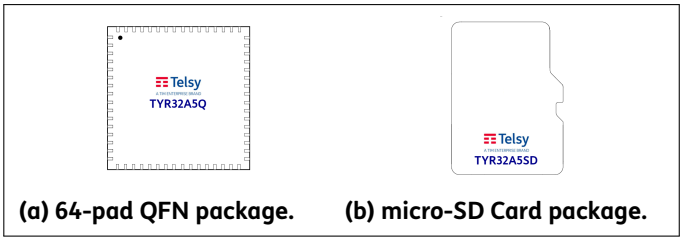
TYR32A5Q/SD
Secure Microchip

The TYR32A5Q/SD offers a comprehensive and integrated secure element solution and it is able to provide multiple security features in order to protect IoT and dependable systems, providing a wide portfolio of standard cryptographic functions, allowing cryptographic-grade key generation and encrypted storing of key credentials.



(a) 64-pad QFN package. **(b) micro-SD Card package.**

Figure 1: TYR32A5Q/SD available packages.

System Specifications

- 32-bit RISC-V with Lockstep processor
- Internally generated clock at 166 MHz
- DMA controller to speed-up data transfer:
  - 32-bit data transfer width
  - 16 channels
  - supports burst operations (1, 4, 8 or 16 transactions)
- 4 general purpose I/O ports with programmable pull-up

Format

The TYR32A5Q/SD is available in two formats:

- 64-pad QFN (Q)
- micro-SD Card (SD)

Hardware-Assisted Security Functions

- Keccak-based AEAD Key Manager, supporting split-knowledge and HPC2 protection scheme against side-channel attacks
- PUF enforced root-of-trust
- True Random Number Generator (TRNG) with cryptographic post-processing
- AES-ECB/CBC with 128/256-bit key
- AES-GCM 256-bit key
- AES ECB/CTR/CCM/CMAC, protected against side-channel attacks with HPC2 protection scheme
- RSA supporting up to 8192-bit keys, based on the PKCS#1 v2.2 RSA Cryptography Standard
- ECDH
- ECDSA, curve's field size up to 640-bit
- SHA-256
- HMAC 256-bit key
- KMAC, supported output lengths (in bits): 128, 224, 256, 384, 512
- SHA3: SHA3-224/-256/-384/-512
- SHAKE-128/256 and cSHAKE-128/-256
- Crystals-Kyber (Kyber-512/-768/-1024) key gen./encapsulation/decapsulation with hardware-based NTT accelerator on prime q=3329 (supported operations FNTT/INTT/PWM2)

Physical Protections

- Protection against various kind of side-channel attacks (power, electromagnetic and timing)
- Multi-level fault attacks protection, acting at logical and physical level:
  - active shield for anti-tampering and anti-probing
  - digital sensor to provide protection against laser, voltage, temperature fault injection attacks
  - lockstep processor for redundancy checks
- Internally generated clock with configurable jitter:
  - no external control of the clock
  - phase instability to provide protection against physical attacks

Memory

- 128kB code RAM
- 128kB data RAM
- System-in-Package 1MB flash for encrypted and authenticated storage
- 128-bit user-available One-Time Programmable (OTP) memory

Telsy S.p.A.
Corso Svizzera 185 Torino (Italy), 10149
secure-microchip@telsy.it

Interfaces

- Standard SDIO target interface, supporting up to SDR25
- x2 I^2C controller/target interfaces*
- x2 UART interfaces*
- x2 SPI controller/target interfaces*, supporting also controller-only QSPI mode

Power and Reset

- Wide range of supported power supply voltage and I/Os:
  - from 1.62V to 3.6V
  - 3.3V and 1.8V SDIO signaling mode supported
- Programmable clock-gating unit to save power on hardware accelerators
- Embedded capless LDO
- On-chip Power-On-Reset
- 84mW of peak power consumption

* available on the QFN format only.

Contents

Description

The TYR32A5Q/SD offers a comprehensive and integrated secure element solution. The TYR32A5Q/SD is able to provide multiple security features in order to protect IoT and dependable systems, guaranteeing confidentiality, authenticity and non-repudiation. It provides a wide portfolio of standard cryptographic functions, such as encryption/decryption, sign/verify, as well as post-quantum key exchange mechanism. The TYR32A5Q/SD guarantees cryptographic-grade generation and encrypted storing of key credentials, offering a flexible solution for implementing, for example:

- integrated root-of-trust
- trusted middleware
- key management unit
- hardware security module

The outstanding flexibility of the TYR32A5Q/SD makes it a perfect platform to easily deploy security enforcement in various scenarios from large systems to IoT applications. It offers a huge number of connection interfaces, such as SPI/QSPI, I^2C, UART and SDIO, all SCP-03 enabled to guarantee secure communication with other devices.

The TYR32A5Q/SD has been designed with top-notch protection and anti-tampering mechanisms, to protect the device against a wide set of invasive and non-invasive attacks. Its lifecycle is enforced cryptographically, to guarantee protection from misuse and unauthorized use.

The TYR32A5Q/SD comes in two different form factors: QFN, to be implemented in custom applications, and a standard micro-SD package, to ease the integration in already-existent systems.

Architecture

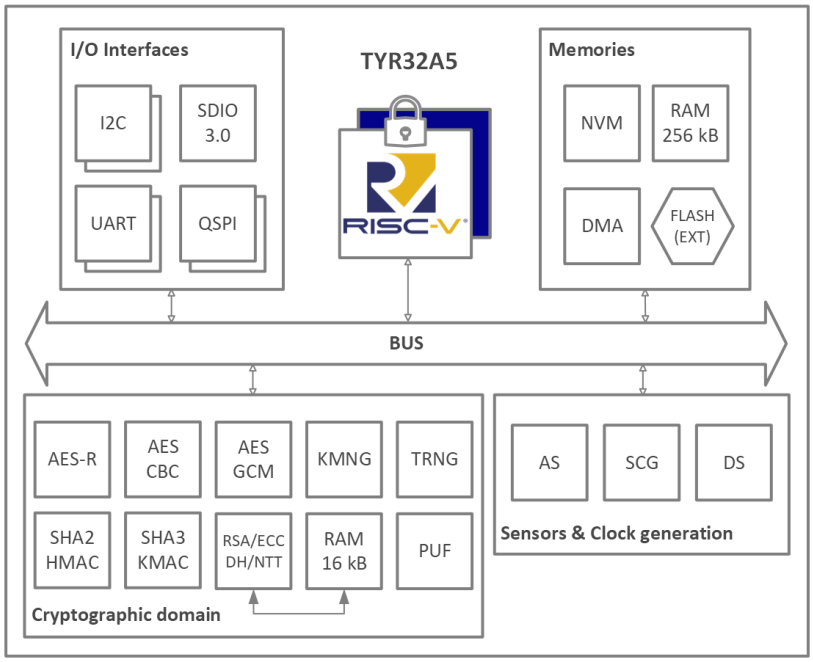


Figure 2: TYR32A5Q Block Diagam

Features

The security architecture of the system is built around the Key Manager that is the key wrapper, authenticator and distributor of the system. The Key Manager uses the Unique Root Key (URK) to unwrap and authenticate all the other keys. Only the Key Manager has physical access to the URK. The URK is unknown, unique and it depends on the PUF and other random non volatile parameters self-generated during the production process.

Table 1: Cryptographic Primitives

Cryptographic Primitive	Attributes	Notes
AES Modes (AES-256 only)	EBC, CBC, GCM, CCM, CTR	
RSA	Up to 8192-bit	
ECC	ECDSA, ECDH	
NTT	FNTT/INTT/PWM2 with q=3329	Crystals-Kyber
MAC	HMAC, KMAC, CMAC	
Hash&XOF	SHA-256, SHA3-256/384/512, SHAKE-256/512, cSHAKE	
KDF	KDF-SHA-256, KDF-SHA3, HKDF, KDF-KMAC	
PUF	256-bit entropy	Root-of-trust
TRNG	Cryptographic post-processing	

Table 2: Security Features

Countermeasures	Protection	Description
Lock-step Core	FI	Detection of faults on the main processor
Digital Sensor	FI	On-chip sensor for voltage and temperature sensing
Secure Clock	SCA/FI	Internal-only clock source with additional jitter
Active Shielding	FI	Anti-tamper and anti-probing protection
Key Manager	SCA	SCA-secured key management
AES-R	SCA	SCA-secured secure boot

Table 3: I/O features.

Type	Characteristics	Instance(s)	Details
QSPI*	up to 12.5Mbps	2	SPI Controller/Device, QSPI Controller-only.
I^2C*	up to 400kbps	2	Controller/Device.
UART*	up to 115.2kbps	2	
SDIO	up to SDR25	1	Compatible with 1.8V/3.3V SDIO voltage modes and with SPI-mode.

* Available on the QFN version only.

Electrical Specifications

The TYR32A5Q/SD is designed to work at two nominal power supply voltages, namely 1.8V and 3.3V.

Table 4: Electrical specifications.

Parameter	Symbol	Min.	Typ.	Max.	Unit	Conditions
Power Supply	V_{DD}	1.62	1.8/3.3	3.6	V	
Input/Output Voltage	V_{IO}	1.62	1.8/3.3	3.6	V	$-40^{\circ}C \leq T_A \leq 85^{\circ}C$
Power consumption[1]	P_C		73.5	84	mW	

[1] Based on engineering data, not yet tested in production.

Secure Bootloader Chain

This section will concisely present the provided secure boot loader mechanisms and configurations. The TYR32A5Q/SD bootloading chain is a two stages process:

1. First-stage bootloader: ROM Secured Bootloade (RSB)
2. Second-stage bootloader: Operational Secured Bootloader (OSB)

The Secure bootloader chain is depicted in Figure 3.

The first-stage bootloader is ROM based. Using a unique factory key K_{RSB}, it decrypts and authenticates the second-stage bootloader named Operational Secure Bootloader (OSB).

The second-stage bootloader is configurable by the application developer with dedicated secured mechanisms and APIs (see Table 6). The OSB authenticates and decrypts the user custom application named Operational Secure Application (OSA). The configurable keys used by the OSB provides secure management and OSA decryption, authentication and signature verification. See Table 5 for a brief overview of the OSB keys.

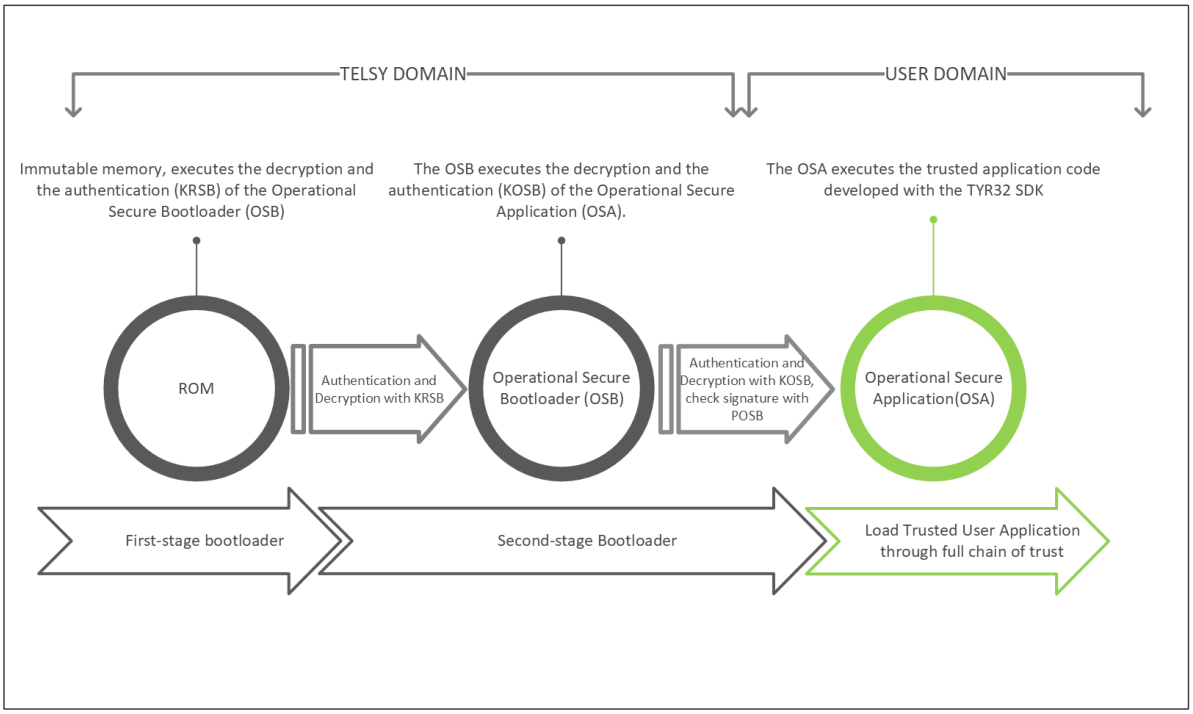


Figure 3: TYR32A5Q Secure Bootloader Chain

Table 5: Secure Boot Keys

Key	Owner	Type	Function
K_{RSB}	Telsy	AES256-CCM	First-stage secure bootloader authenticated encryption key
K_{OSB}	User	AES256-CCM	Second-stage secure boot authenticated encryption key
P_{OSB}	User	ECDSA p256	Second-stage secure boot signature verification key
UMK	User	AES256-CCM	User Management Key for configuration and secure image injection

ROM Secured Bootloader

As stated above, the TYR32A5Q/SD boot-ROM uses the K_{RSB} to provide both decryption and authentication of the Operational Secured Bootloader (OSB). The OSB image is stored in the in-package external secure flash memory. The secure boot process relies on the SCA-resilient Key Manager and the AES-R. From a cryptographic perspective, the security of this operation is guaranteed by the Unique Root Key (URK).

Operational Secured Bootloader

The second-stage bootloader uses the K_{OSB} to decrypt the user image OSA. Image authentication can be configured to be either based on symmetric cryptography with a MAC (CCM obtained using K_{OSB}), or using asymmetric cryptography by means of the public key P_{OSB}. Regarding OSA image authentication, an additional option to support Post-Quantum Cryptography (PQC) based on Crystals-Dilithium is on the roadmap. The secure boot process relies on the SCA-resilient Key Manager and AES-R. Again, from cryptographic perspective, the security of this operation is guaranteed by the Unique Root Key (URK). Finally, also the OSA image is stored in the in-package external secure flash memory.

Table 6: Operational Secured Bootloader - Secured Management APIs

API-CODE	FUNCTION	PARAMETERS	DESCRIPTION
$UPDATE_{UMK}$	command to update UMK	None	Command is encrypted and authenticated with UMK
$CONF_{OSB}$	command to configure the boot options	$PAR_0=BOOT_{MODE}$; $PAR_1=K_{OSB}$; $PAR_2=P_{OSB}$	Command is encrypted and authenticated with UMK
$LOAD_{OSA}$	command to load the OSA image	None	Command is encrypted and authenticated with UMK

Operational Secured Application SDK

In this section we briefly describe the main characteristics of the Operational Secure Application SDK and tools. These development tools are provided for a Linux-based host environment. The OSA is a custom application developed in C language by the end application developer and by using a simple Makefile approach together with a a set of provided pre-compiled libraries. Several OSA examples are provided as part of the framework. Finally, an additional tool is provided to configure the OSB and inject the OSA image. More details follows.

OSA Compilation Tools

The OSA Compilation tools elements are:

- Compiled libraries package: includes all pre-compiled Hardware Abstaction Layer (HAL) libraries to develop the custom OSA.
- Portable Linux-based application for template project creation including many example projects.

OSA Injection Tool

The OSA Injection Tool is a portable Linux-based application that provides:

- OSA Wrapper Tool: securely encrypts and signs the compiled OSA image with the user configured keys (K_{OSB} and P_{OSB}).
- Secured Management APIs: interacts with the OSB to configure the TYR32A5Q/SD, to allow the updating of the OSA image and user keys (see Table 6).

Secured External Flash Memory

The TYR32A5Q/SD's System-in-Package embeds an external flash memory that securely stores the OSB and OSA images as well as most of the management and boot keys. From an OSA perspective, it can be used to securely store a large number of application specific keys and data-objects. The provided file system is designed to ensure wear leveling. All objects stored in the flash are encrypted and authenticated using keys whose protection is guaranteed by the system Unique Root Key (URK). The URK further guarantees a tight coupling between the flash and the core device. Each flash is in fact cryptographically bonded to a specific device during the production phase.

The secure storage of user application keys, as well as the storage of generic data objects, relies on two specific APIs:

- Native Wrapped Key (NWK): stores both symmetric and asymmetric keys natively wrapped by the Key Manager and using the UMK.
- Cryptographic Data Object (CDO): stores generic information, guaranteeing confidentiality and authenticity for data-at-rest. CDO embeds a NWK used to protect the data payload part of the object.

Package Information

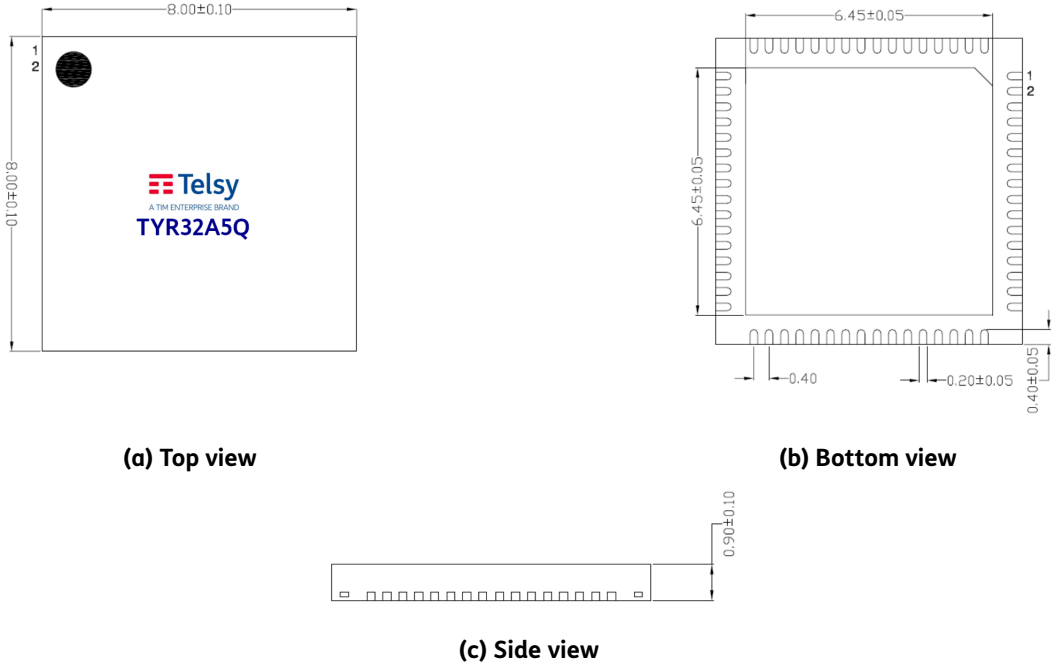
The TYR32A5Q/SD is available in two packages:

- TYR32A5Q: 64-pad QFN;
- TYR32A5SD: standard micro-SD.

All measures in this section are in mm.

TYR32A5Q Package

The TYR32A5Q is packaged in a 64-pad QFN 8x8mm with 40µm pitch and it is depicted in Figure 4.



(a) Top view

(b) Bottom view

(c) Side view

Figure 4: TYR32A5Q package outline drawing.

TYR32A5SD Package

The TYR32A52SD is packaged in a standard micro-SD format. The mechanical outline is shown in Figure 5.

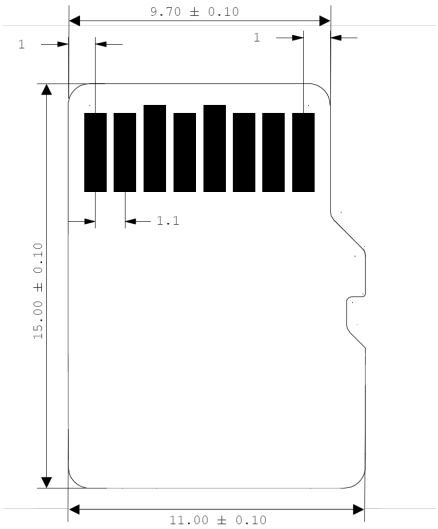


Figure 5: TYR32A5SD package outline drawing.

Pins

TYR32A5Q Pins

The pinout of the QFN version is shown in Figure 6 and described in Table 7. Note that the central pad on the bottom of the QFN package provides ground connection. To ensure the minimization of the impedance to ground of the device, the central pad must to be connected to the ground plane.

TYR32A5SD Pins

The pinout of the micro-SD version is described in Table 8.

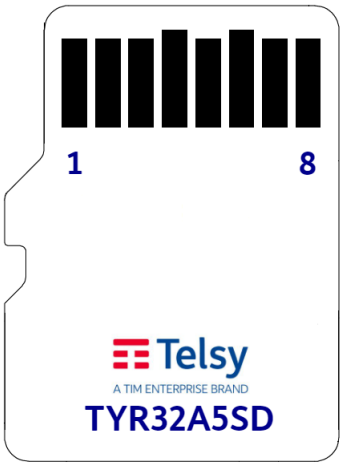


Figure 7: Bottom view of the micro-SD package.

Table 7: QFN-64 package pinout.

Name	QFN Pin	Function	Name	QFN Pin	Function
NC	1	Not connected	NC	33	Not connected
I2C0_SDA	2	I^2C-0 data line	GND	34	Ground
I2C0_SCL	3	I^2C-0 clock line	VDD	35	Power supply
I2C1_SDA	4	I^2C-1 data line	NC	36	Not connected
I2C1_SCL	5	I^2C-1 clock line	NC	37	Not connected
VDD	6	Power supply	GND	38	Ground
SDIO_DAT2	7	SDIO data line 2	NC	39	Not connected
SDIO_DAT3	8	SDIO data line 3	NC	40	Not connected
GND	9	Ground	NC	41	Not connected
SDIO_CMD	10	SDIO command line	NC	42	Not connected
VDD	11	Power supply	VDD	43	Power supply
SDIO_CLK	12	SDIO clock line	RESET_N	44	System reset (active low)
GND	13	Ground	NC	45	Not connected
SDIO_DAT0	14	SDIO data line 0	NC	46	Not connected
SDIO_DAT1	15	SDIO data line 1	NC	47	Not connected
VDD	16	Power supply	NC	48	Not connected
VDD	17	Power supply	GND	49	Ground
QSPI1_SIO0	18	QSPI-1 SIO0 and SPI-1 MOSI	VDD	50	Power supply
QSPI1_SCK	19	QSPI-1/SPI-1 Clock	NC	51	Not connected
GND	20	Ground	UART0_TX	52	UART-0 TX
QSPI1_SS0	21	QSPI-1 SS0 and SPI-1 CSN	UART0_RX	53	UART-0 RX
QSPI1_SIO1	22	QSPI-1 SIO1 and SPI-1 MISO	UART1_TX	54	UART-1 TX
VDD	23	Power supply	UART1_RX	55	UART-1 RX
QSPI1_SIO2	24	QSPI-1 SIO2	QSPI2_SIO0	56	QSPI-2 SIO0 and SPI-2 MOSI
QSPI1_SIO3	25	QSPI-1 SIO3	QSPI2_SCK	57	QSPI-2/SPI-2 Clock
GPIO_0	26	GPIO-0	QSPI2_SS0	58	QSPI-2 SS0 and SPI-2 CSN
GPIO_1	27	GPIO-1	VDD	59	Power supply
GPIO_2	28	GPIO-2	QSPI2_SIO1	60	QSPI-2 SIO1 and SPI-2 MISO
GPIO_3	29	GPIO-3	QSPI2_SIO2	61	QSPI-2 SIO2
VDD	30	Power supply	QSPI2_SIO3	62	QSPI-2 SIO3
GND	31	Ground	NC	63	Not connected
GND	32	Ground	NC	64	Not connected
GND	Pad	Ground			

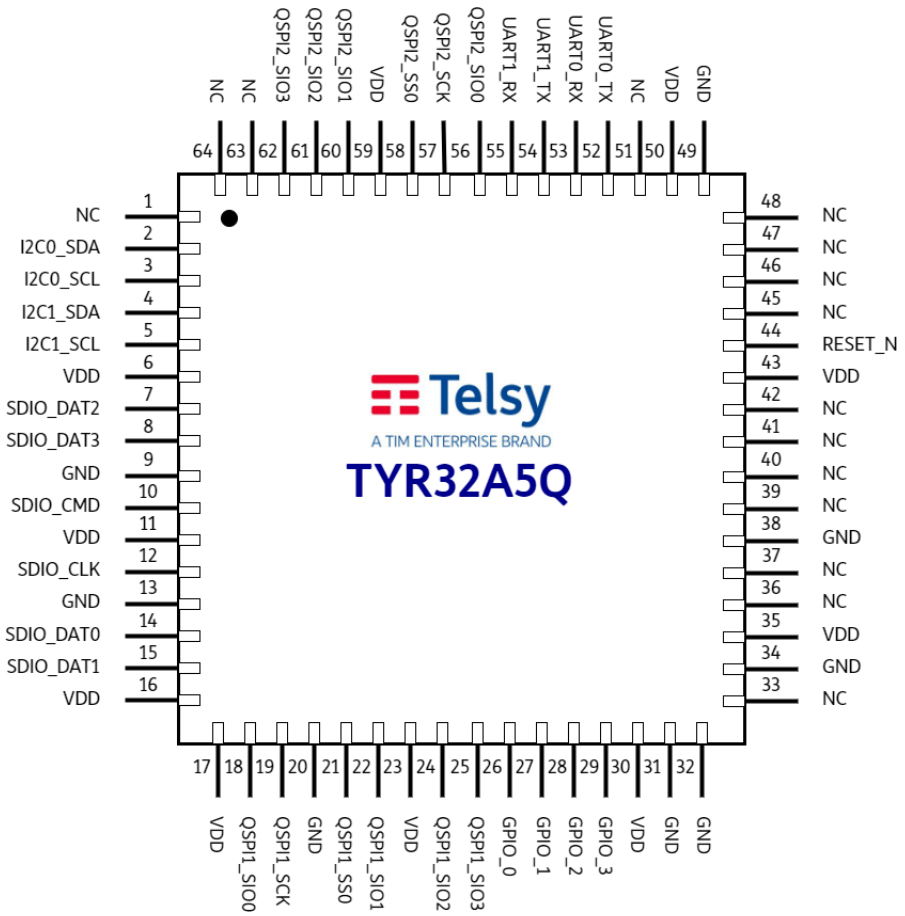


Figure 6: QFN-64 package pinout.

Table 8: SDIO pad description

Name	Pad	SDIO Function	SPI Function
SDIO_DAT2	1	Bi-directional SDIO data line	Not used
SDIO_DAT3	2	Bi-directional SDIO data line	CS
SDIO_CMD	3	SDIO command line	Data Input
VDD	4	Power supply	Power supply
SDIO_CLK	5	SDIO clock line	SCK
VSS	6	Ground	Ground
SDIO_DAT0	7	Bi-directional SDIO data line	Data Output
SDIO_DAT1	8	Bi-directional SDIO data line	Not used

Disclaimer

Telsy S.p.A.
Corso Svizzera 185 Torino (Italy), 10149
secure-microchip@telsy.it