communication interface. It acts as target on all the supported interfaces.

4.1 ST1Wire interface

The ST1Wire protocol is a custom protocol developed by STMicroelectronics to reduce the number of contacts required to perform bidirectional point to point communication between an applicative system (host) and a secure element (*SE*) device from STMicroelectronics.

The hardware implementation of the ST1Wire bus is illustrated below:

Figure 10. ST1Wire 3-contact implementation



The ST1Wire protocol is based on a single serial data line that carries information between a single master device (host) and one STSAFE-L010 device.

The ST1Wire protocol is a half-duplex protocol where the host can communicate with only one STSAFE-L010 device and in only one direction at a time.

. The host and the STSAFE-L010 are alternatively sender and receiver depending on the type of Frame to be exchanged on the bus. Specific bus arbitration based on ST1Wire Line steady state detection and byte acknowledge requires both master and slave communication *I/O* to be configured in open drain mode .

The bus pull-up resistor (Rp) must be selected, based on the *I/O*s electrical characteristics of master device and STSAFE-L010 devices. The following conditions must be met for Rp value selection:

$$VIL_{max\_host} > VCC^* \frac{Ron_{host}}{Rp + Ron_{host}}$$

$$VIL_{max\_STSAFE\text{-}L010} > VCC^* \frac{Rons_{STSAFE\text{-}L010}}{Rp + Ron_{STSAFE\text{-}L010}}$$

$$IOL_{max\_host} > \frac{VCC}{Rp + Ron_{host}}$$

$$IOL_{max\_STSAFE\text{-}L010} > \frac{VCC}{Rp + Ron_{STSAFE\text{-}L010}}$$

To be compliant with the ST1Wire electrical requirements, the host must use an open-drain I/O to interface with the bus. This allows the bus to be in two states:

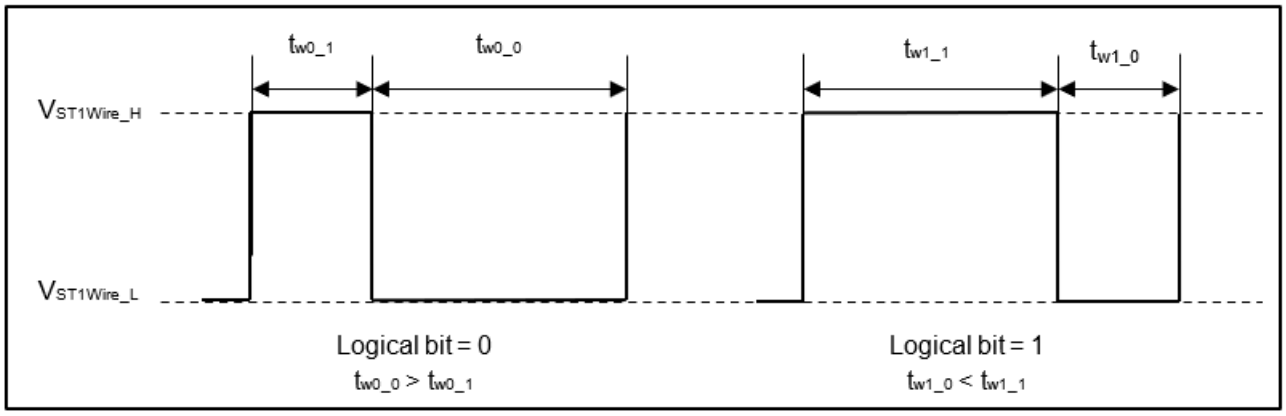
- **Idle state**: Line is at high level $V_{ST1Wire\_H}$ for more than $T_{cyc\_HOST\_min}$. Neither host nor any STSAFE-L010 devices drive the line. There is no communication on the bus.
- **Communicating state:** Line is driven alternatively by the host and the STSAFE-L010 device for frame exchange . During frame exchange both entities act alternatively as transmitter and receiver on the line . Transmitter and receiver cannot hold the line low for a time period higher than $T_{cyc\_HOST\_max}$. Except when the host sends an ST1Wire start of frame (*SOF*). Refer to Section 4.1.3: Frame protocol description for more details.

Note: For voltage and timings, refer to the Section 5.8: ST1Wire electrical characteristics.

4.1.1 Bit-transfer

The ST1Wire protocol encodes bits by applying pulse width modulation (PWM) of the ST1Wire data line. See the bit encoding representation in Figure 2.

Figure 11. Bit encoding



Logical bits are encoded with a $V_{ST1Wire\_H}$ pulse, followed by a $V_{ST1Wire\_L}$ pulse. The table below shows the encoding rules.

Note: For information on allowed durations, refer to Section 5.8: ST1Wire electrical characteristics.

Table 2. Logical bit encoding

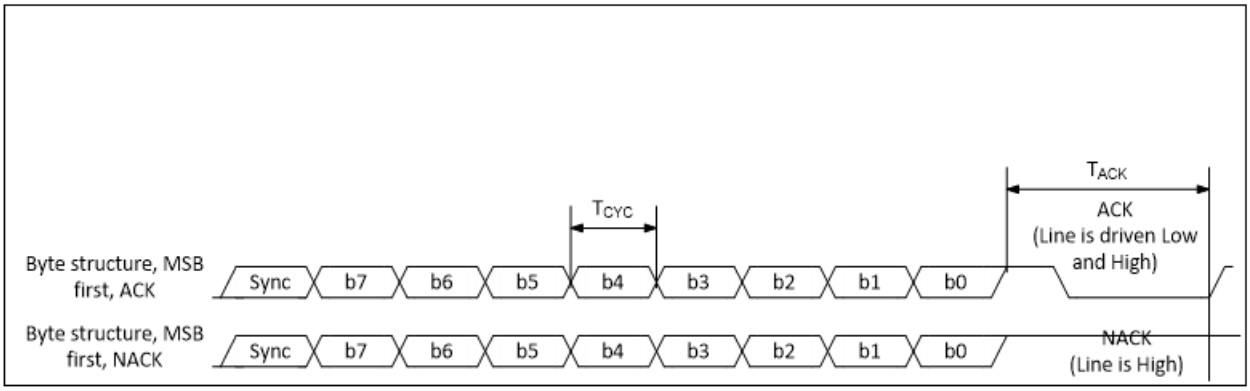
Logical value	Condition	Comment
0	$t_{W0\_0} > t_{W0\_1}$.	duration of $V_{ST1Wire\_L}$ > duration of $V_{ST1Wire\_H}$
1	$t_{W1\_0} < t_{W1\_1}$.	duration of $V_{ST1Wire\_L}$ < duration of $V_{ST1Wire\_H}$

The $V_{ST1Wire\_H}$ and $V_{ST1Wire\_L}$ depends on physical bus implementation and characteristics of both STSAFE-L010 and host *I/O*.

4.1.2 Byte transfer

The ST1Wire interface transfer unit is the byte. Bytes are encapsulated in a data structure containing three parts, as illustrated in the image below.

Figure 12. **Byte structure**

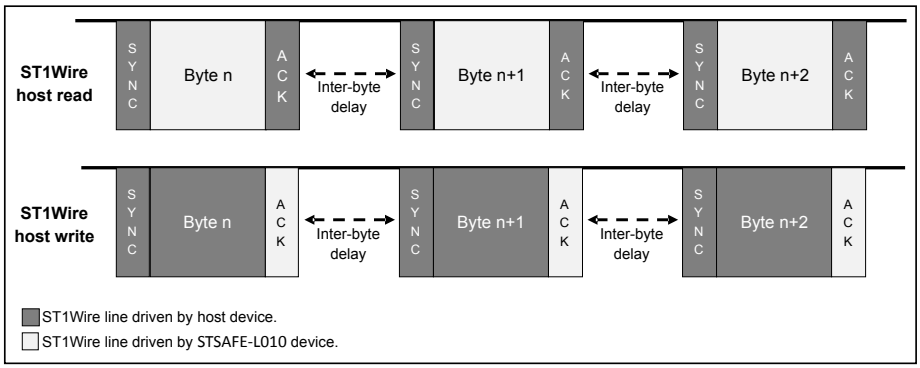


- **Sync** : First symbol of the byte transfer. The sync symbol is always generated by the ST1Wire host device and consists in a low level ($V_{ST1Wire\_L}$) pulse. As before the sync symbol, the ST1Wire is in idle state at ($V_{ST1Wire\_H}$), the implementation of the sync symbol can consist in generating a bit with a logic “1”.
- **Byte**: Contains the byte to transfer. Bits in the byte are transferred in series. After the last bit has been sent to the interface, the transmitter releases the interface, which is set high. It then polls the line for a reply which is called the **ACK** .
- **ACK** : A byte acknowledge symbol generated by the receiver at each byte transfer. This symbol informs the transmitter whether or not the current byte has been received correctly and if the receiver is ready to receive the next byte.
  - *ACK*: A high pulse followed by a low pulse. The ST1Wire line is driven high ($V_{ST1Wire\_H}$), and then low ($V_{ST1Wire\_L}$) and then the ST1Wire line is released again to ($V_{ST1Wire\_H}$). A new byte can then be immediately released by the transmitter. As before the back symbol, the ST1Wire is in idle mode at ($V_{ST1Wire\_H}$) , the implementation of the ACK symbol can consist in generating a logic "0" bit.
  - *NACK* = ST1Wire line stays at ST1Wire_H level for more than T_{ACK}.

  The *ACK* symbol duration (T_{ACK}) is bounded to [2xT_{CYC}]. The transmitter detects that a *NACK* has occurred when T_{ACK} has expired, and no “low” pulse of the appropriate length has been received. If the receiver *NACK*s a byte, the transfer is aborted. The bus is in idle state and the master must repeat the transfer from the beginning.

The ST1Wire protocol supports inter-byte delay as illustrated in the figure below. The inter-byte delay slows down the communication between the master and the STSAFE-L010 device. The inter-byte duration must be managed by the ST1Wire master when generating the Sync bit for each byte to be read or written. During the inter-byte delay, the line must be kept at $V_{ST1Wire\_H}$.

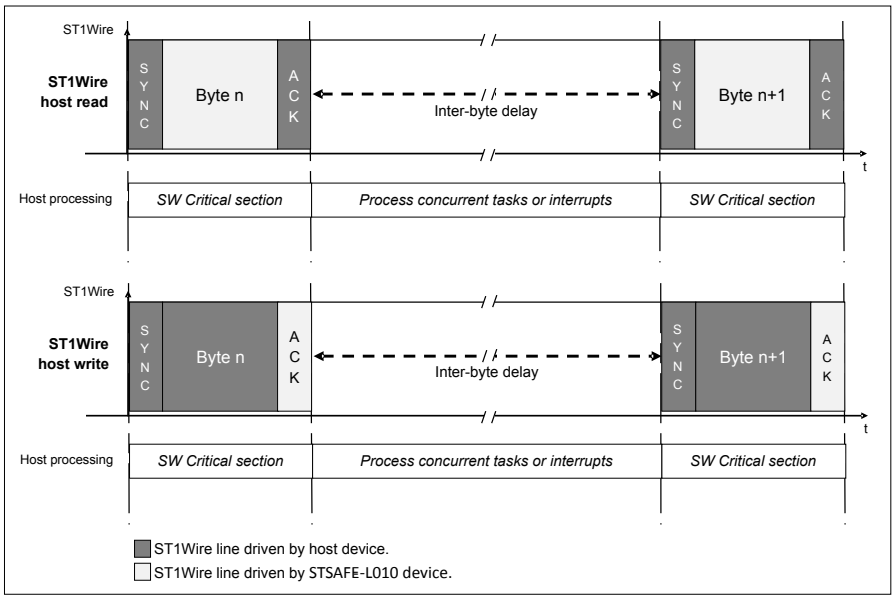
Figure 13. **ST1Wire inter-byte delay**



DT75502V1

On host systems running specific *OS* or *RTOS*, it is recommended to use critical software section during byte transfer. Critical software sections ensure correct byte read timings and byte write timings on the ST1Wire bus. During a critical section, the host must disable all interrupt and potential *OS*/*RTOS* concurrent task management. As represented in the figure below. To minimize the impact of the critical section at system/host level, the inter-byte delay allows the host to process interrupts and concurrent *OS* tasks between each ST1Wire byte transfer.

Figure 14. Host processing vs inter-byte management



DT75505V1

4.1.3 Frame protocol description

When the ST1Wire bus is in the idle state , the host can initiate the communication by sending an ST1Wire *SOF* followed by either a command frame (*CF*) or a response frame.

Figure 15. **ST1Wire start of frame (*SOF*)**

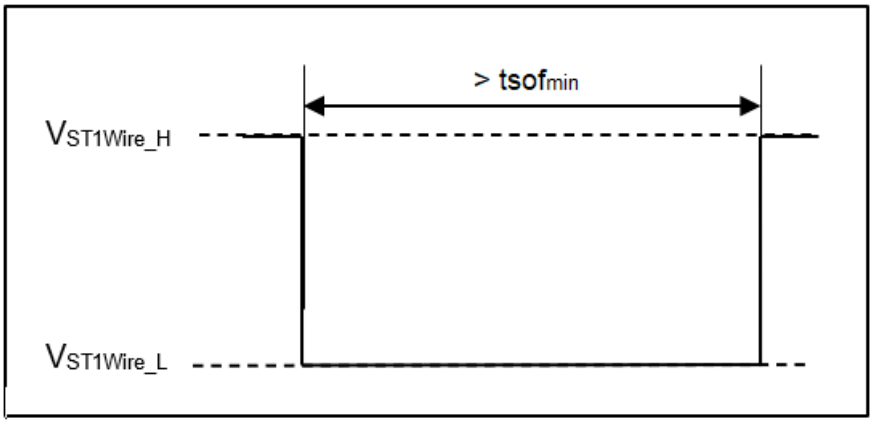
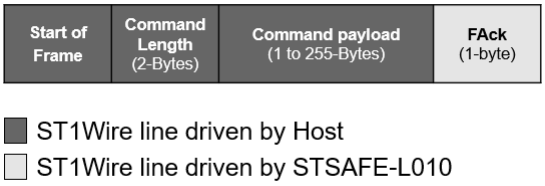


Figure 16. **STSAFE-L010 ST1Wire command frame**

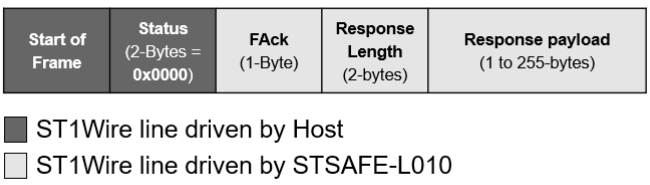


Important: *A command frame must always be followed by a response frame. If an error is reported on the bus, the whole command plus responses which were exchanged must be repeated.*

An ST1Wire command frame is always composed of the following elements.

- ***Start of frame (SOF)*****:** $V_{ST1Wire}$ line is pulled low for a minimum duration $t_{SOF\ min}$ duration.
- ***Command length (2-byte)*****:** Defines the command type and payload size. The command frame length must always be superior to 0x0000.
- ***Command payload (n-byte)*****:** Command data with content aligned with STSAFE-L010 device user manual
- ***Frame acknowledge (FAck) (1-byte):***Both command and status frames must be acknowledged (*ACK*) by the slave using an *FAck* byte equal to 0x20. Other values are considered as a *NACK*. In the case the slave *NACK* the frame, the ST1Wire is moved into Idle state.

Figure 17. **STSAFE-L010 ST1Wire response frame**



An ST1Wire response frame is always composed of the following elements.

- ***Start of frame (SOF)*****:** VST1Wire line pulled LOW for a minimum duration t_{SOF} min duration.
- ***Status byte (2-byte)*****:** must be equal to 0x0000. This byte notifies the STSAFE-L010 device that a response to the previous command is requested.

- ***Frame acknowledge (FAck) (1-byte):***Status frames acknowledgement by the slave using an *FAck* byte equal to 0x20. Other values are considered as a *NACK*. In the case where the slave *NACK*s the frame, the ST1Wire is moved into idle state.
- ***Response length (2-byte):***length of the response payload to be sent by the STSAFE-L010 device.
- ***Response payload (n-byte):***Response data with content aligned with STSAFE-L010 device User Manual

5 AC/DC characteristics

This section summarizes the operating and measurement conditions, and the DC and AC characteristics of the device. The parameters in the DC and AC characteristic tables that follow are derived from tests performed under the measurement conditions summarized in the relevant tables. Designers should check that the operating conditions in their circuit match the measurement conditions when relying on the quoted parameters.

5.1 Absolute maximum ratings

Table 3. Absolute maximum ratings

Symbol	Parameter	Value	Unit
V_{CC}	Supply voltage	–0.3 to 6.5	V
V_{IO}	Input or output voltage relative to ground	–0.3 to V_{CC} + 0.3	V
T_A	Ambient operating temperature	–25 to +85	°C
T_{STG}	Storage temperature (Refer to package specification)	–65 to +150	°C
V_{ESD}	Electrostatic discharge voltage according to JESD22-A114, Human Body Model	4000	V

Note: Stresses listed above may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or any other conditions above those indicated in the operational sections of the specification is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

5.2 Recommended power supply filtering

Supply filtering is recommended as shown in Figure 18.

Figure 18. Recommended filtering capacitors on VCC

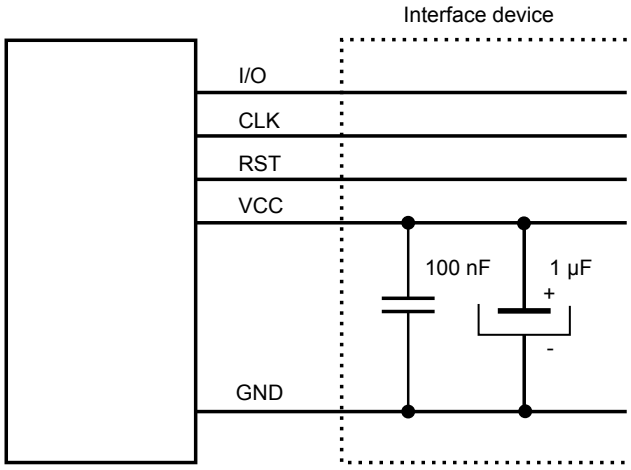


Table 4. Maximum V_{CC} rising slope

Symbol	Parameter	Value	Unit
S_{VCC}	Maximum V_{CC} rising slope	5	V/µs

5.3 AC characteristics

T_A = –25 °C to 85 °C, unless otherwise specified.

Table 5. 1.8 V and 3 V AC characteristics

Symbol	Parameter	Condition	Min.	Typ.	Max.	Unit
$t_{WLReset}$(1)	Pulse width for reset	-	5	-	-	µs
$t_{HLReset}$	Minimum time for reset active after power-up	-	80	-	-	µs
t_{BOOT}	Delay between V_{CC} reaching the POR threshold and STSAFE-L010 ready to receive first command	-	-	10	20	ms
		-				
t_R, t_{FReset}	Reset rise and fall time	-	-	-	1	µs
t_R, t_F I/O	I/O rise and fall time	Load capacitance = 30 pF	-	-	1	µs

1. *Anylow pulse (from `1' to `0', then `0' to `1') shorter than 100 ns is ignored. Reset is not guaranteed for pulses between 100 ns and 500 ns; reset is guaranteed for pulses longer than 500 ns.*

5.4 DC characteristics

T_A = –25 °C to 85 °C, unless otherwise specified.

Note: The voltage on all inputs or outputs must not exceed V_{CC} + 0.3 V or be less than –0.3 V.

Table 6. DC characteristics

Symbol	Parameter	Condition	Min.	Typ.	Max.	Unit
POR	Power-on-reset voltage	-	-	1.45	1.61	V
V_{cc}	Standard operating voltage (1.8 V to 5 V ± 10%)	-	1.62	-	5.5	V

Table 7. 1.8 V DC characteristics (V_{CC} = 1.8 V ±10%)

Symbol	Parameter	Condition	Min.	Typ.	Max.	Unit
V_{IL}	Input low voltage (RESET, *I/O*)	-	0	-	0.2 × V_{CC}	V
V_{IH}	Input high voltage (RESET, *I/O*)	-	0.7 × V_{CC}	-	V_{CC}	V
I_{IL}	Input low current (*I/O*)	0 < V_{IL} < 0.2 × V_{CC}	-100	-	1	µA
	Input low current (RESET)	0 < V_{IL} < 0.2 × V_{CC}	-1	-	10	µA
I_{IH}	Input high current (*I/O*)	0.7 × V_{CC} < V_{IH} < V_{CC}	-100	-	1	µA
I_{IH}	Input high current (RESET)	0.7 × V_{CC} < V_{IH} < V_{CC}	-1	-	10	µA
V_{OL}	Output low voltage (*I/O*)	I_{OLMAX} = 1 mA	0	-	0.15 × V_{CC}	V

Table 8. 3 V DC characteristics (V_{CC} = 3 V ± 10%)

Symbol	Parameter	Condition	Min.	Typ.	Max.	Unit
V_{IL}	Input low voltage (RESET, *I/O*)	-	0	-	0.2 × V_{CC}	V
V_{IH}	Input high voltage (RESET, *I/O*)	-	0.7 × V_{CC}	-	V_{CC}	V
I_{IL}	Input low current (*I/O*)	0 < V_{IL} < 0.2 × V_{CC}	-200	-	1	µA
	Input low current (RESET)	0 < V_{IL} < 0.2 × V_{CC}	-1	-	10	µA
I_{IH}	Input high current (*I/O*)	0.7 × V_{CC} < V_{IH} < V_{CC}	-200	-	1	µA
	Input high current (RESET)	0.7 × V_{CC} < V_{IH} < V_{CC}	-1	-	10	µA
V_{OL}	Output low voltage (*I/O*)	I_{OLMAX} = 4 mA	0	-	0.15 x V_{CC}	V

5.5 Performance and power consumption characteristics

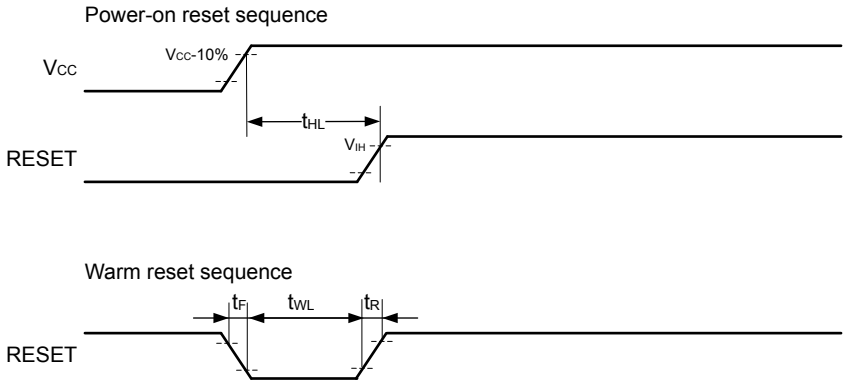
T_A = –25 °C to 85 °C, unless otherwise specified.

Table 9. 1.8 V and 3 V power consumption characteristics

Symbol	Parameter	Conditions	Typ.	Max.	Unit
I_{CCPROC}	Supply current when executing instructions stored in ROM	-	1.3	4	mA
$I_{CCHibernate}$	Supply current in hibernate mode	-	1	2	µA
$I_{CCReset}$	Supply current in reset	-	0.2	0.5	mA

5.6 Timings

Figure 19. Power-on and warm reset sequences



5.7 AC measurement conditions

T_A = –25 °C to 85 °C, f = 1 MHz, unless otherwise specified.

Table 10. AC measurement conditions

Parameter	Value
Input rise and fall times	10 ns (max.)
Input pulse voltage	V_{IL} to V_{IH}

Parameter	Value
Input timing reference voltage	$0.5 \times V_{CC}$
Output timing reference voltage	V_{OL} to V_{OH}

Figure 20. AC testing input/output waveforms

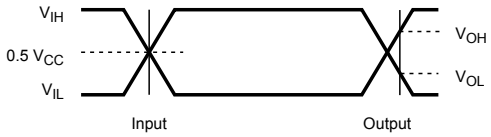


Figure 21. AC testing load circuit

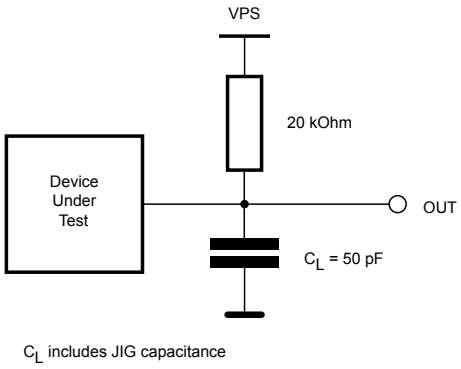


Table 11. Capacitance on IO pad

Symbol	Parameter	Min.	Max.	Unit
C_{IN}	Input capacitance	-	30	pF
C_{OUT}	Output capacitance	-	30	pF

5.8 ST1Wire electrical characteristics

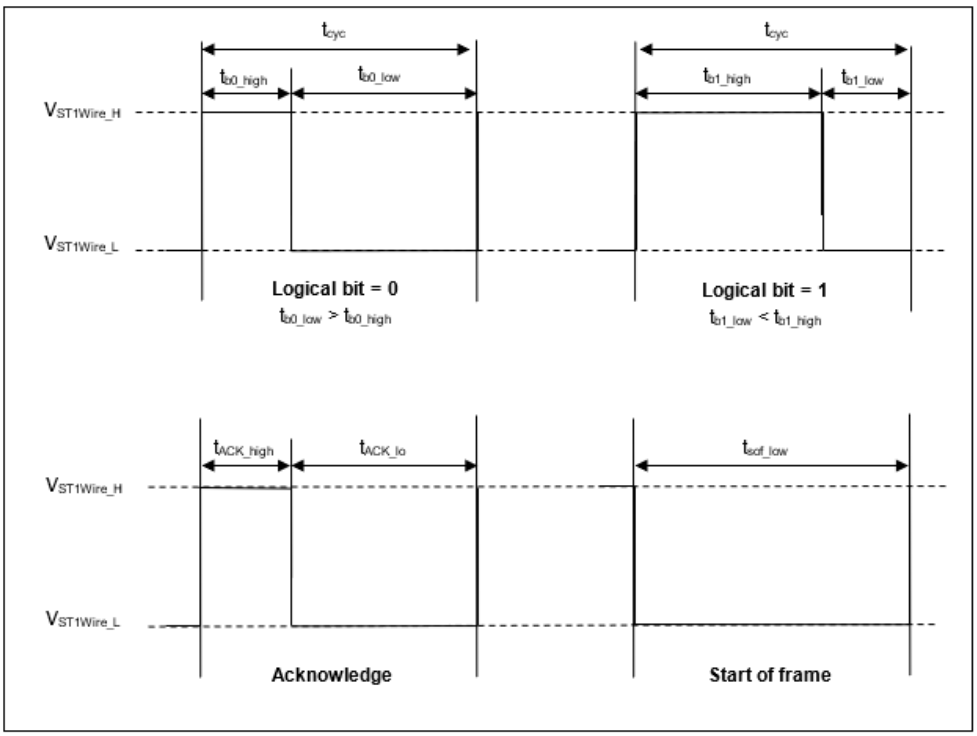
The following tables give the electrical characteristic of the ST1Wire protocol.

Table 12. ST1Wire 3-contacts DC characteristics (1.62 to 5.5 V; -25°C to 85°C ; CL = 20 pF; Pull-up = 1.375 kΩ)

Symbol	Description	Min.	Max.	Unit
$t_{b0\_low\_STSAFE}$	STSAFE-L010 logical ‘0’ bit low pulse duration	4.9	7.4	µs
$t_{b0\_high\_STSAFE}$	STSAFE-L010 logical ‘0’ bit high pulse duration	1.7	3.5	µs
$t_{b1\_low\_STSAFE}$	STSAFE-L010 logical ‘1’ low pulse duration	1.8	3.7	µs
$t_{b1\_high\_STSAFE}$	STSAFE-L010 logical ‘1’ bit high pulse duration	5.3	6.6	µs
$t_{ACK\_high\_STSAFE}$	STSAFE-L010 byte acknowledge high pulse duration.	2	3.9	µs
$t_{ACK\_low\_STSAFE}$	STSAFE-L010 byte acknowledge low pulse duration.	4.1	5.2	µs
t_{cyc_HOST}	HOST bit duration	10	200	µs

Symbol	Description	Min.	Max.	Unit
$t_{b0\_low\_HOST}$	HOST logical ‘0’ bit low pulse duration	0.6	0.75	t_{cyc_HOST}
$t_{b0\_high\_HOST}$	HOST logical ‘0’ bit high pulse duration	0.25	0.4	t_{cyc_HOST}
$t_{b1\_low\_HOST}$	HOST logical ‘1’ low pulse duration	0.25	0.4	t_{cyc_HOST}
$t_{b1\_high\_HOST}$	HOST logical ‘1’ bit high pulse duration	0.6	0.75	t_{cyc_HOST}
$t_{ACK\_high\_HOST}$	HOST byte acknowledge high pulse duration.	0.1	-	us
$t_{ACK\_low\_HOST}$	HOST byte acknowledge low pulse duration.	0.5	20	µs
$t_{sof\_low\_HOST}$	HOST Start of frame low pulse duration	37	-	µs
$t_{sync\_low\_HOST}$	HOST sync bit low pulse duration	5.1	11.9	µs
$t_{inter\text{-}byte}$	HOST sync bit high pulse duration	3.1	-	µs
$t_{SoF\_low\_to\_sync\_high}$	Delay between rising edge of SoF and beginning of t_{sync_high}	3.6	5	µs

Figure 22. ST1Wire DC timings description



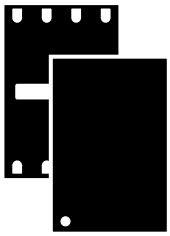
6 Package information

6.1 UFDFPN8 package specification

This section provides specific information concerning the 2 × 3 × 0.50 mm, 8 lead, ultra thin, fine-pitch, dual flat, no-lead package (UFDFPN8).

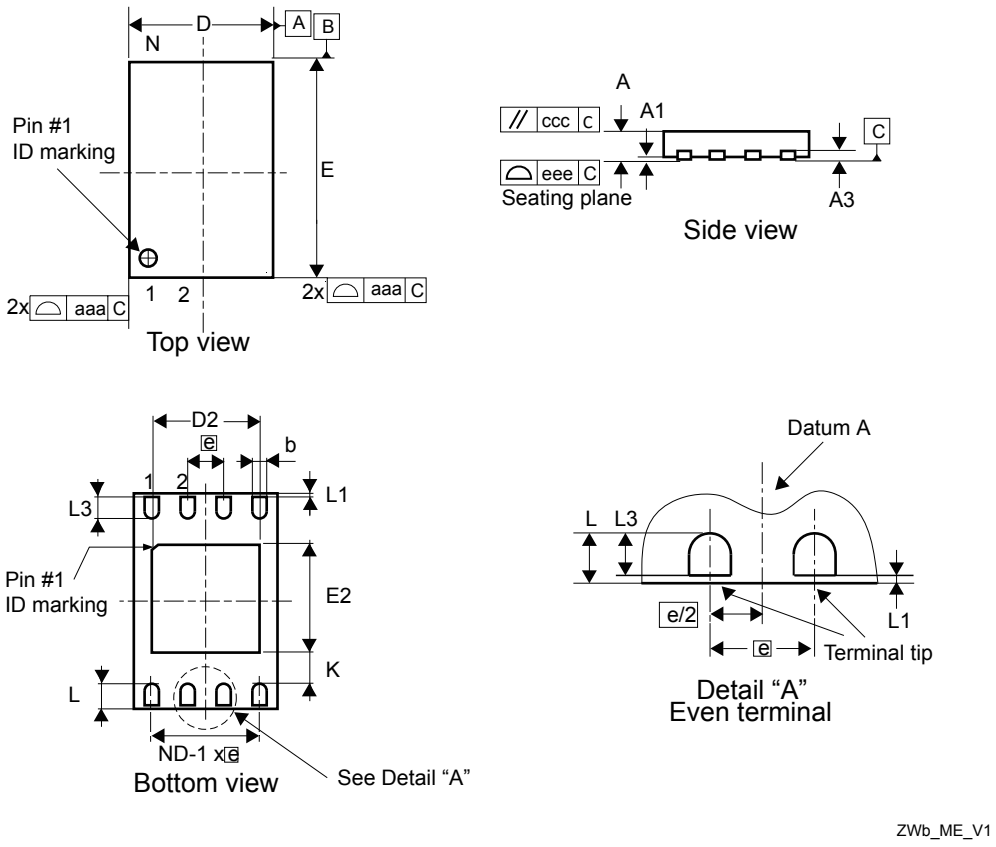
In order to meet environmental requirements, ST offers these devices in different grades of ECOPACK® packages, depending on their level of environmental compliance. ECOPACK® specifications, grade definitions and product status are available at: www.st.com. ECOPACK® is an ST trademark.

Figure 23. UFDFPN8 package



6.1.1 UFDFPN8 package information

Figure 24. UFDFPN8 - 8-lead, 2 × 3 mm, 0.5 mm pitch ultra thin profile fine pitch dual flat package outline



1. *Maximum package warpage is 0.05 mm.*
2. *Exposed copper is not systematic and can appear partially or totally according to the cross-section.*
3. *Drawing is not to scale.*

Table 13. UFDFPN8 - 8-lead, 2 × 3 mm, 0.5 mm pitch ultra thin profile fine pitch dual flat package mechanical data

Symbol	millimeters			inches[1]		
	Min.	Typ.	Max.	Min.	Typ.	Max.
A	0.45	0.55	0.60	0.018	0.022	0.024
A1	0.00	0.02	0.05	0.000	0.001	0.002
b [2]	0.20	0.25	0.30	0.008	0.010	0.012
D	1.90	2.0	2.10	0.075	0.079	0.083
D2	1.20	-	1.60	0.047	-	0.063
E	2.90	3.00	3.10	0.114	0.118	0.122
E2	1.20	-	1.60	0.047	-	0.063
e	-	0.5 BSC[3]	-	-	0.020 BSC[3]	-
K	0.30	-	-	0.012	-	-
L	0.30	-	0.50	0.012	-	0.020
L1	-	-	0.15	-	-	0.006

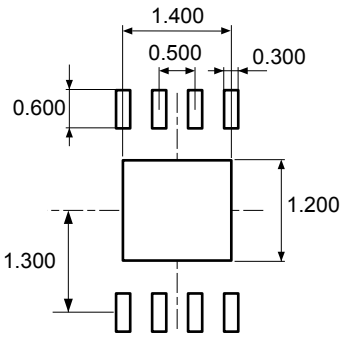
Symbol	millimeters			inches[1]		
	Min.	Typ.	Max.	Min.	Typ.	Max.
L3	0.30	-	-	0.012	-	-
aaa	-	-	0.15	-	-	0.006
bbb	-	-	0.10	-	-	0.004
ccc	-	-	0.10	-	-	0.004
ddd	-	-	0.05	-	-	0.002
eee[4]	-	-	0.08	-	-	0.003

1. *Values in inches are converted from mm and rounded to 3 decimal digits.*
2. *Dimension b applies to plated terminal and is measured between 0.15 and 0.30 mm from the terminal tip.*
3. *Basic spacing between centers.*
4. *Applied for exposed die paddle and terminals. Excludes embedding part of exposed die paddle from measuring.*

6.1.2 Recommended footprint information for UFDFPN8 (landing pattern)

The figure below describes ST recommendations in terms of the printed circuit board landing pattern for the UFDFPN8 2 × 3 mm package.

Figure 25. Recommended footprint for UFDFPN8



1. *All dimensions are in millimeters.*

6.1.3 UFDFPN8 tape and reel packing

Surface-mount packages can be supplied with tape and reel packing. The reels have a 13" typical diameter. They contain 5000 devices each.

Reels are in plastic, either antistatic or conductive, with a black conductive cavity tape. The cover tape is transparent antistatic or conductive.

The devices are positioned in the cavities with the identifying pin (normally Pin “1”) on the same side as the sprocket holes in the tape.

The STMicroelectronics Tape & Reel specifications are compliant to the EIA 481-A standard specification.

Table 14. UFDFPN8 package on tape and reel

Package	Description	Tape width	Tape pitch	Reel diameter	Quantity per reel
UFDFPN8 2 × 3 mm	Flat package, no lead	8 mm	4 mm	13 in.	5000

Figure 26. **Dimensions of a 13" reel for 8 mm tape**

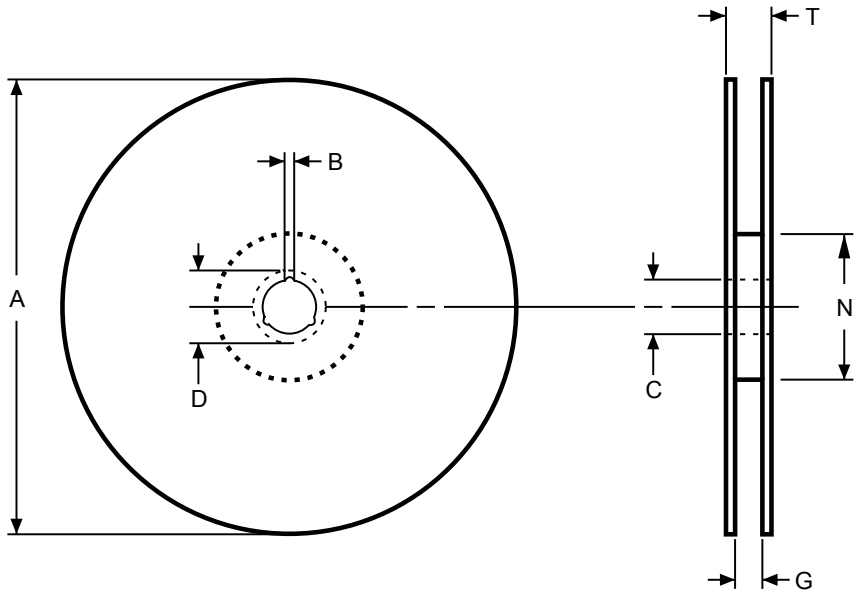
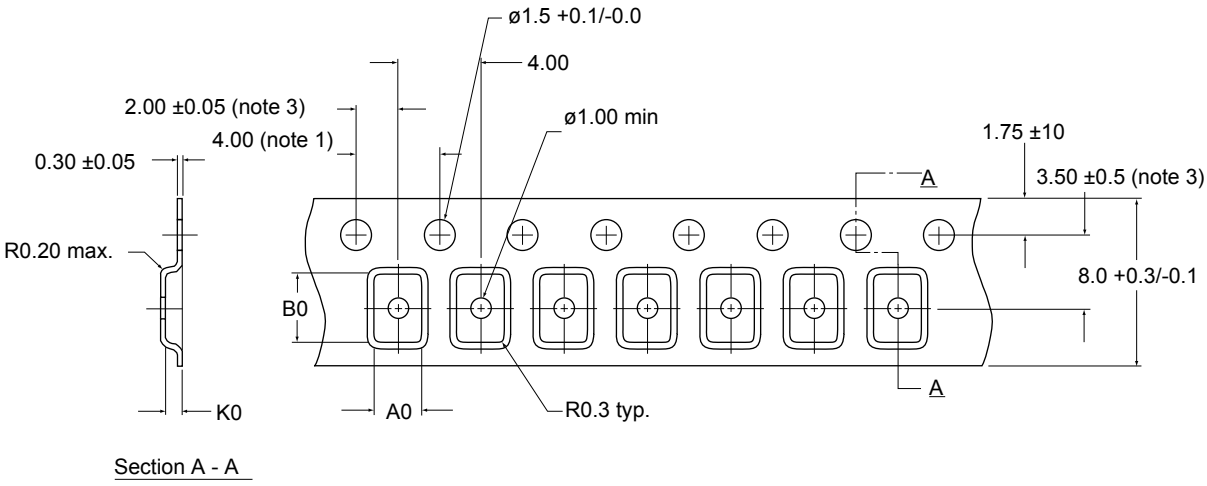


Table 15. **UFDFPN8 reel dimensions**

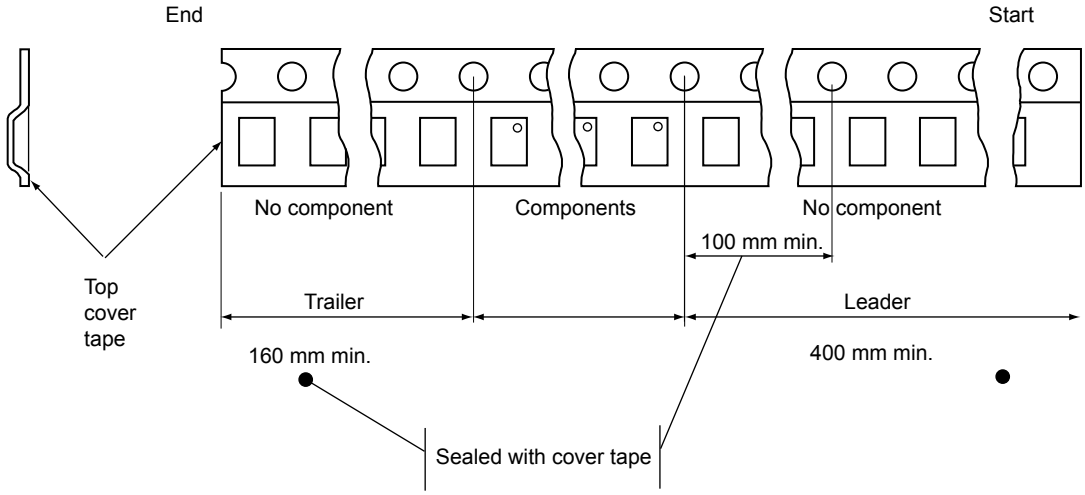
Reel size	Tape size	A Max.	B Min.	C	D Min.	G Max.	N Min.	T Max.	Unit
13"	8	330	1.5	13 ±0.25	20.2	8.6	100	14.4	mm

Figure 27. **Embossed carrier tape for UFDFPN8**



1. *Cumulative tolerance of ten sprocket hole pitches: ±0.2.*
2. *Camber in compliance with EIA 481.*
3. *Pocket position relative to sprocket hole measured as the true position of the pocket, not pocket hole.*
4. *All dimensions are in millimeters.*
5. *Unless otherwise noted, tolerances are ±0.02 for one decimal place and ±0.10 for two decimal places.*
6. *A0 = 2.30; Bo = 3.30; K0 = 0.75.*

Figure 28. **Leader and trailer for UFDFPN8**



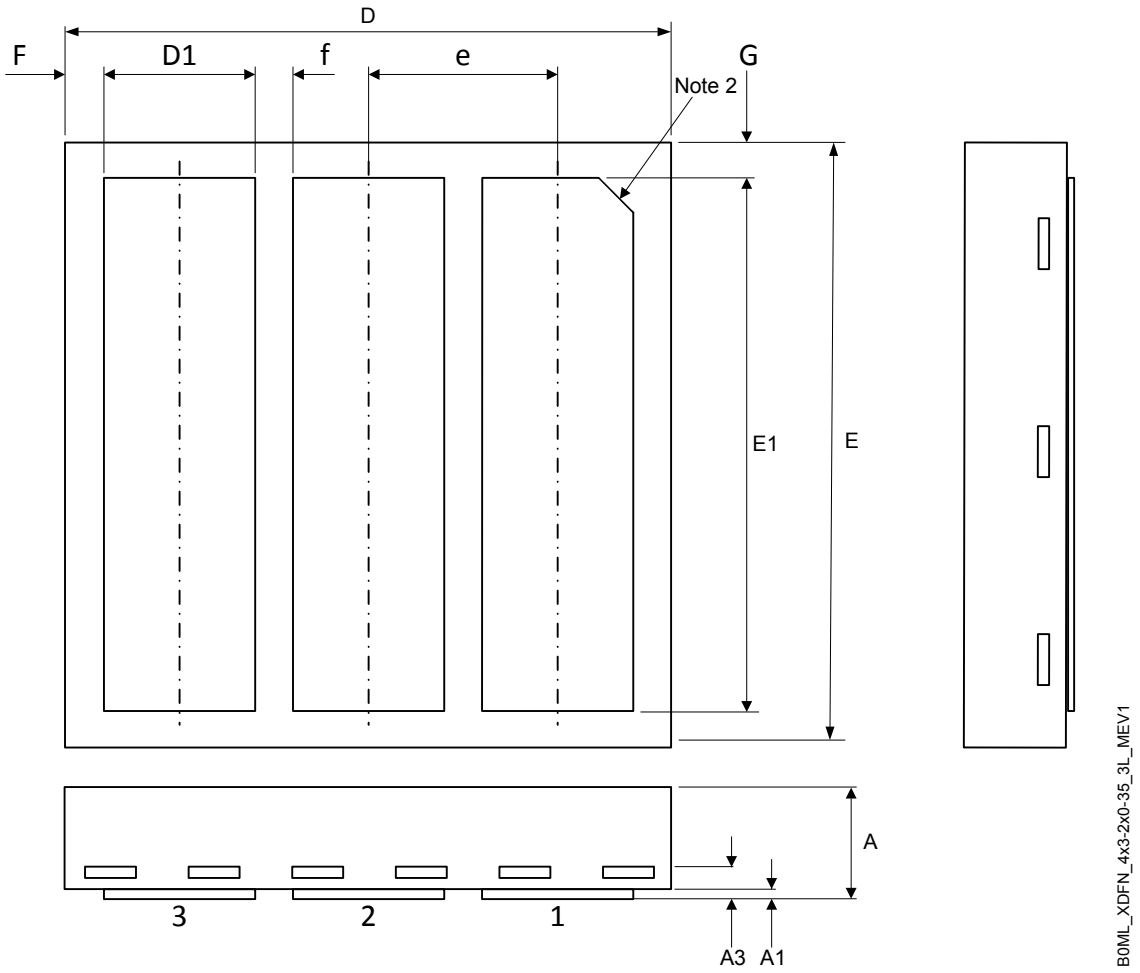
Die orientation into the tape - Leader and trailer

6.2 DFN3 package specification

6.2.1 XDFN3 package information

XDFN3 is an three-terminal, 4 × 3.2 mm, extremely thin dual flat no lead package.

Figure 29. XDFN3 package outline



1. *Drawing is not to scale.*
2. *This stands for C0.15*

Table 16. **XDFN3 package mechanical data**

Symbol	Millimeters[1][2]		
	Min.	Typ.	Max.
A	-	-	0.38
A1	-	-	0.05
A3		0.10 REF	
D	3.90	4.00	4.10
D1	1.05	1.10	1.15
E	3.10	3.20	3.30
E1	2.80	2.85	2.90
e		1.240 BSC[3]	
F		0.21 REF	
f		0.14 REF	
G		0.175 REF	
N (number of pins)		3[4]	

1. *Dimensioning and tolerancing schemes according to ASME Y14.5M-1994.*
2. *All values are in millimeters rounded to the second decimal except for N.*
3. *Basic space between centers.*
4. *Total number of terminals*

6.2.2 XDFN3 4 x 3.2 x 0.35 tape and reel packing

Surface-mount packages can be supplied with tape and reel packing. The reels have a 13" typical diameter. They contain 5000 devices each.

Reels are in plastic, either antistatic or conductive, with a black conductive cavity tape. The cover tape is transparent antistatic or conductive.

The devices are positioned in the cavities with the identifying pin (normally pin “1”) on the same side as the sprocket holes in the tape.

The STMicroelectronics tape and reel specifications are compliant with the EIA 481-A standard specification.

Table 17. **XDFN3 4 x 3.2 x 0.35 packages on tape and reel**

Package	Description	Tape width	Tape pitch	Reel diameter	Quantity per reel
B0ML	XDFN 4×3.2 3L	12 mm	8.00 ± 0.10	13"	5000 units

Figure 30. **XDFN3 4 x 3.2 x 0.35 reel diagram**

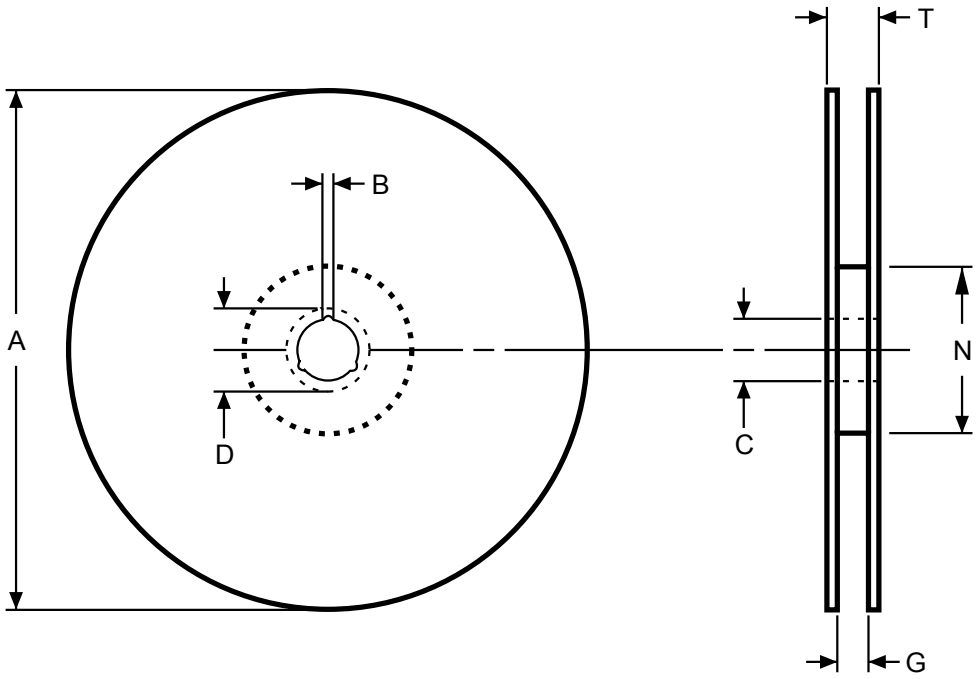


Table 18. **XDFN3 4 x 3.2 x 0.35 reel dimensions**

Reel size	Tape size	A Max.	B Min.	C	D Min.	G Max.	N Min.	T Max.	Unit
13" Hub 7"	12 mm	332 mm	1.50 mm	13 + 0.50 / -0.20 mm	20.20 mm	14.40 mm	176 mm	18.40 mm	5000 units/reel

Figure 31. **XDFN3 4 x 3.2 x 0.35 Leader and trailer**

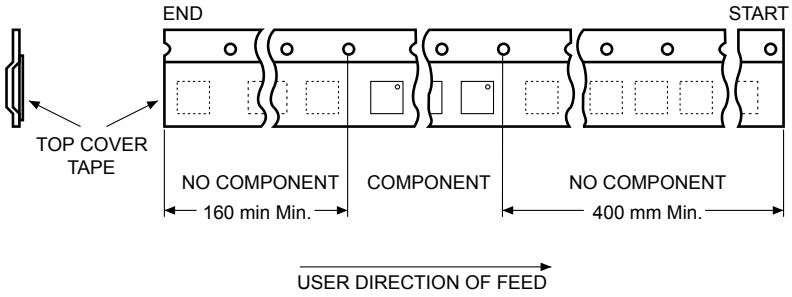
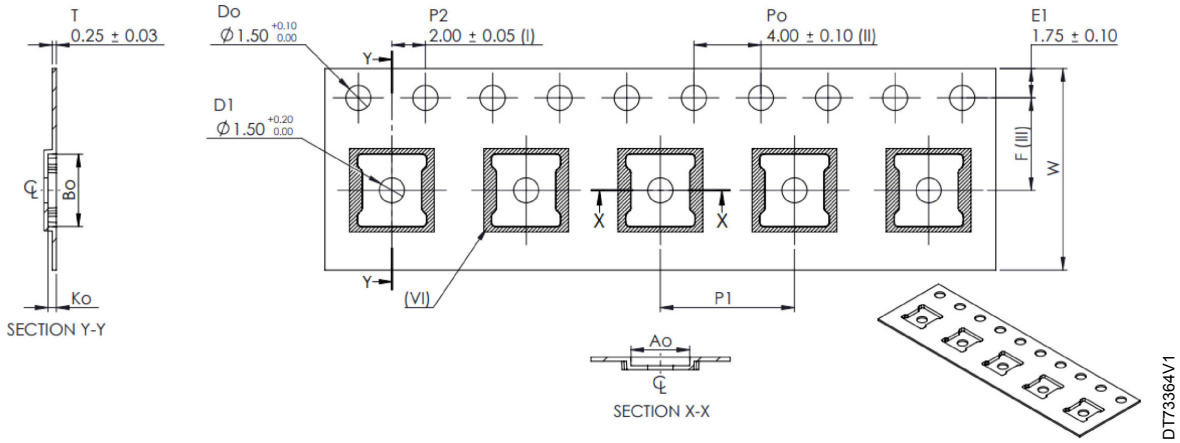


Figure 32. Embossed carrier tape for XDFN3 4 x 3.2 x 0.35



1. *Measured from center line of sprocket hole to center line of pocket (I)*
2. *Cumulative tolerance of 10 sprocket hole pitch = ± 0.20 (II).*
3. *Measured from center line of sprocket hole to center line of pocket (III)*
4. *Other materials available*
5. *Dimension with () is used for design reference purposes. No measurement required*
6. *Shinning imprint (It occurs in all pockets) (VI)*
7. *SPOT patented by C_PAK*

Note: The roman numerals in brackets refer to specific notes in Figure 32

Table 19. Carrier tape dimensions for XDFN3 4 x 3.2 x 0.35

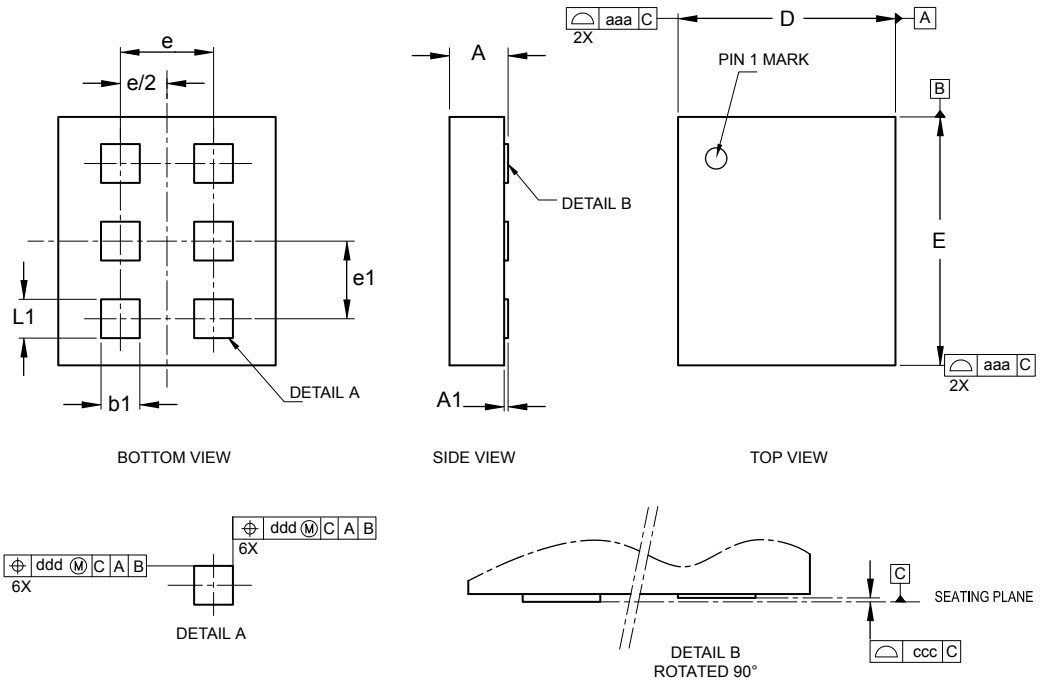
Package	A0	B0	K0	F	P1	W	Unit
XDFN3 4 x 3.2 x 0.35 mm	3.50 ± 0.10	4.30 ± 0.10	0.50 ± 0.10	5.50 ± 0.05	8.00 ± 0.10	12.00 +0.30 / -0.10	mm

6.3 GQFN6 package specification

6.3.1 X2F-PSON6 package information (B0G5)

This X2F-PSON is a 6-lead , 1.4 x 1.6 mm, plastic ultra and super thin small outline, non-leaded package.

Figure 33. **X2F-PSON6 - Outline**



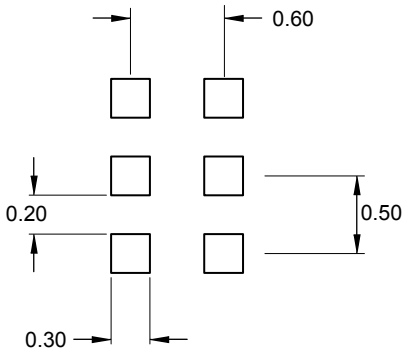
1. *Drawing is not to scale.*

Table 20. **X2F-PSON - Mechanical data**

Symbol	millimeters			inches[1]		
	Min	Typ	Max	Min	Typ	Max
A[2]	0.35	-	0.40	0.014	-	0.016
A1	0	-	0.05	0	-	0.002
L1	0.20	0.25	0.30	0.007	0.009	0.012
b1	0.20	0.25	0.30	0.007	0.009	0.012
D	1.40 BSC			0.055 BSC		
E	1.6 BSC			0.063 BSC		
e	0.60 BSC			0.024 BSC		
e1	0.50 BSC			0.020 BSC		
N[3]	6					
aaa	-	0.05	-	-	0.002	-
ccc	-	0.03	-	-	0.001	-
ddd	-	0.10	-	-	0.004	-

1. *Values in inches are converted from mm and rounded to 4 decimal digits.*
2. • *X2F-PSON stands for plastic ultra and super thin small outline, non-leaded package family*
   • *Super thin profile: 0.30 mm < A ≤ 0.40 mm*
3. *Total number of terminals*

Figure 34. **X2F-PSON6 - Footprint example**

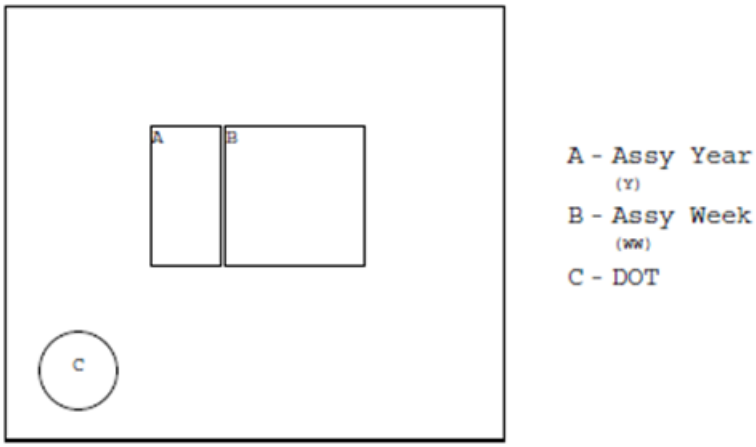


1. *Dimensions are express in mm.*

6.3.2 X2F-PSON6 package marking

The following figure shows the device marking for the X2F-PSON6 package.

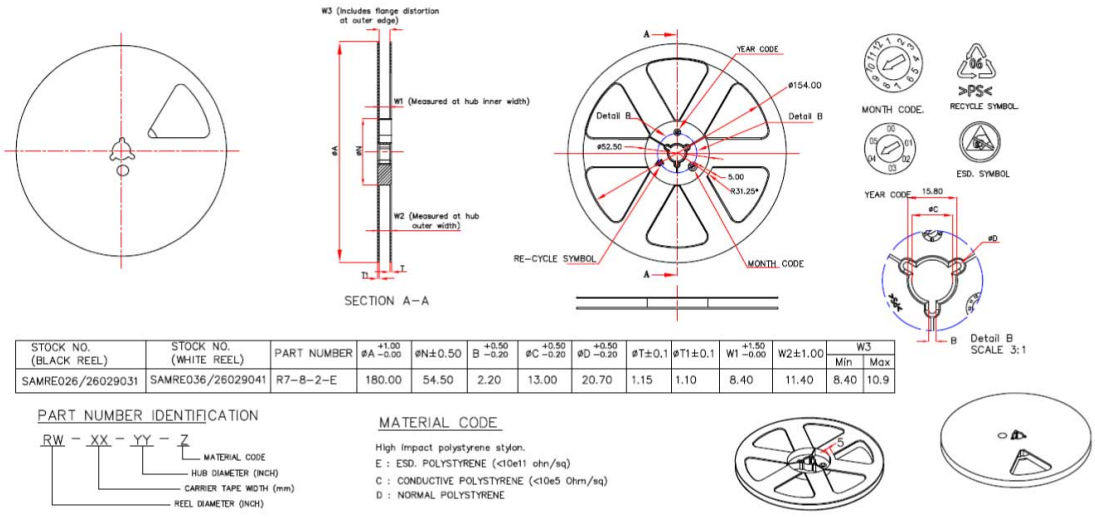
Figure 35. **X2F-PSON6 package marking**



6.3.3 X2F-PSON6 tape and reel packing

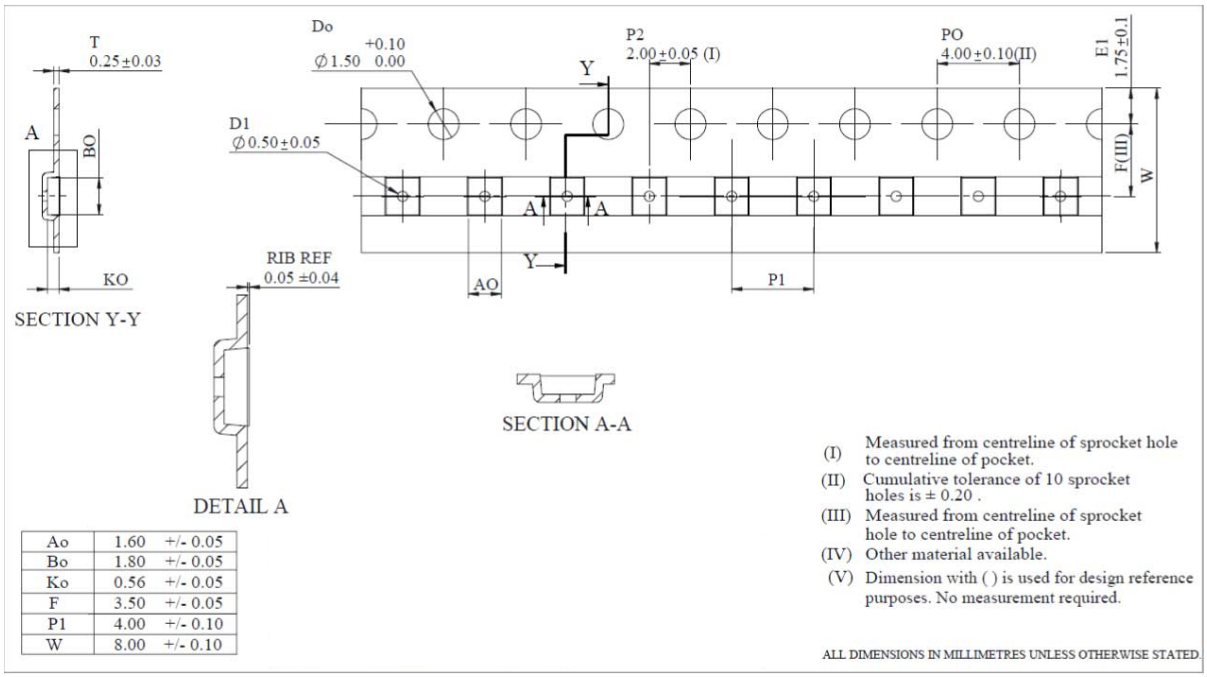
X2F-PSON6 packages can be supplied with tape and reel packing. The reels have a 7 inches typical diameter. They contain 5000 devices each.

Figure 36. **Dimensions of a 7" reel for 8 mm tape**



STOCK NO. (BLACK REEL)	STOCK NO. (WHITE REEL)	PART NUMBER	øA +1.00 −0.00	øN±0.50	B +0.50 −0.20	øC +0.50 −0.20	øD +0.50 −0.20	øT±0.1	øT1±0.1	W1 +1.50 −0.00	W2±1.00	W3 Min	W3 Max
SAMRE026/26029031	SAMRE036/26029041	R7–8–2–E	180.00	54.50	2.20	13.00	20.70	1.15	1.10	8.40	11.40	8.40	10.9

Figure 37. **Embossed carrier tape for X2F-PSON6**



Ao	1.60	+/- 0.05
Bo	1.80	+/- 0.05
Ko	0.56	+/- 0.05
F	3.50	+/- 0.05
P1	4.00	+/- 0.10
W	8.00	+/- 0.10

7 Ordering information

Example: STSAFL010 DF YY XXX

Product name

STSAFL010

Package codification

DF = UFDFPN8

F6 = GQFN6

F3 = GQFN3

Customer ID

XXX = Customer identification

Personalization revision code

YY = Personalization setup

Note: For a list of available options (speed, package, etc.) or for further information on any aspect of this device, please contact your nearest STMicroelectronics sales office.

Revision history

Table 21. **Document revision history**

Date	Revision	Changes
01-Jul-2025	1	Initial release.
04-Jul-2025	2	Minor change.

Glossary

AC Access condition

ACK Acknowledge

CA Certification Authority

CF Command frame

ECC Elliptic curve cryptography

FAck Frame acknowledge

I/O Input/output

ID Identity

I²C Inter-integrated circuit

LSB Least significant byte

MAC Message authentication code

MCU Microcontroller unit

MSB Most significant byte

NACK Not acknowledge

NVM Nonvolatile memory

OS Operating system

POR Power-on reset

R-MAC Response message authentication code

ROM Read-only memory

RTOS Real-time operating system

SE Secure element

SOF Start of frame

Contents

List of tables

List of figures