EM MICROELECTRONIC

A COMPANY OF THE SWATCH GROUP

FACT SHEET | em|aura-C

Subject to change without notice
Version 4.0, 22-March-18

www.emmicroelectronic.com

em | aura-C

Crypto-Enhanced RAIN RFID

UHF RFID Crypto Transponder IC

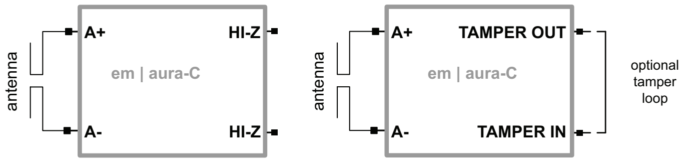
General Description

em|aura-C is a UHF RFID crypto transponder IC compliant with ISO/IEC 18000-63 (formerly ISO/IEC 18000 6 Type C) and EPC^{TM} Generation-2 Version 2 (Gen2 V2), also known as RAIN RFID. em|aura-C incorporates AES-128 and Grain-128A Crypto Suites (CS) defined by ISO/IEC 29167. The AES 128 CS provides security services for Tag authentication, interrogator authentication, mutual authentication and data exchange during authentication including key update. The Grain-128A CS provides security services for Tag authentication, mutual authentication, data exchange during authentication including key update and authenticated communication.

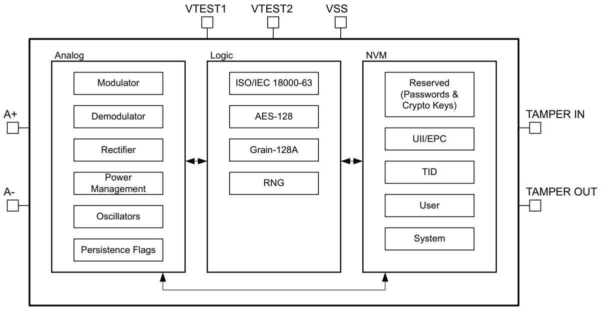
em|aura-C implements superior security features against man-in-the-middle, harvesting, and cloning attacks, therefore preventing the use of fake tags in secure applications. It also includes tamper detection capability for usage in high-security tags as well as a pseudo-random number generator (PRNG) meeting the highest US government security standards (NIST SP 800-22 compliant).

These security features enable the usage of em|aura-C based solutions in applications requiring a high level of security at a long range, such as road tolling, border crossing, and protection of high-value items. Its features allow tackling challenges such as cloning of tags, eavesdropping on the tag-reader communication, and impersonation of readers. Only genuine tags and readers can be used in an application, and the ciphertext data intercepted by a spoofing device cannot be used to create fake tags.

Typical Operating Configurations



Block Diagram



Features

- ISO/IEC 18000-63 compliant
- ISO/IEC 29167-10 (AES-128) compliant
- ISO/IEC 29167-13 (Grain-128A) compliant
- EPC^{TM} Generation-2 Version 2 compliant:
  - Alteration EAS compliant
  - Tag Alteration (Authenticate) compliant
  - Tag Alteration (Challenge) compliant
- NIST SP 800-22 compliant
- User configurable Cryptographic Suites (CS):
  - Enable AES-128 and/or Grain-128A
  - Assignment of keys to CS and key privileges
- High performance 3072-bit non-volatile memory:
  - Endurance of 100,000 cycles
  - Retention of 10 years @ 70ºC, 30 years @ 55 °C
  - BlockWrite operation for 1 to 8 words
- 32-bit Access and Kill passwords
- XTID with 48-bit serialization
- 416 bits for UII/EPC encoding
- User configurable memory options:
  - 6 crypto keys and 1280 bits of User memory
  - 2 crypto keys and 1792 bits of User memory
  - User Memory segments for public/private profiles
- Optional tamper detection via continuity loop
- Optional secure counter mode operation
- Read sensitivity up to -18.5dBm with dipole antenna
- Crypto sensitivity up to -18dBm with dipole antenna
- Write sensitivity up to -15.5dBm with dipole antenna
- Available in DFN package or bumped wafers

Applications

- Access control
- Product authentication
- Public transport
- Event ticketing

RAIN RFID is a trademark of the RAIN RFID Alliance.
EPC is a trademark of EPCglobal Inc.
DPA logo is a trademark of Cryptography Research, Inc.