MF4SAM3

MIFARE SAM AV3 secure access module

Rev. 3.0 — 2 August 2019
561930

Product short data sheet
COMPANY PUBLIC

1 General description

The NXP MIFARE SAM AV3 secure hardware solution is the ideal add-on for reader devices offering additional security services. Supporting DES, TDEA, AES and RSA capabilities, it offers secure storage and secure communication in a variety of infrastructures.

Unlike other products in the field, MIFARE SAM AV3 has proven interoperability with all of NXP's broad card and RFID product portfolio, (MIFARE, NTAG DNA, ICODE DNA, UCODE DNA and SmartMX product families), making it the most versatile and secure SAM solution on the market today.

The MIFARE SAM AV3 is built on NXP's SmartMX2 P60 secure smart card controller with CC EAL6+ certification. Its software implementation is evaluated and composite certified by the MIFARE Security Evaluation Scheme. Similar to the hardware CC evaluation, the MIFARE Scheme also evaluates against high attack potential. Hence, systems using MIFARE SAM AV3 are reassured with the state-of-the-art security measures adopted by the industry.

Programmable Logic

The MIFARE SAM AV3 is equipped with a new Programmable Logic functionality which allows customers to flexibly create their business logic on the SAM. This new functionality opens up many new possibilities with the creation of project-specific customization such as a new key diversification algorithm, a new secure messaging, or a new secure storage.

X-mode communication

When used in combination with a reader IC supporting innovative "X" features, MIFARE SAM AV3 provides a significant boost in performance to the reader along with faster communication between reader and module. The "X" feature is a new way to use the SAM in a system, with SAM connected to the microcontroller and the reader IC simultaneously.

Secured communication

The connection between the SAM and the reader is performed using security protocols based on either AES symmetric cryptography or PKI RSA asymmetric cryptography. The protocols comply with the state-of-art standards and thereby ensure data confidentiality and integrity.

2 Features and benefits

2.1 Cryptography

- Supports MIFARE Crypto1, DES, TDEA (112 and 168 bits), AES (128, 192 and 256 bits), RSA (up to 2048 bits) and ECC (up to 256 bits) cryptography
- Supported NXP's products:
  - MIFARE DESFire, MIFARE DESFire EV1, MIFARE DESFire EV2
  - MIFARE Plus, MIFARE Plus EV1
  - MIFARE Classic, MIFARE Classic EV1
  - MIFARE Ultralight EV1, MIFARE Ultralight C
  - MIFARE DESFire Light
  - NTAG DNA
  - ICODE DNA
  - UCODE DNA
- Secure storage and updating of keys
  - 128 key entries for symmetric cryptography
  - 3 RSA key entries for asymmetric cryptography
  - 8 ECC public key entries for signature verification
  - 4 ECC curves entries
  - 48 EMV CA public key entries (supports 8 RID minimum)
- SHA-1, SHA-224 and SHA-256 hashing computation
- TDEA and AES-based key diversification
- Generic cryptography commands for user-defined schemes
- Supports EMVCo terminal functionality
- True random number generator (TRNG) compliant to AIS-31

2.2 Communication

- ISO/IEC 7816 (part 2 and 3) contact interface
  - Support Class A, B and C operating condition
  - Support ISO/IEC 7816 baud rates
  - Support high-speed baud rates up to 1.5 Mbit/s
- Optional I2C slave mode host interface (only available on HVQFN package)
- Communication protocol compliant with ISO/IEC 7816-3 T=1 protocol
- Up to four logical channels; simultaneous multiple card support
- Support for MIFARE DESFire and MIFARE Plus authentication (with related secure messaging and session key generation)
- Secure Host to SAM and back end to SAM communication with symmetric cryptography including 3-pass authentication for confidentiality and integrity
- Secure Host to SAM and back end to SAM communication with RSA-based cryptography for key updating
- X-mode direct interface with NXP's contactless reader ICs (RC663, RC52x, PN512)

2.3 Programmable logic (restricted feature) [2]

- Up to 32 kB of code and data in EEPROM for user customized functionality
- 1 kB of RAM for user's dynamic data
- Internal Host access to all MIFARE SAM AV3 commands

2.4 Security evaluation and certification

- CC EAL6+ certified hardware platform (based on NXP's SmartMX2 P6022y VB)
- Composite certified with MIFARE Security Evaluation Scheme (Equivalent to EMVCo Security Evaluation)
  (Evaluation lab: TÜViT, Certification lab: UL)
- FIPS140-2 CAVP certified

2.5 New features

This section gives an overview of the new features compared to MIFARE SAM AV2. Please see [1] for details.

- All new features from MIFARE DESFire EV2 requiring cryptographic operations. This includes EV2 secure messaging and Transaction MAC support (incl CommitReaderID).
- All new features from MIFARE Plus EV1 requiring cryptographic operations. This includes EV1 secure messaging, Transaction MAC support (incl CommitReaderID) and Sector Security Level Switching.
- New Virtual Card Selection and Proximity Check protocols.
- Post-Delivery Configuration support.
- MIFARE Ultralight EV1 password authentication.
- AES authentication according to ISO/IEC 29167-10 for UCODE and ICODE support.
- LRP support for DESFire secure messaging, as supported by DESFire Light and NTAG42x(TT) and for Offline Crypto operations.
- ECC originality signature verification as supported by all recent MIFARE products.
- Generic CMAC-based key derivation for a.o. Transaction MAC session key generation and (e.g. UCODE) key diversification.
- Fine-grained key access control.
- EMV terminal support for certificate verification, offline authentication and pin code verification.
- Programmable Logic feature to allow customized business logic and a.o. key diversifications to be run within the SAM.
- Personalization SAM feature to generate cryptogram to export keys for injection in another SAM for AES variant and for RSA variant.
- AES-256 support for Offline Crypto and SAM-Host protection.
- RSA OAEP encryption and decryption.
- ATR configuration.
- I2C slave interface in addition to ISO/IEC 7816 interface (for HVQFN only).

---

2 **Note: The PL code uploading functionality is only available to a limited set of customers.**

3 Ordering information

Table 1. Ordering information

Type number	Package		
	Name	Description	Version
MF4SAM3X84/9BA6AU	PCM1.5	contact chip card module (super 35 mm tape format, 8 contact), minimum order quantity: 11.900	SOT658-1
MF4SAM3X84/9BA6AUS	PCM1.5	contact chip card module (super 35 mm tape format, 8 contact), minimum order quantity: 1.000	SOT658-1
MF4SAM3HN/9BA6AU	HVQFN32	plastic thermal enhanced very thin quad flat package; no leads; 32 terminals; body 5 x 5 x 0.85 mm; reel pack; minimum order quantity: 6.000	SOT617-3
MF4SAM3U15/9BA6AU	wafer	150 mm thickness sawn wafer on film frame carrier (FFC)	NAU000

4 Block diagram

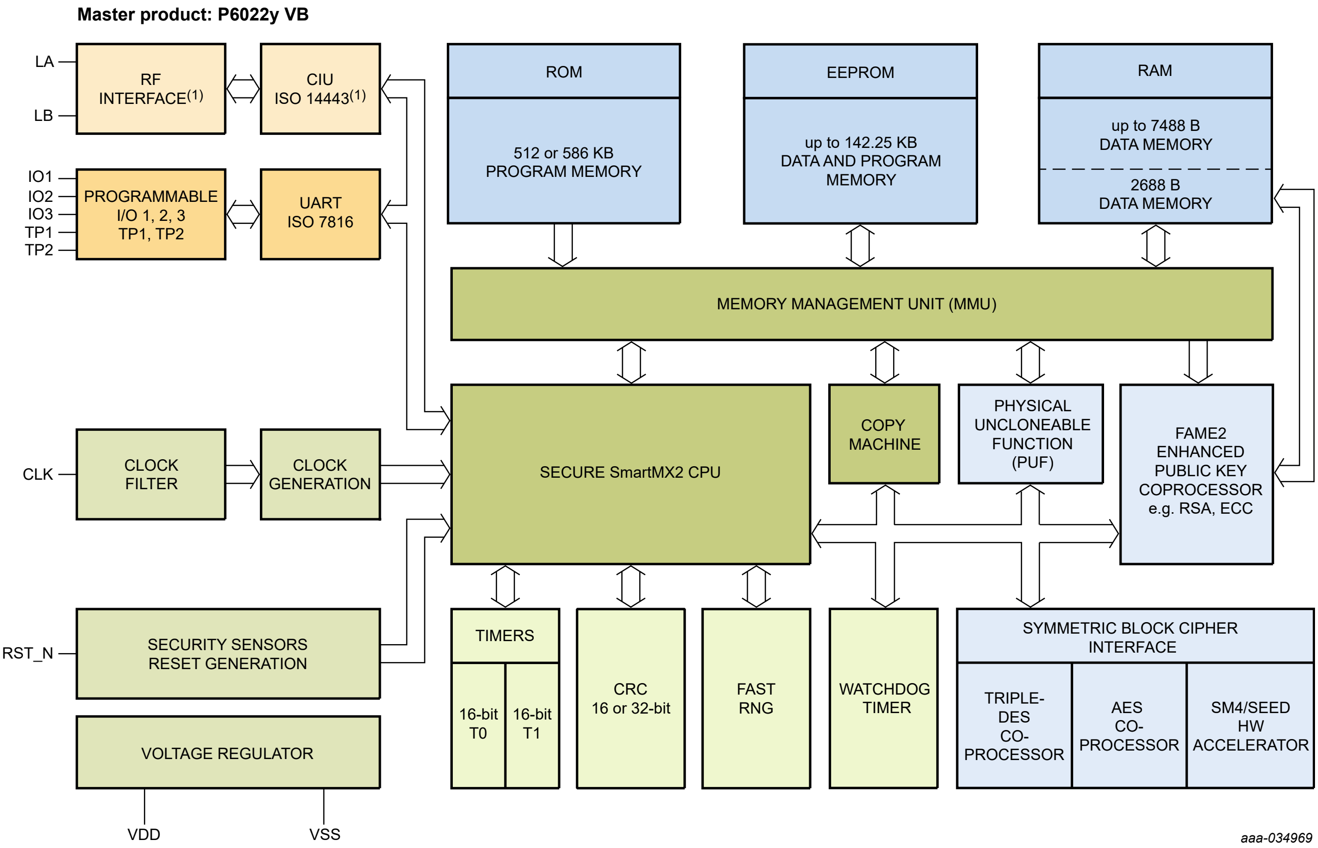


Figure 1. Block diagram

5 Pinning information

5.1 Pin description

5.1.1 PCM1.5 pin configuration

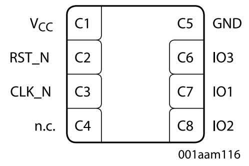
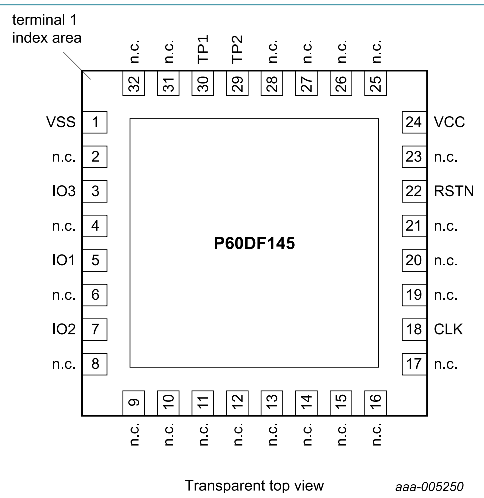


Figure 2. Pin configuration PCM1.5

Table 2. Pin description PCM 1.5 MIFARE SAM AV3

ISO 7816		MIFARE SAM AV3		
Pad	**Symbol**	**Symbol**	**Pad**	**Description**
C1	VCC	V_{CC}	C1	power supply voltage input
C2	RST	RST_N	C2	reset input, active LOW
C3	CLK	CLK_N	C3	clock input
C4	reserved	n.c.	C4	n.c.
C5	GND	GND	C5	ground (reference voltage) input
C6	VPP	IO3	C6	used for I2C communication to RC (SCL)
C7	IO1	IO1	C7	input/output for serial data (host communication)
C8	reserved	IO2	C8	used for I2C communication to RC (SDA)

5.1.2 HVQFN32 pin configuration



Remark: Central pad is isolated.

Figure 3. Pin configuration HVQFN32

Table 3. Pin description HVQFN32 MIFARE SAM AV3

Pad	Symbol	Description
1	GND	ground (reference voltage) input
3	IO3	used for I2C communication to RC (SCL)
5	IO1	input/output for serial data (ISO7816 or SDA_Slave for I2C host communication)
7	IO2	used for I2C communication to RC (SDA)
24	VCC	power supply voltage input
22	RST_N	reset input, active LOW
18	CLK_N	clock input
29	TP2	SCL_Slave: used for I2C communication to Host when I2C host communication is enabled
30	TP1	I2C_Enable: enable I2C host communication when high

6 Limiting values

Table 4. Limiting values

In accordance with the Absolute Maximum Rating System (IEC 60134). Voltages are referenced to VSS (ground = 0 V).

Symbol	Parameter	Conditions		Min	Max	Unit
$V_{DD(AMR)}$	supply voltage			-0.5	+6.0	V
$V_{I(AMR)}$	input voltage	any signal pad		-0.5	V_{DD} +0.5	V
$I_{I(AMR)}$	input current	pads IO1, IO2, IO3 and TP1, TP2[1]		-	± 15.0	mA
I_O	output current	pads IO1, IO2, IO3 and TP1, TP2[1]		-	± 15.0	mA
I_{lu}	latch-up current	V_I < 0 V or V_I > V_{DD}		-	± 100	mA
V_{esd}	electrostatic discharge voltage (HBM)	pads VDD, VSS, CLK, RST_N, IO1, IO2, IO3	[2]	-	± 4.0	kV
		TP1, TP2	[3]	-	± 2.0	kV
	electrostatic discharge voltage (CDM)	all pads	[4]	-	± 500	V
P_{tot}	Total power dissipation		[5]	-	1	W
T_{stg}	Storage temperature		[6]	-55	125	℃

[1] If IO2 and IO3 are available.
[2] In accordance with ANSI/ESDA/JEDEC JS-001-2011, ESDA/JEDEC Joint Standard for Electrostatic Discharge Sensitivity Testing - Human Body Model (HBM) - Component Level.
[3] Only available if enabled via OEF setting.
[4] In accordance with JEDEC JESD22-C101 for Charged-Device Model (CDM).
[5] Depending on appropriate thermal resistance of the package.
[6] Depending on delivery type, refer to *NXP Semiconductors General Specification for 12" Wafers* (15) and to *NXP Semiconductors Contact & Dual Interface Chip Card Module Specification* (16).

CAUTION

This device is sensitive to ElectroStatic Discharge (ESD). Observe precautions for handling electrostatic sensitive devices.
Such precautions are described in the *ANSI/ESD S20.20, IEC/ST 61340-5, JESD625-A* or equivalent standards.

7 Recommended operating conditions

Table 5. Operating conditions

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
V_{DD} (5.0)	Supply voltage [1]	Class A/5 V nominal supply voltage contact interface operation	4.5	5.0	5.5	V
V_{DD} (3.0)		Class B/3 V nominal supply voltage contact interface operation	2.7	3.0	3.3	V
V_{DD} (1.8)		Class C/1.8V nominal supply voltage contact interface operation	1.62	1.8	1.98	V
V_I	DC input voltage on digital inputs and digital I/O pads	-	0	-	V_{DD}	V
T_{amb}	Operating ambient temperature[2]		-25	-	+85	°C

[1] All described supply voltages according to ISO/IEC 7816-3.

[2] All product properties and values specified within this data sheet are only valid within the operating ambient temperature range.

The supported operating supply voltage ranges limited by exception sensors covers the whole range of classes A, B and C. The Product Name devices operate within the full voltage range described in Figure 4.

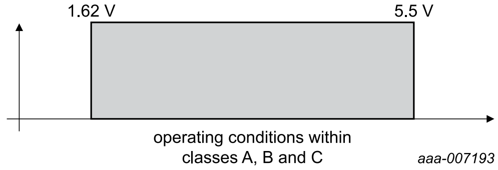


Figure 4. Operating conditions over voltage range

8 Static characteristics

8.1 Measurement conventions

Testing measurements are performed at the contact pads of the device under test. All voltages are defined with respect to the ground contact pad VSS. All currents flowing into the Smart Card IC are considered positive.

8.2 Levels and currents

Table 6. Electrical DC characteristics of Input/Output: IO1, IO2 and IO3

Conditions: V_{DD} = 1.62 V to 5.5 V; V_{SS} = 0 V; T_{amb} = -25 °C to +85 °C, unless otherwise specified

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
V_{IH}	HIGH level input voltage			0.7 V_{DD}	-	V_{DD} + 0.3	V
V_{IL}	LOW level input voltage			-0.3	-	0.25 V_{DD}	V
I_{IH}	HIGH level input current in "weak pull-up" input mode	0.7 $V_{DD} \leq V_I \leq V_{DD}$; Test conditions for the maximum absolute value: $I_{IH(max)}$: V_I = 0.7 V_{DD}, V_{DD} = $V_{DD(max)}$ of the respective supply voltage class A, B or C		0	-	-20	µA
I_{IL}	LOW level input current	0 V $\leq V_I \leq$ 0.3 V_{DD}; Test conditions for the maximum absolute value: $I_{IL(max)}$: V_I = 0 V, V_{DD} = $V_{DD(max)}$ of the respective supply voltage class A, B or C		-	-	-50	µA
I_{TL}	HIGH-to-LOW transition input current (only in "quasi-bidirectional" mode)	0.3 $V_{DD} < V_I \leq V_{DD}$; Test conditions for the maximum absolute value: V_I = 0.5 V_{DD}, V_{DD} = $V_{DD(max)}$ of the respective supply voltage class A, B or C	[1]				
		Class A		-	-	-300	µA
		Class B		-	-	-250	µA
		Class C		-	-	-200	µA
I_I	Input current in "weak pull-up" input mode	0 V $\leq V_I \leq V_{DD}$; Test conditions for the maximum absolute value: $I_{I(max)}$: V_I = 0 V, V_{DD} = $V_{DD(max)}$ of the respective supply voltage class A, B or C		0	-	-50	µA

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
I_{ILIH}	Leakage input current at input voltage beyond V_{DD} in "weak pull-up" input mode	$V_{DD} < V_I \leq V_{DD} + 0.3$ V; -25 °C ≤ T_{amb} ≤ +85 °C; Test conditions: $V_I = V_{DD} + 0.3$ V; $V_{DD} = V_{DD(max)}$ of the respective supply voltage class A, B or C; T_{amb} = +85 °C		-	-	20	μA
I_{ILIL}	Leakage input current at input voltage below V_{SS} in "weak pull-up" input mode	-0.3 V ≤ V_I < 0 V; -25 °C ≤ T_{amb} ≤ +30 °C Test conditions: V_I = -0.3 V; $V_{DD} = V_{DD(max)}$ of the respective supply voltage class A, B or C; T_{amb} = +30 °C		-	-	-50	μA
		-0.3 V ≤ V_I < 0 V; +30 °C < T_{amb} ≤ +85 °C Test conditions: V_I = -0.3 V; $V_{DD} = V_{DD(max)}$ of the respective supply voltage class A, B or C; T_{amb} = +85 °C		-	-	-275	μA
I_{ILIHQ}	Leakage input current at input voltage beyond V_{DD} (only in "quasi-bidirectional" mode)	$V_{DD} < V_I \leq V_{DD} + 0.3$ V; -25 °C ≤ T_{amb} ≤ +85 °C Test conditions: $V_I = V_{DD}$ + 0.3 V; $V_{DD} = V_{DD(max)}$ of the respective supply voltage class A, B or C; T_{amb} = +85 °C		-	-	100	μA
I_{ILILQ}	Leakage input current at input voltage below V_{SS} (only in "quasi-bidirectional" mode)	-0.3 V ≤ V_I < 0 V; -25 °C ≤ T_{amb} ≤ +30 °C Test conditions: V_I = -0.3 V; $V_{DD} = V_{DD(max)}$ of the respective supply voltage class A, B or C; T_{amb} = +30 °C		-	-	-75	μA
		-0.3 V ≤ V_I < 0 V; +30 °C < T_{amb} ≤ +85 °C Test conditions: V_I = -0.3 V; $V_{DD} = V_{DD(max)}$ of the respective supply voltage class A, B or C; T_{amb} = +85 °C		-	-	-300	μA
V_{OH}	HIGH level output voltage	I_{OH} = -20 μA; Class A condition	[2]	3.8 0.7 V_{DD}	-	-	V
		I_{OH} = -20 μA; Class B or C condition	[2]	0.7 V_{DD}	-	-	V
V_{OL}	LOW level output voltage	Class A or B condition; I_{OL} = 1.0 mA		-	-	0.3	V
		Class C condition; I_{OL} = 1.0 mA I_{OL} = 0.5 mA		-	-	0.3 0.15 V_{DD}	V

[1] IO1, IO2 and IO3 source a transition current when being externally driven from HIGH to LOW. This transition current (I_{TL}) reaches its maximum value when the input voltage V_I is approximately 0.5 V_{DD}. Input current I_{TL} is tested at input voltage V_I = 0.5 V_{DD}. Current IIL is tested at input voltage V_I = 0.3 V. Figure 5 shows the input characteristic of this quasi-bidirectional port mode.

[2] External pull-up resistor 20 kΩ to V_{DD} assumed. The worst case test condition for parameter V_{OH} is present at minimum V_{DD}. For class A supply voltage conditions V_{DD} = 4.5 V is the worst case with respect to the fix specification limit V_{OHmin} = 3.8 V (0.844 V_{DD}). The supply voltage related limit "0.7 V_{DD}"is a stricter requirement than the fix value 3.8 V at high V_{DD} values (0.7 V_{DD} = 3.85 V at V_{DD} = 5.5 V). So, in the V_{DD} range 4.5 V to 5.5 V, V_{OHmin} is specified as "the larger value of 0.7 V_{DD} and 3.8 V, respectively". The V_{OHmin} value (0.7 V_{DD}) cannot be guaranteed in "quasi-bidirectional" mode at an output current of I_{OH} = -20 µA - the strong output drive mode must be used.

Table 7. Electrical DC characteristics of Inputs CLK and RST_N[1][2]

Conditions: V_{DD} = 1.62 V to 5.5 V; V_{SS} = 0 V; T_{amb} = -25 °C to +85 °C, unless otherwise specified

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
Inputs CLK (when the IC is not in reset) and RST_N							
V_{IH1}	HIGH level input voltage			0.7 V_{DD}	-	V_{DD} + 0.3	V
V_{IL1}	LOW level input voltage			-0.3	-	0.25 V_{DD}	V
I_{IH1}	HIGH level input current (weak pull-down is on)	0.7 V_{DD} ≤ V_I ≤ V_{DD}; Test conditions for the maximum absolute value: $I_{IH1(max)}$: V_I = V_{DD}, V_{DD} = $V_{DD(max)}$ of the respective supply voltage class A, B or C		-	-	20	µA
I_{IL1}	LOW level input current (weak pull-down is on)	0 V ≤ V_I ≤ 0.3 V_{DD}; Test conditions for the maximum absolute value: $I_{IL1(max)}$: V_I = 0.3 V_{DD}, V_{DD} = $V_{DD(max)}$ of the respective supply voltage class A, B or C		0	-	20	µA
I_{I1}	Input current (weak pull-down is on)	0 V ≤ V_I ≤ V_{DD}; Test conditions for the maximum absolute value: $I_{I1(max)}$: V_I = V_{DD}, V_{DD} = $V_{DD(max)}$ of the respective supply voltage class A, B or C		0	-	20	µA
I_{ILIH1}	Leakage input current at input voltage beyond V_{DD}	V_{DD} < V_I ≤ V_{DD} + 0.3 V; -25 °C ≤ T_{amb} ≤ +85 °C Test conditions: V_I = V_{DD} + 0.3 V; V_{DD} = $V_{DD(max)}$ of the respective supply voltage class A, B or C; T_{amb} = +85 °C		-	-	20	µA
I_{ILIL1}	Leakage input current at input voltage below V_{SS}	-0.3 V ≤ V_I < 0 V; -25 °C ≤ T_{amb} ≤ +30 °C Test conditions: V_I = -0.3 V; V_{DD} = $V_{DD(max)}$ of the respective supply voltage class A, B or C; T_{amb} = +30 °C		-	-	-50	µA

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
		-0.3 V ≤ V_I < 0 V; +30 °C < T_{amb} ≤ +85 °C Test conditions: V_I = -0.3 V; V_{DD} = $V_{DD(max)}$ of the respective supply voltage class A, B or C; T_{amb} = +85 °C		-	-	-200	µA
Input CLK (during IC reset)							
V_{IH2}	HIGH level input voltage			0.7 V_{DD}	-	V_{DD} + 0.3	V
V_{IL2}	LOW level input voltage			-0.3	-	0.25 V_{DD}	V
I_{IH2}	HIGH level input current (weak pull-up is on)	0.7 V_{DD} ≤ V_I ≤ V_{DD}; Test conditions for the maximum absolute value: $I_{IH2(max)}$: V_I = 0.7 V_{DD}, V_{DD} = $V_{DD(max)}$ of the respective supply voltage class A, B or C		0	-	-20	µA
I_{IL2}	HIGH level input current (weak pull-up is on)	0 V ≤ V_I ≤ 0.3 V_{DD}; Test conditions for the maximum absolute value: $I_{IL2(max)}$: V_I = 0V, V_{DD} = $V_{DD(max)}$ of the respective supply voltage class A, B or C		-	-	-20	µA
I_{I2}	Input current (weak pull-up is on)	0 V ≤ V_I ≤ V_{DD}; Test conditions for the maximum absolute value: $I_{I2(max)}$: V_I = 0 V, V_{DD} = $V_{DD(max)}$ of the respective supply voltage class A, B or C		0	-	-20	µA
I_{ILIH2}	Leakage input current at input voltage beyond V_{DD}	V_{DD} < V_I ≤ V_{DD} + 0.3 V; -25 °C ≤ T_{amb} ≤ +85 °C Test conditions: V_I = V_{DD} + 0.3 V; V_{DD} = $V_{DD(max)}$ of the respective supply voltage class A, B or C; T_{amb} = +85 °C		-	-	20	µA
I_{ILIL2}	Leakage input current at input voltage below V_{SS}	-0.3 V ≤ V_I < 0 V; -25 °C ≤ T_{amb} ≤ +30 °C Test conditions: V_I = -0.3 V; V_{DD} = $V_{DD(max)}$ of the respective supply voltage class A, B or C; T_{amb} = +30 °C		-	-	-50	µA
		-0.3 V ≤ V_I < 0 V; +30 °C < T_{amb} ≤ +85 °C Test conditions: V_I = -0.3 V; V_{DD} = $V_{DD(max)}$ of the respective supply voltage class A, B or C; T_{amb} = +85 °C		-	-	-200	µA

[1] The active low RST_N input and outside reset state also the CLK input internally activate a resistive pull-down device to VSS. Accordingly a current is flowing into the pad at voltages above 0 V. Figure 7 shows this input characteristic. In CLOCKSTOP mode the preferred electrical state on CLK is a LOW level, in order to minimize the power consumption.

[2] The CLK input internally has a resistive pull-up device to VDD activated during IC reset. Accordingly a current is flowing out of the pad at voltages below V_{DD}. Figure 8 shows this input characteristic.

Table 8. Electrical DC characteristics of TP1 and TP2

Conditions: (A) V_{DD} = 1.62 to 1.98 V: V_{DDAE} = V_{DD};
(B) V_{DD}= 2.2 to 5.5 V (i.e. outside Class C supply range): $V_{DDAE(NOM)}$ = 1.8 V;
V_{SS} = 0 V; T_{amb} = -25 °C to +85 °C, unless otherwise specified

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
V_{IHT}	HIGH level input voltage			0.7 V_{DDAE}	-	V_{DDAE} + 0.3	V
V_{ILT}	LOW level input voltage			-0.3	-	0.25 V_{DDAE}	V
I_{IHD}	HIGH level input current maximum (resistive pull-down is on)	0.7 V_{DDAE} ≤ V_I ≤ V_{DDAE}; Test conditions for the maximum absolute value: V_I = V_{DDAE}; V_{DDAE} = $V_{DDAE(max)}$; for the minium absolute value: V_I = 0.7 V_{DDAE}; V_{DDAE} = $V_{DDAE(min)}$		10	-	100	µA
I_{ILD}	LOW level input current maximum (resistive pull-down is on)	0 V ≤ V_I ≤ 0.3 V_{DDAE}; Test conditions for the maximum absolute value: V_I = 0.3 V_{DDAE}; V_{DDAE} = $V_{DDAE(max)}$;		0	-	20	µA
I_{ILIH3}	Leakage input current at input voltage beyond V_{DDAE} (resistive pull-down is on)	V_{DDAE} < V_I ≤ V_{DDAE} + 0.3 V; -25 °C ≤ T_{amb} ≤ 85 °C; Test conditions: V_I = 2.3 V; T_{amb} = +85 °C		-	-	150	µA
I_{ILIL3}	Leakage input current at input voltage beyond V_{SS} (resistive pull-down is on)	-0.3 V ≤ V_I < 0 V; -25 °C ≤ T_{amb} ≤ +30 °C; Test conditions: V_I = -0.3 V; T_{amb} = +30 °C		0	-	-150	µA
		-0.3 V ≤ V_I < 0 V; +30 °C < T_{amb} ≤ +85 °C; Test conditions: V_I = -0.3 V; T_{amb} = +85 °C		-	-	-300	µA
V_{OH2}	HIGH level output voltage	I_{OH2} = -0.1 µA		V_{DDAE} - 0.3	-	-	V
V_{OL2}	LOW level output voltage	I_{OL2} = 1.2 µA		-	-	0.3	V

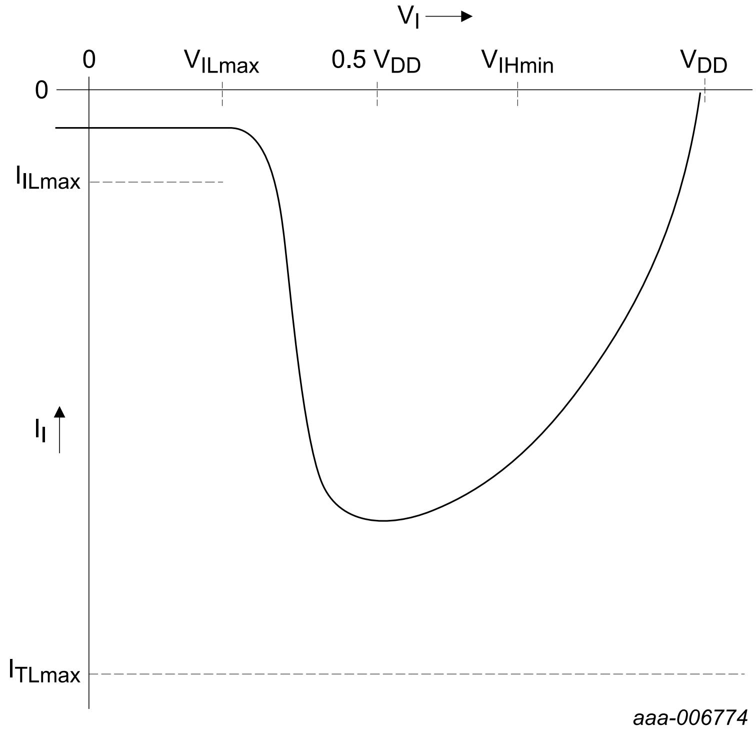


Figure 5. Input characteristic of IO1, IO2, IO3 in "quasi-bidirectional" mode

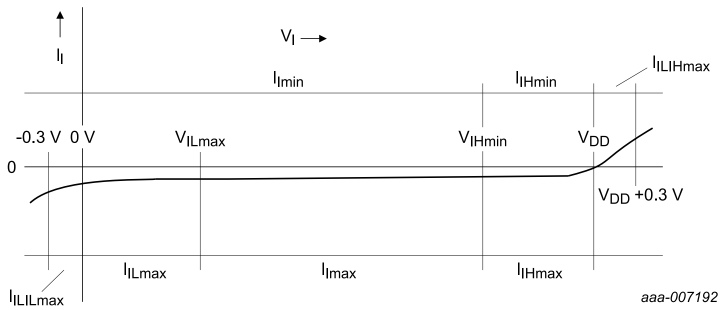


Figure 6. Input characteristic of IO1, IO2, IO3 in "weak pull-up" input mode

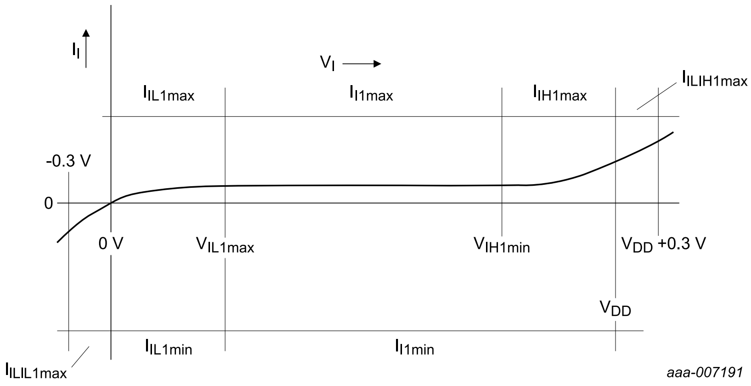


Figure 7. Input characteristic of CLK when the IC is not in reset and of RST_N

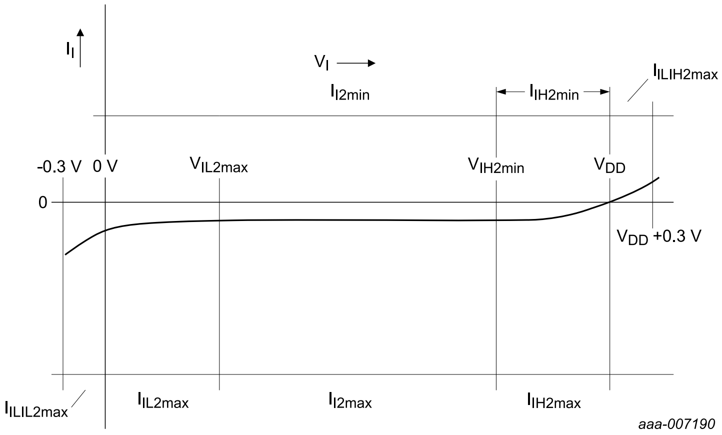


Figure 8. Input characteristic of CLK during IC reset

8.3 General and ISO/IEC 7816 I/O interface at ISO/IEC 7816-3: A/5 V, class B/3 V or class C/1.8 V class operation

Table 9. Electrical characteristics of IC supply current[1]

Conditions: V_{DD} = 1.62 V to 5.5 V; V_{SS} = 0 V; T_{amb} = -25 °C to +85 °C, unless otherwise specified

Symbol	Parameter	Conditions	Supply voltage class		Min	Typ	Max	Unit
Supply								
V_{DD}	supply voltage range	Class A: 5 V range	A (5 V)		4.50	5.00	5.50	V
		Class B: 3 V range	B (3 V)		2.70	3.00	3.30	V
		Class C: 1.8 V range	C (1.8 V)		1.62	1.80	1.98	V
	operating mode: Reset State							
I_{DD}	supply current operating mode	f_{CLK} = 10 MHz, RESET state	A (5 V) B (3 V) C (1.8 V)		-	1.20	4.00	mA
	operating mode: typical CPU							

Symbol	Parameter	Conditions	Supply voltage class		Min	Typ	Max	Unit
	no coprocessor active	f_{CLK} = 10 MHz, CPU at f_{CLK}	A (5 V) B (3 V) C (1.8 V)		-	1.60	4.00	mA
	no coprocessor active	f_{CLK} = 10 MHz, CPU in free running mode	A (5 V) B (3 V) C (1.8 V)		-	2.50	4.00	mA
	DES coprocessor active (DES int. 32 MHz)	f_{CLK} = 10 MHz, CPU at int. 4 MHz	A (5 V) B (3 V) C (1.8 V)		-	4.00	6.00	mA
	DES coprocessor active (DES int. 96 MHz)	f_{CLK} = 10 MHz, CPU at int. 4 MHz	A (5 V) B (3 V) C (1.8 V)		-	8.60	10.50	mA
	AES coprocessor active (AES int. 32 MHz)	f_{CLK} = 10 MHz, CPU at int. 4 MHz	A (5 V) B (3 V) C (1.8 V)		-	3.10	5.00	mA
	AES coprocessor active (AES int. 96 MHz)	f_{CLK} = 10 MHz, CPU at int. 4 MHz	A (5 V) B (3 V) C (1.8 V)		-	5.60	8.00	mA
	Fame2 coprocessor active (Fame2 clock = 16 MHz, double multiplier mode)	f_{CLK} = 10 MHz, CPU at int. 4 MHz	A (5 V) B (3 V) C (1.8 V)		-	3.90	6.50	mA
	Fame2 coprocessor active (Fame2 clock = 48 MHz, double multiplier mode)	f_{CLK} = 10 MHz, CPU at int. 4 MHz	A (5 V) B (3 V) C (1.8 V)		-	5.40	8.50	mA
	Fame2 coprocessor active (Fame2 clock = free running, double multiplier mode)	f_{CLK} = 10 MHz, CPU at int. 4 MHz	A (5 V) B (3 V) C (1.8 V)		-	5.40	10.50	mA
$I_{DD(ID)}$	supply current CPU IDLE mode (this parameter should not be mixed-up with the ETSI "idle state")	f_{CLK} = 10 MHz, T_{amb} = 25 °C	A (5 V) B (3 V) C (1.8 V)		-	0.80	1.50	mA
$I_{DD(SLP)}$	supply current SLEEP mode (this parameter should not be mixed-up with the ETSI "idle state")	f_{CLK} = 10 MHz, T_{amb} = 25 °C (VDDCO power domain switched off)	A (5 V) B (3 V) C (1.8 V)		-	175.00 150.00	200.00	μA
$I_{DD(PD)}$	supply current CLOCKSTOP mode	$V_{DDmin} \leq V_{DD} \leq V_{DDmax}$; Clock to input CLK stopped, T_{amb} = 25 °C (VDDCO power domain and CLIF switched off)	A (5 V)		-	80.00	200.00	μA
			B (3 V) C (1.8 V)		-	60.00	100.00	μA

[1] Typical values are only referenced for information. They are subject to change without notice.

9 Dynamic characteristics

Remark: The P6022y VB only supports one single IO1.

9.1 General, ISO/IEC 7816 I/O and ISO/IEC 14443 I/O interfaces

Table 10. Electrical AC characteristics of IO1, IO2, IO3, CLK and RST_N

Conditions: V_{DD} = 1.62 V to 5.5 V; V_{SS} = 0 V; T_{amb} = -25°C to +85 °C, unless otherwise specified

Symbol	Parameter	Conditions		Min	Typ[1]	Max	Unit
Input/Output: IO1, IO2 and IO3							
tr_{IO}	I/O Input rise time	Input/reception mode	[2]	-	-	1	μs
			[3]	-	-	0.25 × t_{IOWx_min}	μs
tf_{IO}	I/O Input fall time	Input/reception mode	[2]	-	-	1	μs
			[3]	-	-	0.25 × t_{IOWx_min}	μs
tr_{OIO}	I/O Output rise time	Output/transmission mode; C_L = 30 pF		-	-	0.1	μs
tf_{OIO}	I/O Output fall time	Output/transmission mode; C_L = 30 pF		-	-	0.1	μs
Inputs: CLK and RST_N							
f_{CLK}	External clock frequency in ISO/IEC 7816 UART applications	t_{CLKW}, T_{amb} and V_{DD} in their spec'd limits	[4]	0.85	-	11.5	MHz
t_{CLKW}	Clock pulse width i.r.t. clock period (positive pulse duty cycle of CLK)		[5]	40	-	60	%
tr_{CLK}	CLK input rise time		[6]	-	-	see [6]	
tf_{CLK}	CLK input fall time		[6]	-	-	see [6]	
tr_{RST}	RST_N input rise time		[7]	-	-	400	μs
tf_{RST}	RST_N input fall time		[7]	-	-	400	μs
t_{RW}	Reset pulse width (RST_N low)			40	-	-	μs
t_{WKP}	Wake-up time from SLEEP mode	$f_{CLKmin} \leq f_{CLK} \leq f_{CLKmax}$		-	17	20	μs
t_{WKPIO}	I/Ox LOW time for wake-up from SLEEP mode	level triggered ext.int.		-	20	-	μs
		edge triggered ext.int.		-	20	-	μs
t_{WKPRST}	RST_N LOW time for wake-up from SLEEP mode			40	-	-	μs
Inputs: CLK, RST_N, IO1, IO2, IO3							
C_{PIN}	Pin capacitances CLK, RST_N, IO1, IO2, IO3	Test frequency = 1 MHz; T_{amb} = 25 °C		-	-	10	pF

[1] Typical values are only referenced for information. They are subject to change without notice.

[2] At minimum IOx input signal HIGH or LOW level voltage pulse width of 3.2 μs. This timing specification applies to ISO7816 configurations down to a minimum etu duration of 16 CLK cycles at a maximum CLK frequency of 5 MHz (TA1=0x96, (Fi/Di)=(512/32)), for example.

[3] At minimum IOx input signal HIGH or LOW level voltage pulse width of less than 3.2 μs. This timing specification applies to ISO7816 configurations beyond the conditions listed in note [2], down to a minimum etu duration of 8 CLK cycles at a maximum CLK frequency of 5 MHz (TA1=0x97, (Fi/Di)=(512/64)), for example. An 8 CLKs/etu @ fclk = 5 MHz configuration results in t_{IOWx_min} = 1.6 μs, and in a time of 400 ns for tr_{IO_max} and tf_{IO_max}, matching the (Fi/Di)=(512/64) speed enhancement requirements of ETSI TS 102 221.

[4] ISO/IEC 7816 I/O applications have to supply a clock signal to input CLK in the frequency range of 1 MHz to 10 MHz nominal. A ± 15 % tolerance range yields the allowed limits of 0.85 MHz and 11.5 MHz.

[5] During AC testing the inputs CLK, RST_N, IO1, IO2 and IO3 are driven at 0 V to +0.3 V for a LOW input level and at V_{DD} - 0.3 V to V_{DD} for a HIGH input level. Clock period and signal pulse (duty cycle) timing is measured at 50% of V_{DD} (see Figure 9).

[6] The maximum CLK rise and fall time is 10% of the CLK period $1/f_{CLK}$ - with the following exception: In the CLK frequency range of 1 MHz to 5 MHz the maximum allowed CLK rise and fall time is 50 ns, if 10% of the CLK period is shorter than 50 ns.

[7] The ETSI TS102 221/GSM 11.1x specifications specify a maximum reset signal (RST_N) rise time and fall time of 400,000 μs, respectively.

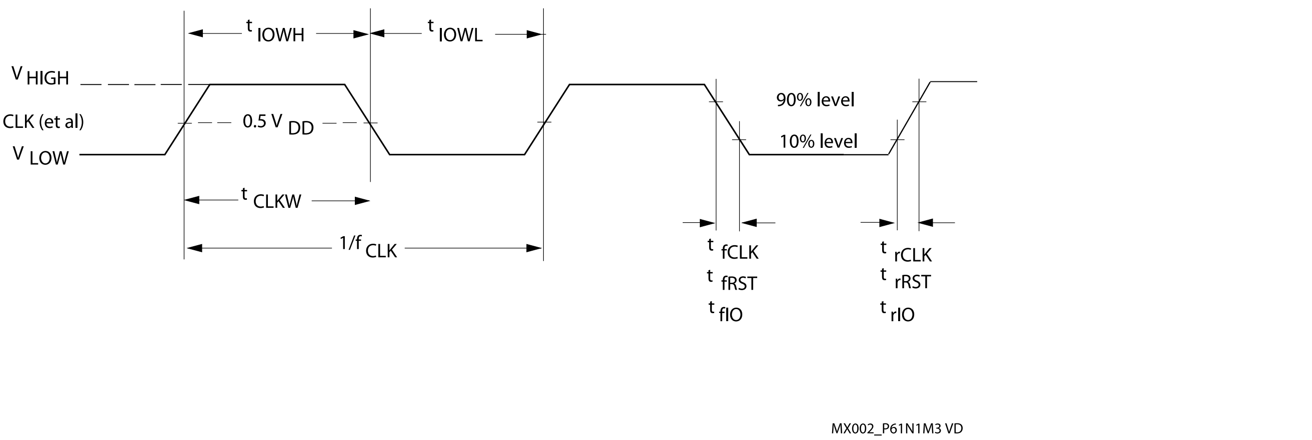


Figure 9. External clock drive and AC test timing reference points of CLK, RST_N, IO1, IO2 and IO3 (see [1] and [2])

[1] During AC testing the inputs CLK, RST_N, IO1, IO2 and IO3 are driven at 0 V to +0.3 V for a LOW input level and at V_{DD} - 0.3 V to V_{DD} for a HIGH input level. Clock period and signal pulse (duty cycle) timing is measured at 50% of V_{DD}.

[2] t_r is defined as rise time between 10% and 90% of the signal amplitude.

t_f is defined as fall time between 90% and 10% of the signal amplitude.

Table 11. Electrical AC characteristics of TP1 and TP2

Conditions: (A) V_{DD} = 1.62 to 1.98 V: V_{DDAE} = V_{DD}; (B) V_{DD} = 2.2 to 5.5 V (i.e. outside Class C supply range): $V_{DDAE}(nom)$ = 1.8 V; V_{SS} = 0 V; T_{amb} = -25 °C to +85 °C, unless otherwise specified

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
tr_{TP}	TP input rise time	Input/reception mode		-	-	1	μs
tf_{TP}	TP input fall time	Input/reception mode		-	-	1	μs
tr_{OTP}	TP output rise time	Output/transmission mode; C_L = 30 pF		-	-	50	ns
tf_{OTP}	TP output fall time	Output/transmission mode; C_L = 30 pF		-	-	50	ns
Ci_{TP}	Pin characteristics TP1, TP2	Test frequency = 1 MHz; T_{amb} = -25 °C		-	-	15	pF

9.2 Non-Volatile memory

Table 12. Non-volatile memory characteristics

Conditions: V_{DD} = 1.62 V to 5.5 V; V_{SS} = 0 V; T_{amb} = -25°C to +85 °C, unless otherwise specified

Symbol	Parameter	Conditions		Min	Typ[1]	Max	Unit
t_{EEP}	EEPROM erase/program time		[2]	-	2.00	-	ms
t_{EEE}	EEPROM erase time			-	1.25	-	ms
t_{EEW}	EEPROM program time			-	0.75	-	ms
t_{EER}	EEPROM data retention time	T_{amb} = +55 °C		25	-	-	years
N_{EEC}	EEPROM endurance (number of programming cycles)			5×10^5	-	-	cycles
N_{EECM}	EEPROM endurance (maximum number of programming cycles applied to the whole memory block)			20×10^6	100×10^6	-	cycles

[1] Typical values are only referenced for information. They are subject to change without notice.
[2] Given value specifies physical access times of EEPROM memory only.

9.3 I^2C Slave interface bus timing

Table 13. Non-volatile memory characteristics

Conditions: V_{DD} = 1.62 V to 5.5 V; V_{SS} = 0 V; T_{amb} = -25°C to +85 °C, unless otherwise specified

Symbol	Parameter	Conditions	Min	Max	Unit
f_{SCL}	SCL clock frequency		0	350	kHz
$t_{HD;STA}$	hold time (repeated) START condition	after this period, the first clock pulse is generated	4000	-	ns
$t_{SU;STA}$	set-up time for a repeated START condition		4700	-	ns
$t_{SU;STO}$	set-up time for STOP condition		4000	-	ns
t_{LOW}	LOW period of the SCL clock		4700	-	ns
t_{HIGH}	HIGH period of the SCL clock		4000	-	ns
$t_{HD;DAT}$	data hold time		300	3450	ns
$t_{SU;DAT}$	data set-up time		250	-	ns
$t_{VD,DAT}$	data valid time		-	3450	ns
$t_{VD,ACK}$	data vlid acknowledge		-	3450	ns
t_r	rise time	SDA and SCL signals	-	1000	ns
t_f	fall time	SDA and SCL signals	-	300	ns
t_{BUF}	bus free time between a STOP and START condition		4700	-	ns

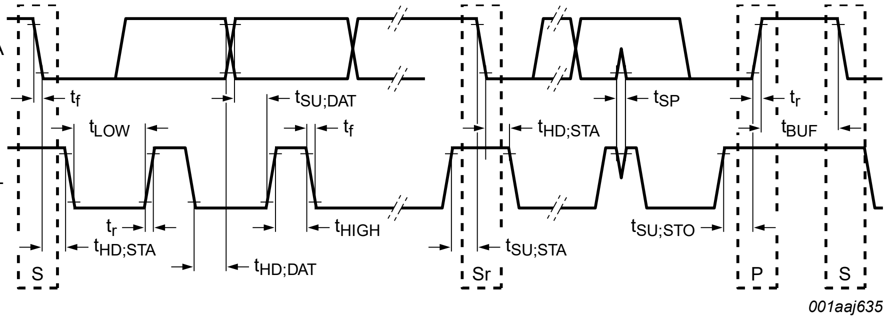
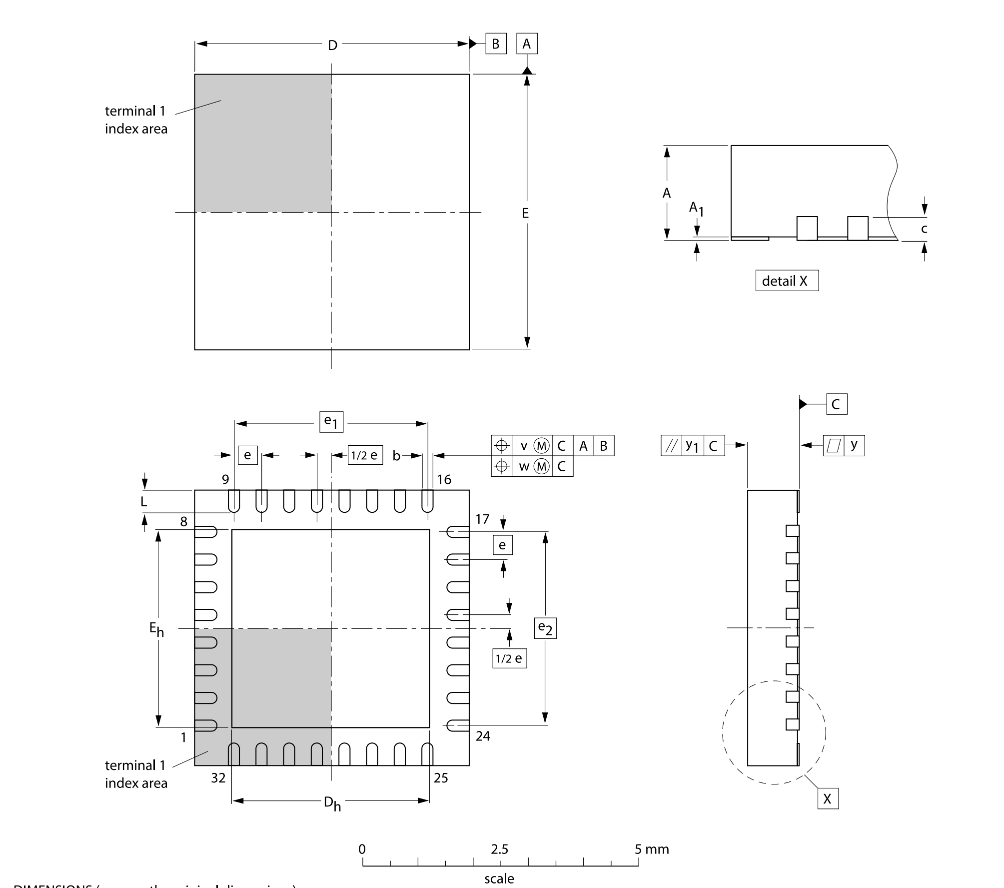


Figure 10. Timing for I²C Slave bus

10 Package outline

HVQFN32: plastic thermal enhanced very thin quad flat package; no leads;
32 terminals; body 5 x 5 x 0.85 mm

SOT617-3



DIMENSIONS (mm are the original dimensions)

UNIT	$A^{(1)}$ max.	A_1	b	c	$D^{(1)}$	D_h	$E^{(1)}$	E_h	e	e_1	e_2	L	v	w	y	y_1
mm	1	0.05 0.00	0.30 0.18	0.2	5.1 4.9	3.75 3.45	5.1 4.9	3.75 3.45	0.5	3.5	3.5	0.5 0.3	0.1	0.05	0.05	0.1

Note

1. Plastic or metal protrusions of 0.075 mm maximum per side are not included.

OUTLINE VERSION	REFERENCES				EUROPEAN PROJECTION	ISSUE DATE
	IEC	JEDEC	JEITA			
SOT617-3	---	MO-220	---			~~02-04-18~~ 02-10-22

Figure 11. Package outline SOT617-3

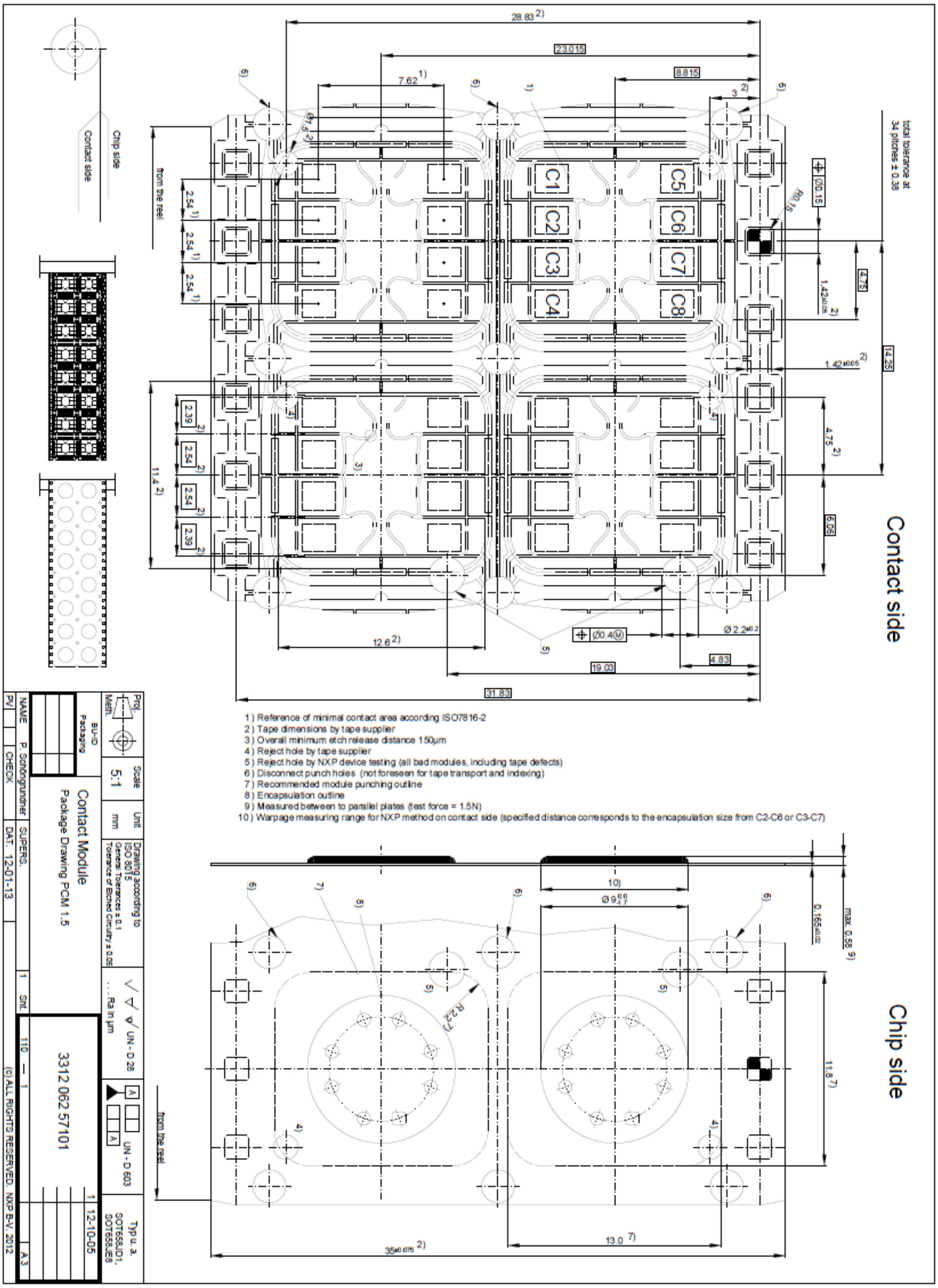


Figure 12. Package outline SOT658-1

11 Packing information

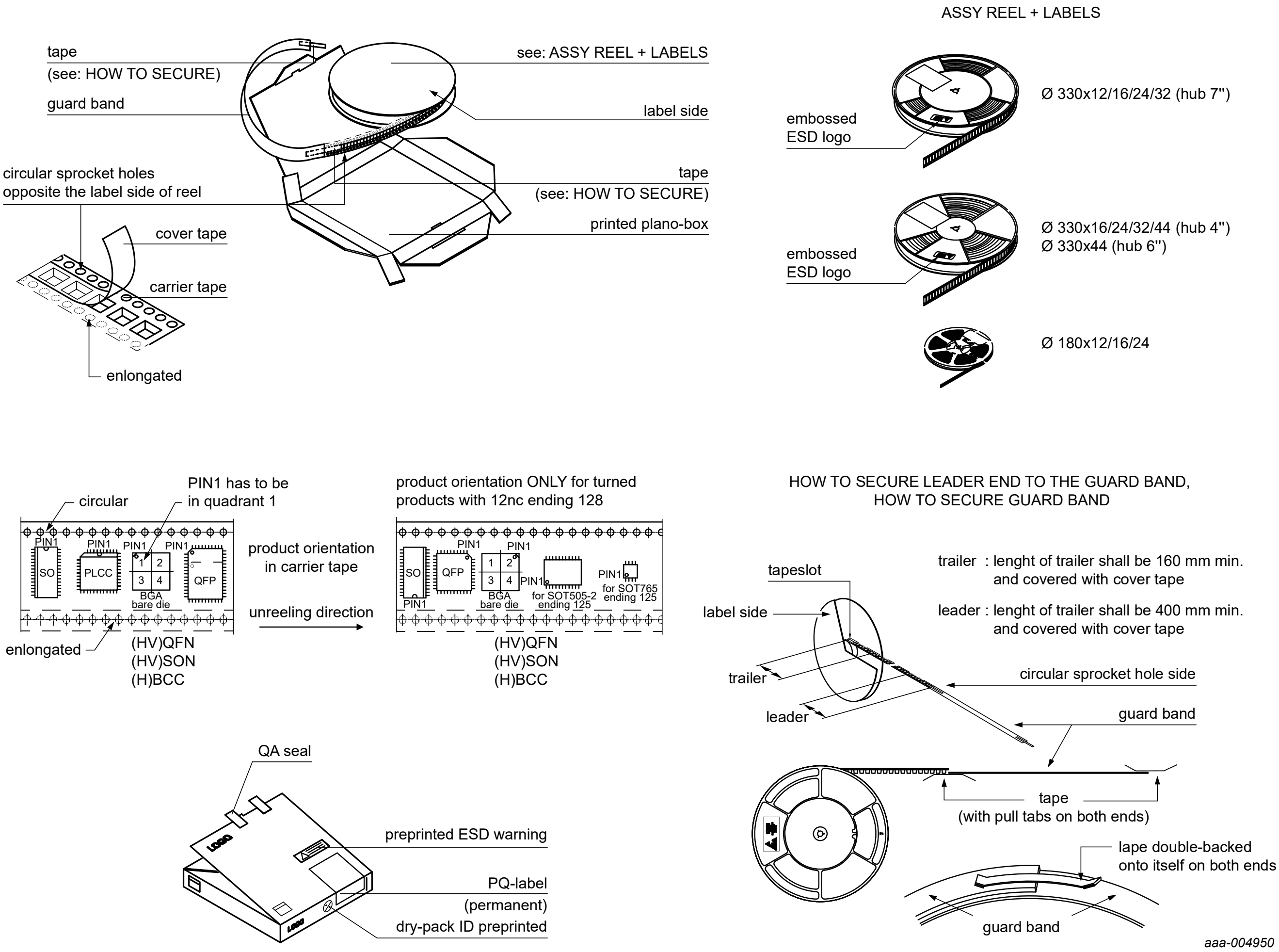


Figure 13. Packing information for HVQFN32 package - Reel

12 References

[1] Data sheet — MF4SAM3 MIFARE SAM AV3 secure access module product daa sheet, Doc No. 3235**[3]

3 ** denote the document version number

13 Revision history

Table 14. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
MF4SAM3_SDS	20190802	Product data sheet		--
Modifications:	• Initial released version			

14 Legal information

14.1 Data sheet status

Document status[1][2]	Product status[3]	Definition
Objective [short] data sheet	Development	This document contains data from the objective specification for product development.
Preliminary [short] data sheet	Qualification	This document contains data from the preliminary specification.
Product [short] data sheet	Production	This document contains the product specification.

[1] Please consult the most recently issued document before initiating or completing a design.
[2] The term 'short data sheet' is explained in section "Definitions".
[3] The product status of device(s) described in this document may have changed since this document was published and may differ in case of multiple devices. The latest product status information is available on the Internet at URL http://www.nxp.com.

14.2 Definitions

Draft — The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

Short data sheet — A short data sheet is an extract from a full data sheet with the same product type number(s) and title. A short data sheet is intended for quick reference only and should not be relied upon to contain detailed and full information. For detailed and full information see the relevant full data sheet, which is available on request via the local NXP Semiconductors sales office. In case of any inconsistency or conflict with the short data sheet, the full data sheet shall prevail.

Product specification — The information and data provided in a Product data sheet shall define the specification of the product as agreed between NXP Semiconductors and its customer, unless NXP Semiconductors and customer have explicitly agreed otherwise in writing. In no event however, shall an agreement be valid in which the NXP Semiconductors product is deemed to offer functions and qualities beyond those described in the Product data sheet.

14.3 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors. In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory. Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification. Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products. NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Limiting values — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) will cause permanent damage to the device. Limiting values are stress ratings only and (proper) operation of the device at these or any other conditions above those given in the Recommended operating conditions section (if present) or the Characteristics sections of this document is not warranted. Constant or repeated exposure to limiting values will permanently and irreversibly affect the quality and reliability of the device.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

No offer to sell or license — Nothing in this document may be interpreted or construed as an offer to sell products that is open for acceptance or the grant, conveyance or implication of any license under any copyrights, patents or other industrial or intellectual property rights.

Quick reference data — The Quick reference data is an extract of the product data given in the Limiting values and Characteristics sections of this document, and as such is not complete, exhaustive or legally binding.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Non-automotive qualified products — Unless this data sheet expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications. In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — While NXP Semiconductors has implemented advanced security features, all products may be subject to unidentified vulnerabilities. Customers are responsible for the design and operation of their applications and products to reduce the effect of these vulnerabilities on customer's applications and products, and NXP Semiconductors accepts no liability for any vulnerability that is discovered. Customers should implement appropriate design and operating safeguards to minimize the risks associated with their applications and products.

14.4 Trademarks

Notice: All referenced brands, product names, service names and trademarks are the property of their respective owners.

I^{2}C-bus — logo is a trademark of NXP B.V.

MIFARE — is a trademark of NXP B.V.

DESFire — is a trademark of NXP B.V.

ICODE and I-CODE — are trademarks of NXP B.V.

UCODE — is a trademark of NXP B.V.

MIFARE Plus — is a trademark of NXP B.V.

MIFARE Ultralight — is a trademark of NXP B.V.

MIFARE Classic — is a trademark of NXP B.V.

NTAG — is a trademark of NXP B.V.

Tables

Figures

Contents

Date of release: 2 August 2019
Document identifier: MF4SAM3
Document number: 561930