AT88RF04C

CryptoRF EEPROM Memory
13.56MHz, 4 Kilobits

SUMMARY DATASHEET

Features

- One of a family of devices with user memory of 4 kilobits to 64 kilobits
- Contactless 13.56MHz RF communications interface
  - ISO/IEC 14443-2:2001 Type B Compliant
  - ISO/IEC 14443-3:2001 Type B Compliant Anticollision Protocol
  - Tolerant of Type A Signaling for multi-protocol applications
- Integrated 82pF tuning capacitor
- User EEPROM memory
  - Four kilobits configured as four 128-byte (1-Kbit) user zones
  - Byte, page, and partial page write modes
  - Self-timed write cycle
- 256-byte (2-Kbit) configuration zone
  - User-programmable Application Family Identifier (AFI)
  - User-defined anticollision polling response
  - User-defined keys and passwords
  - Read-only unique die serial number
  - Secure personalization mode
- High-security features
  - Selectable access rights by zone
  - 64-bit Mutual Authentication Protocol (under license of ELVA)
  - Encrypted checksum
  - Stream encryption using 64-bit key
  - Four key sets for authentication and encryption
  - Four sets of two 24-bit passwords
  - Password and authentication attempts counters
  - Anti-tearing function
  - Tamper sensors
- High reliability
  - Endurance: 100,000 write cycles
  - Data retention: 10 years
  - Operating temperature: −40°C to +85°C

This is a summary document. The complete document is available on the Atmel website at www.atmel.com.

1. Description

The Atmel® CryptoRF® family integrates a 13.56MHz RF interface into an Atmel CryptoMemory®. This product line is ideal for RF tags and contactless smart cards that can benefit from advanced security and cryptographic features. This device is optimized as a contactless secure memory for data storage without the requirement of an internal microprocessor.

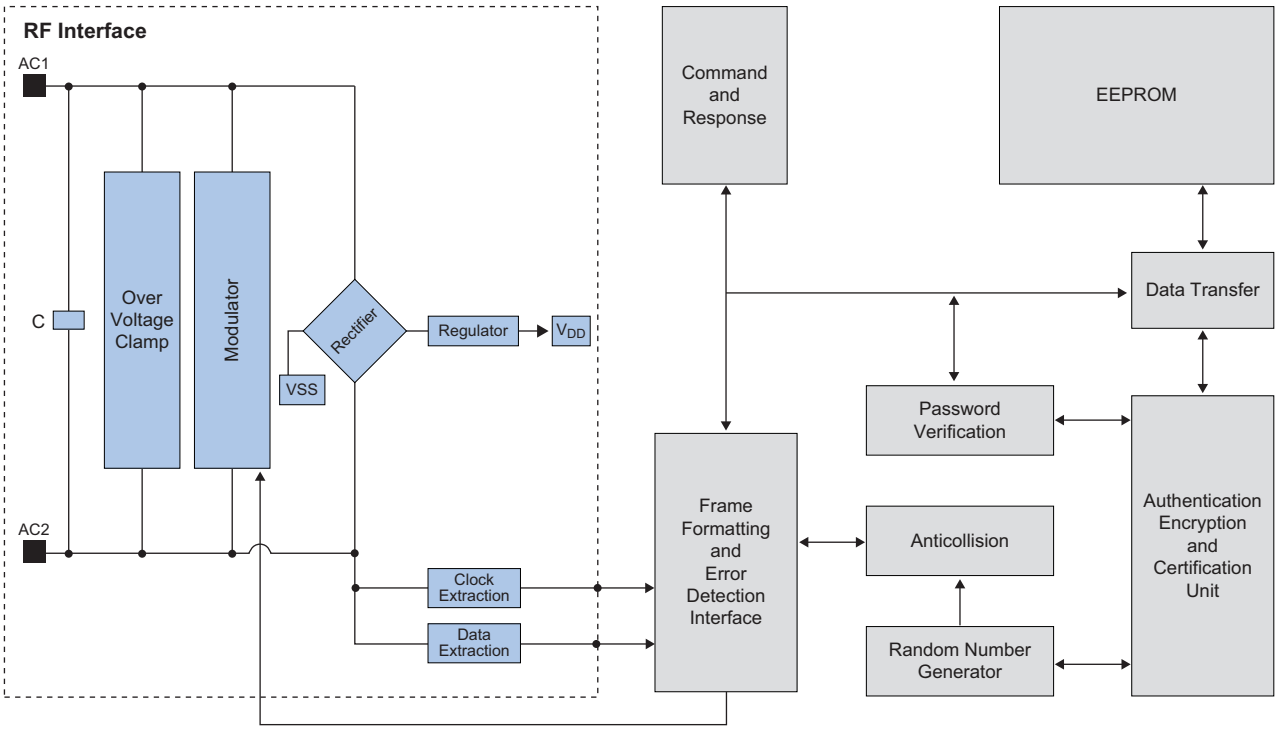
For communications, the RF interface utilizes the ISO/IEC 14443-2 and -3 Type B bit timing and signal modulation schemes, and the ISO/IEC 14443-3 Slot-MARKER Anticollision Protocol. Data is exchanged half duplex at a 106-kbit per second rate, with a two-byte CRC_B providing error detection capability. The RF interface powers the other circuits; no battery is required. Full compliance with the ISO/IEC 14443-2 and -3 standards and provides both a proven RF communication interface and a robust anticollision protocol.

AT88RF04C contains four kilobits of user memory and two kilobits of configuration memory. The two kilobits of configuration memory contain:

- Four sets of read/write passwords
- Four Crypto key sets
- Security access registers for each user zone
- Password/Key registers for each zone

The CryptoRF command set is optimized for a multi-card RF communications environment. A programmable AFI register allows this IC to be used in numerous applications in the same geographic area with seamless discrimination of cards assigned to a particular application during the anticollision process.

Figure 1-1. Block Diagram



2. Communications

All personalization and communication with this device is performed through the RF interface. The IC includes an integrated tuning capacitor, enabling it to operate with only the addition of a single external coil antenna.

The RF communications interface is fully compliant with the electrical signaling and RF power specifications in ISO/IEC 14443-2:2001 for Type B only. Anticollision operation and frame formatting are compliant with ISO/IEC 14443-3:2001 for Type B only.

ISO/IEC 14443 nomenclature is used in this specification where applicable. The following abbreviations are utilized throughout this document. Additional terms are defined in the section in which they are used.

Table 2-1. Terms

Abbrev.	Term	Definition
PCD	Proximity Coupling Device	The reader/writer and antenna.
PICC	Proximity Integrated Circuit Card	The tag/card containing the IC and antenna.
RFU	Reserved for Future Use	Any feature, memory location, or bit that is held as reserved for future use.
$ xx	Hexadecimal Number	Denotes a hex number “xx” (Most Significant Bit on left).

3. Anticollision Protocol

When the PICC enters the 13.56MHz RF field of the host reader (PCD), it performs a Power-On Reset (POR) function and waits silently for a valid Type B Polling command. The CryptoRF PICC processes the anti-tearing registers as part of the POR process.

The PCD initiates the anticollision process by issuing an REQB or WUPB command. The WUPB command activates any card (PICC) in the field with a matching AFI code.

The REQB command performs the same function but does not affect a PICC in the Halt state. The CryptoRF command set is available only after the anticollision process has been completed.

4. CRC Error Detection

A 2-byte CRC_B is required in each frame transmitted by the PICC or PCD to permit transmission error detection. The CRC_B is calculated on all of the command and data bytes in the frame. The SOF, EOF, start bits, stop bits, and EGT are not included in the CRC_B calculation. The 2-byte CRC_B follows the data bytes in the frame.

Figure 4-1. Location of the Two CRC_B Bytes within a Frame

5. Type A Tolerance

The RF Interface is designed for use in multi-protocol applications. It will not latch or lock-up if exposed to Type A signals and will not respond to them. The PICC may reset in the presence of Type A field modulation but is not damaged by exposure to Type A signals.

6. User Memory

The EEPROM user memory is divided into four user zones as shown in Table 6-1. Multiple zones allow for different types of data or files to be stored in different zones. Access to the user zones is allowed only after security requirements have been met. These security requirements are defined by the user in the configuration memory during personalization of the device. The EEPROM memory page length is 16 bytes.

Table 6-1. Memory Map

Zone		$0	$1	$2	$3	$4	$5	$6	$7
User 0	$00								
	—	128 Bytes							
	—								
	$78								
User 1	$00								
	—	128 Bytes							
	—								
	$78								
User 2	$00								
	—	128 Bytes							
	—								
	$78								
User 3	$00								
	—	128 Bytes							
	—								
	$78								

7. Configuration Memory

The configuration memory consists of 2048 bits of EEPROM memory used for storing system data, passwords, keys, codes, and security-level definitions for each user zone. Access rights to the configuration zone are defined in the control logic and may not be altered by the user. These access rights include the ability to program certain portions of the configuration memory and then lock the data written through use of the security fuses.

8. Security Fuses

There are three fuses on the device that must be blown during the device personalization process. Each fuse locks certain portions of the configuration memory as OTP memory. Fuses are designated for locking the secrets and the user zone access requirements. The fuses must be blown in sequence.

9. Communication Security

Communication between the PICC and reader operates in three basic modes:

- **Standard Communication Security Mode —** The default mode for the device after power-up and anticollision.
- **Authentication Communication Security Mode** — Activated by a successful authentication sequence.
- **Encryption Communication Security Mode** — Activated by a successful encryption activation sequence, following a successful authentication.

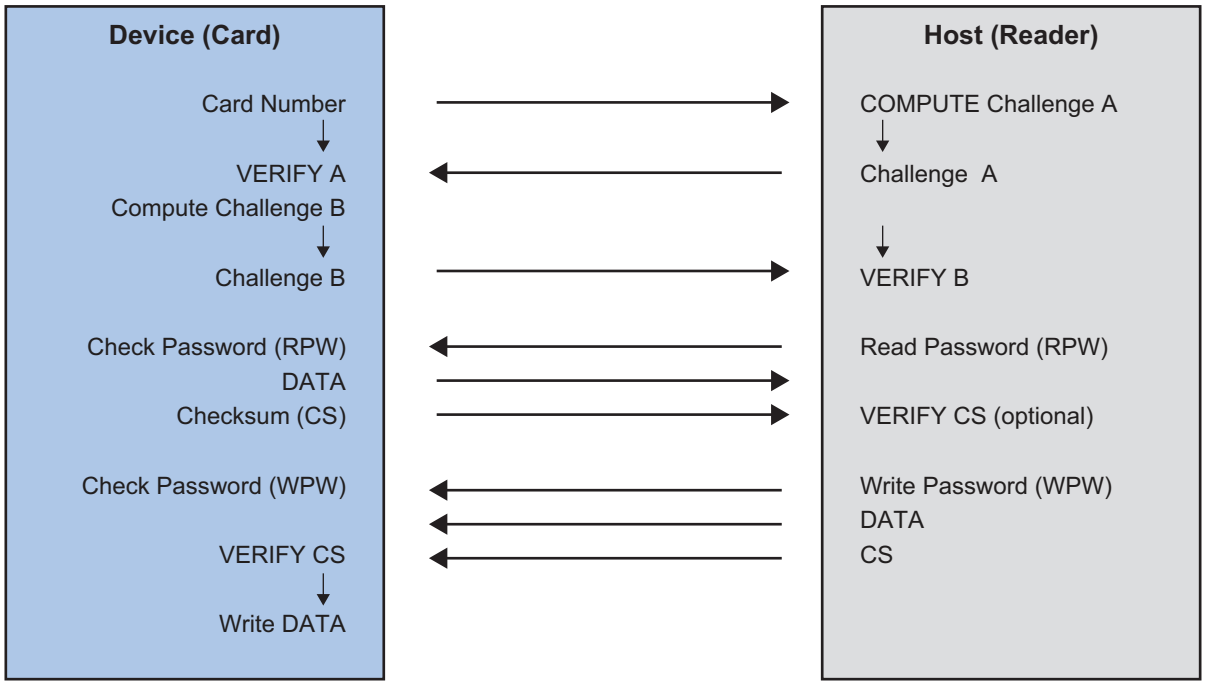
Table 9-1. Configuration Security Modes

Communication Mode	User Data	System Data	Passwords
Normal	Clear	Clear	Clear
Authentication	Clear	Clear	Encryption
Encryption	Encryption	Clear(1)	Encryption

Note: 1. AT88RF04C supports an encryption option for programming secrets.

10. Security Methodology

Figure 10-1. Security Methodology



11. Memory Access

Depending on the device configuration, the host will carry out the authentication protocol and/or present different passwords for each operation: Read or Write. To insure security between the different user zones, each zone can use a different set of passwords or keys. A specific attempts counter for each password and for each authentication key provides protection against systematic attacks.

12. Security Operations

12.1 Anti-tearing

In the event of a power loss during a write cycle, the integrity of the device's stored data may be recovered. This function is optional — The host may choose to activate the anti-tearing function depending on application requirements.

- When anti-tearing is active, write commands take longer to execute since more write cycles are required to complete them.
- Data writes are limited to 8-byte pages when anti-tearing is active.

Data is written first to a buffer zone in EEPROM instead of to the intended destination address, but with the same access conditions. The data is then written to the required location. If this second write cycle is interrupted due to a power loss, the device will automatically recover the data from the buffer zone at the next power-up.

12.2 Password Verification

Passwords may be used to protect user zone read and/or write access. When a password is presented using the Check Password command, it is memorized and active until power is removed unless a new password is presented or a valid DESELECT or IDLE command is received. Only one password is active at a time, but write passwords also give read access.

12.3 Authentication Protocol

The access to a user zone may be protected by an authentication protocol in addition to password dependent rights. Passwords are encrypted in Authentication Communication Security mode. The authentication success is memorized and active as long as the chip is powered, unless a new authentication is initialized or a valid DESELECT or IDLE command is received. If the new authentication request is not validated, the card loses its previous authentication and it must be presented again. Only the last request is memorized.

12.4 Encryption

The data exchanged between the card and the reader during Read, Write, and Check Password commands may be encrypted to ensure data confidentiality.

The issuer may choose to protect the access to a user zone with an encryption key by settings made in the configuration memory. In that case, activation of the Encryption Communication Security mode is required in order to read/write data in the zone.

The encryption activation success is memorized and active as long as the chip is powered, unless a new initialization is initiated or a valid DESELECT or IDLE command is received. If the new encryption activation request is not validated, the card will no longer encrypt data during read operations nor will it decrypt data received during write or Check Password operations.

12.5 Checksum

The PICC implements a data validity check function in the form of a checksum. The checksum may function in standard or cryptographic mode. In the standard mode, the checksum is optional and may be used for transmission error detection. The cryptographic mode is more powerful since it provides data origin authentication capability in the form of a Message Authentication Code (MAC). To write data to the device, the host is required to compute a valid MAC and provide it to the device. If after an in going command the device computes a MAC different from the MAC transmitted by the host, not only is the command abandoned but the cryptographic mode is also reset. A new authentication is required to reactivate the cryptographic mode.

12.6 Initial Device Programming

CryptoRF is delivered with all security features disabled. To program the polling response or enable the security features of CryptoRF the device must be personalized by programming several registers. This is accomplished by programming the configuration memory using simple write and read commands. AT88RF04C supports an optional Secure Personalization mode which encrypts the secrets during programming.

12.7 Transport Password

To gain access to the configuration memory, a transport password known as the secure code must be presented using the Check Password command. The transport password for AT88RF04C is $30 1D D2.

13. Tuning Capacitance

The capacitance between the coil pins AC1 and AC2 is 82pF nominal and may vary ±10pF due to process variation.

14. Reliability

Table 14-1. Reliability

Parameter	Min	Typical	Max	Units
Write Endurance (Each Byte)	100,000			Write Cycles
Anti-tearing Write Endurance	50,000			Writes
Data Retention (At 55°C)	10			Years
Data Retention (At 35°C)	30	50		Years
Read Endurance	Unlimited			Read Cycles

15. Ordering Information

Ordering Code	Package	Tuning Capacitor	Max Range(1)	Temperature Range
AT88RF04C-MR1G	R Module	82pF	—	Commercial (0°C to 70°C)
AT88RF04C-MX1G	MX1 RFID Tag, 13mm square		5 – 13mm	Commercial (-25°C to 70°C)
AT88RF04C-MVA1	RFID Tag, 8.6mm x 18.1mm		10 – 15mm	
AT88RF04C-WA1	6mil Wafer, 150mm diameter		—	Industrial (-40°C to 85°C)

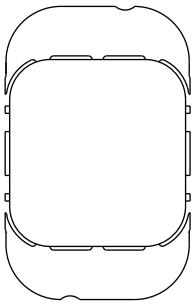
Note: 1. Communication range is dependent on the reader and reader antenna design.

Package Type	Description
R Module	2-lead RF Smart Card Module, XOA2 style, on 35mm tape, Ag finish, Green(1)
MX1 RFID Tag	13mm x 13mm Square Epoxy Glass RFID Tag on 35mm tape, Au finish, Green(1)
MVA1 RFID Tag	8.6mm x 18.1mm Rectangular Epoxy Glass RFID Tag on 35mm tape, Au finish, Green(1)

Note: 1. Lead-free, halogen-free package. Exceeds RoHS requirements.

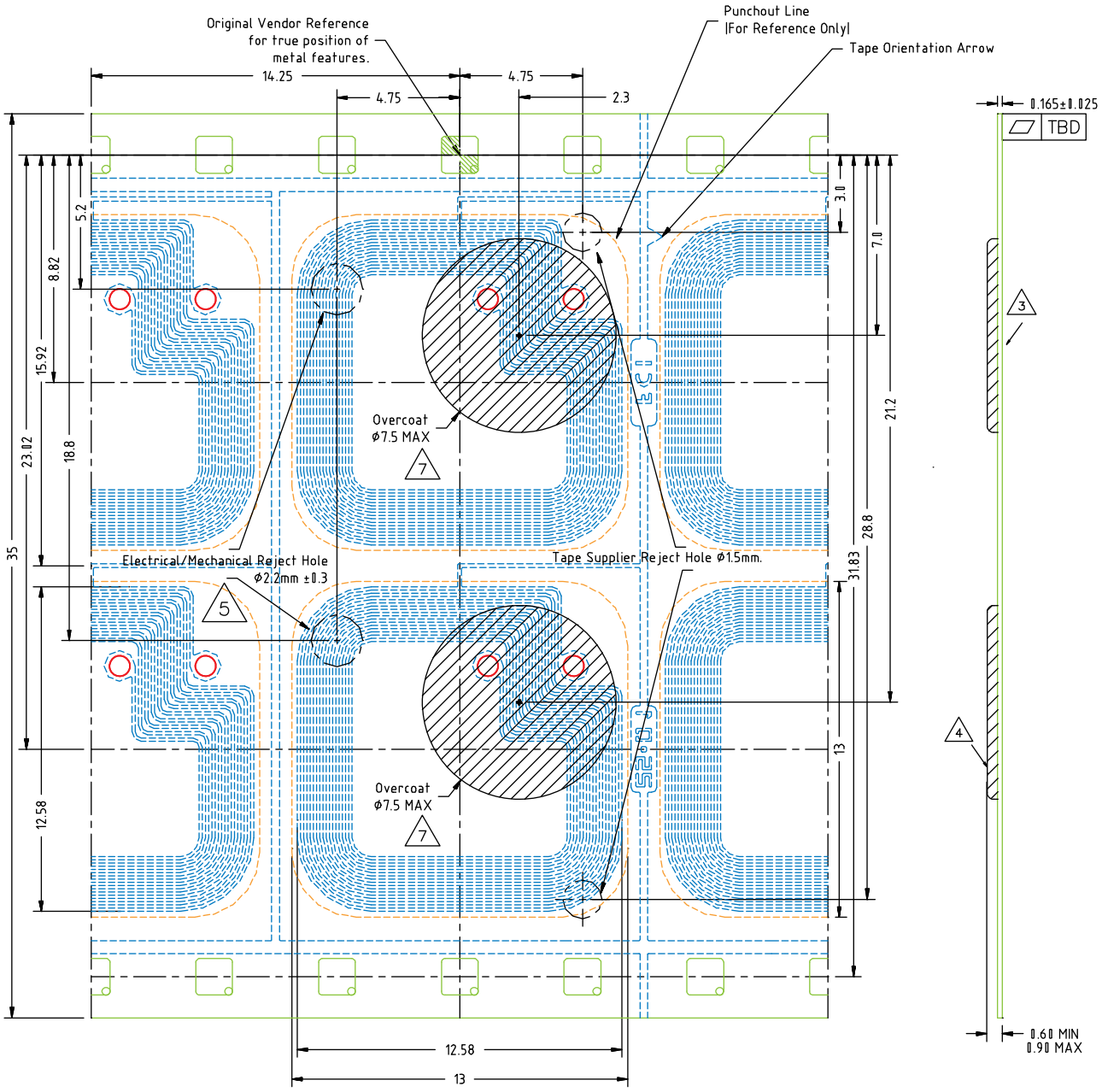
16. Packaging Information — Mechanical Drawings

16.1 Module R Package (XOA2 Style) — Ordering Code: AT88RF04C-MR1G

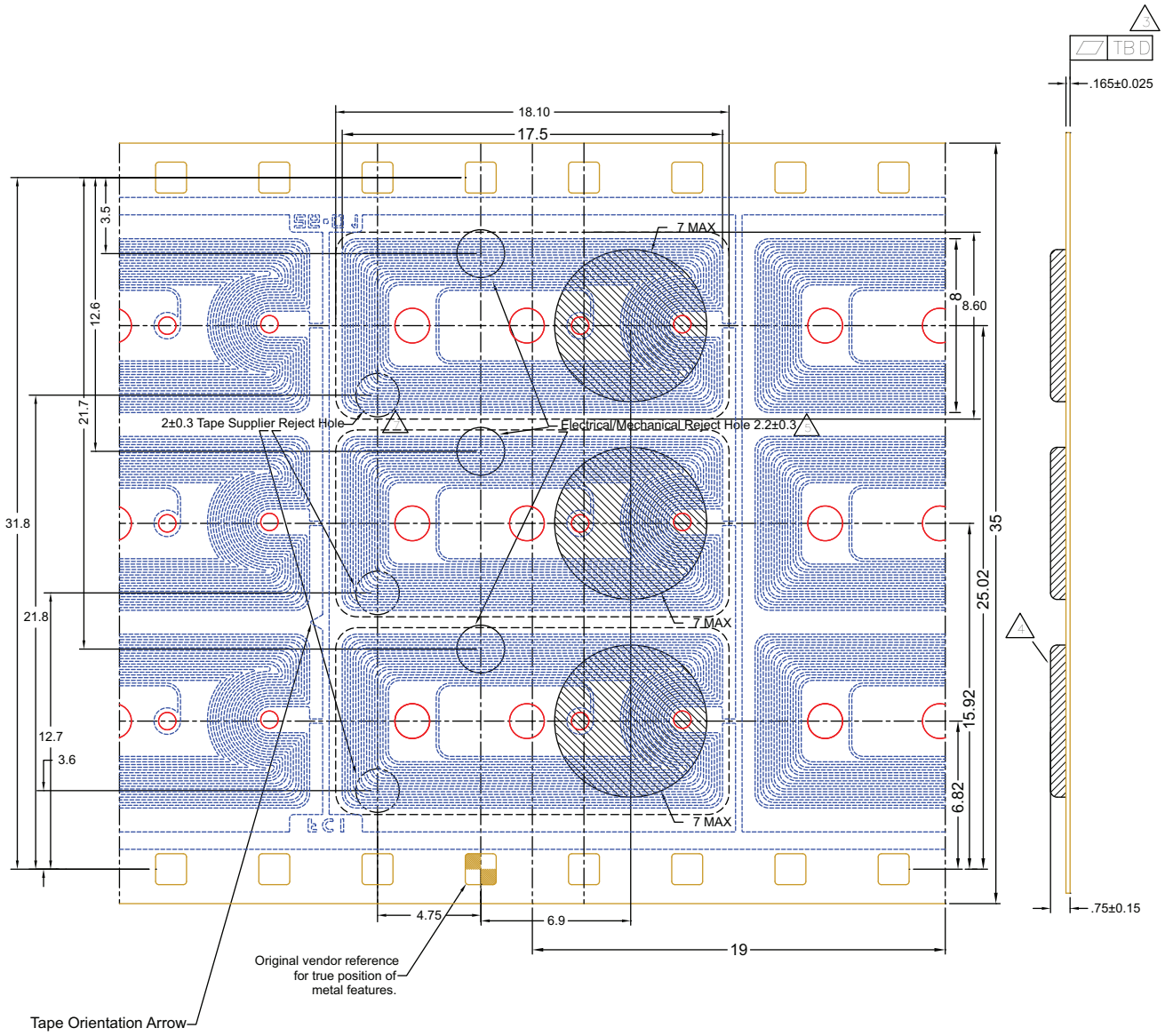


Module Size:	M5
Dimension:	5.06mm x 8.00mm
Glob Top:	Square – 4.8mm x 5.1mm
Thickness:	0.38mm
Pitch:	9.5mm

16.2 MX1 Epoxy Glass RFID Tag — Ordering Code: AT88RF04C-MX1G



16.3 MVA1 Epoxy Glass RFID Tag — Ordering Code: AT88RF04C-MVA1



17. Revision History

Doc. Rev.	Date	Comments
8672CS	01/2014	Add MVA1 ordering option. Remove enginerring samples section. Update footers and disclaimer page.
8672BS	08/2012	Remove MY1 package option.
8672AS	04/2009	Initial document summary release.

Atmel Corporation 1600 Technology Drive, San Jose, CA 95110 USA **T:** (+1)(408) 441.0311 **F:** (+1)(408) 436.4200 | **www.atmel.com**