AT88SC0104CRF to AT88SC6416CRF

FAMILY OF CRYPTORF™ SECURITY CHIPS

The AT88SC0104CRF to AT88SC6416CRF is a family of contactless secure memory devices with advanced security and cryptography.

Key Features

- A Family of Devices with User Memories from 1 Kbit to 64 Kbits:
  1K, 2K, 4K, 8K, 16K, 32K, 64K Bits
- Symmetrical Dynamic Mutual Authentication with 64-bit Cryptographic Keys
- Encrypted Passwords with Attempts Counters
- Stream Encryption Ensures Data Privacy
- Antitearing Recovers Data in Case of Power Loss
- Contactless 13.56-MHz Interface, Compliant with ISO/IEC 14443 Type B
- Integrated 82 pF Tuning Capacitor
- High Reliability Memory, 100K Write Cycles with 10 Year Data Retention

Applications

- Health Care Cards
- Security Focus ID Cards
  (Biometric ID Cards, Passports, etc.)
- Drivers Licenses
- E-purses
- Multi-applications

ATMEL

CRYPTORF™ CRYPTOGRAPHIC RF SMART CARD ICs

5038A-CRRF-04/03/10K

Atmel's CryptoRF™ is a new secure RF family of devices with memory densities from 1 Kbit (AT88SC0104CRF) to 64 Kbits (AT88SC6416CRF) for contactless smart card applications. This new family of secure RF circuits makes available to the industry a low cost, high security chip solution that fills the void between simple RFID memories and RF microcontrollers.

Security

This device contains a random number generator and proprietary algorithm that generates new keys for each authentication and encryption activation. Read and Write access requirements for each user zone are programmed by the customer during card personalization. The device's secret keys for mutual authentication and encryption are defined using a customer selected algorithm. Only a computer knowing both the CryptoRF and customer algorithms can provide the required authentication codes.

Product Features

- Contactless 13.56 MHz RF Communications Interface
  - ISO/IEC 14443-2: 2001 Type B Compliant
  - ISO/IEC 14443-3: 2001 Type B Compliant Anticollision Protocol
  - Command Set Optimized for Multicard RF Communications
  - Tolerant of Type A Signaling for Multiprotocol Applications
  - Operating Distance Up to 10 cm
- Integrated 82 pF Tuning Capacitor
- User Memory of 1 Kbit to 64 Kbit
  - User Memory Configured as 4, 8, or 16 User Zones
  - Byte, Page, and Partial Page Write Modes
  - Self-timed Write Cycle
- 2 Kbit (256-byte) Configuration Zone
  - User-programmable Application Family Identifier (AFI)
  - User-defined Anticollision Polling Response
  - User-defined Keys and Passwords

- High-Security Features
  - 64-bit Mutual Authentication Protocol (under exclusive patent license from ELVA)
  - Encrypted Checksum
  - Stream Encryption
  - Four Key Sets for Authentication and Encryption
  - Eight Sets of Two 24-bit Passwords
  - Password and Authentication Attempts Counters
  - Selectable Access Rights by Zone
  - Write Lock Mode
  - Antitearing Function
  - Tamper Sensors
- High Reliability
  - Endurance: 100,000 Write Cycles
  - Data Retention: 10 Years
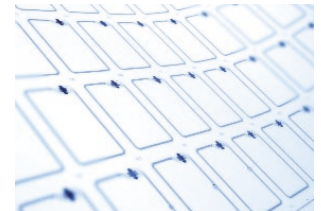 - Operating Temperature: -40 to +85°C

Package Options
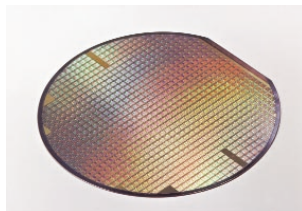
Wafer Form, Thinned to 6 Mils
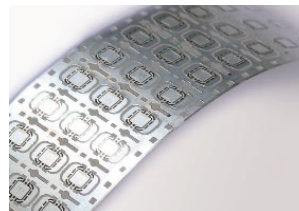
RF Smart Card Modules

Prelaminate Sheets

Development Tools

AT88SC6416CRF-EK Evaluation Kit, including RF reader and software
AT88SC6416CRF-DK Development Kit, including RF reader and software

Atmel contact: cryptorf@atmel.com