ARMATURA

DESIGNED
& ENGINEERED
IN THE USA
ARMATURA

Armatura Encrypted RFID Card Solution for High-Security Access Control

What is RFID Card in Access Control Usage

RFID (Radio-Frequency Identification) cards are contactless smart cards widely used in physical access control systems. They enable fast, secure, and convenient user authentication at entry points without the need for physical contact. RFID cards are commonly used for:

- Employee or visitor identification
- Entry to restricted areas
- Secure time attendance logging

In high-security environments, standard RFID cards are insufficient due to vulnerabilities such as cloning or unauthorized duplication. To address this, encrypted RFID cards are implemented to provide secure mutual authentication and robust data protection.

ARMATURA

Format in DESFire (EV1, EV2, EV3) and Encryption Advantage

MIFARE DESFire cards are high-security RFID smart cards developed for advanced access control systems.
They are available in three main generations: EV1, EV2, and EV3.

Version Key	Version Key Features	Security Standard
EV1	Supports 3DES, fast transaction, multiple applications	ISO/IEC 14443
EV2	Adds AES128, improved file management, proximity checks, enhanced key diversification	3DES, AES-128, Random ID
EV3	Adds Secure Messaging, Transaction MAC, EAL5+ Certification, enhanced key diversification	Common Criteria EAL5+, AES-128, 3DES, 3K3DES

Encryption Advantages:

- Advanced encryption (3DES, AES-128, 3K3DES) for strong data protection
- Prevents unauthorized access and card cloning
- Enables secure, encrypted communication between card and reader
- Supports key diversification and random IDs for enhanced security

ARMATURA

What Armatura Can Do to Enhance Security

Armatura provides a complete ecosystem for managing encrypted RFID cards, ensuring high-level security and operational efficiency.

1. Secure Card Issuance Process (Master Key Configuration)
2. Identity Authority Process (Authentication with Armatura Readers)

Together, these functions enhance system integrity and prevent any unauthorized duplication or use of RFID credentials.

Secure Card Issuance
(Master Key Configuration)

Armatura
Desfire（EV1, EV2, EV3)

+

EP20ENC
Card Enroller

=

High-security format of EV1, EV2, and EV3
with 3DES, AES-128 and 3K3DES

Identity Authority Process
(Authentication with Armatura Readers)

High-security format of EV1, EV2, and EV3
with 3DES, AES-128 and 3K3DES

+

EP20CKQ
(RNI, SFMH)

=

1. Secure Card Issuance (Master Key Configuration)

- Use Armatura EP20ENC Enroller to clone a DESFire card securely
- Apply Master Type Configuration: 3DES / AES / 3K3DES
- Supports full encryption programming and key definition

EP20 ENC
Intelligent Multi-tech Enroller

- RFID Reading and Cloning Capabilities
- USB Plug and Play
- Housing Material Meets UL94-V0 Standard
- Designed For Advanced Security

USB Plug and Play
ENCRYPTION AES 256 ENCRYPTION
100% SECURE TLS CERTIFIED
CERTIFIED CC EAL6+ CERTIFIED
OSDP™
ARMATURA
EP20 ENC
ARMATURA

ARMATURA

2. Identity Authority Process (Authentication with Armatura Readers)

- Use Armatura Reader and Terminal to read DESFire EV1, EV2, and EV3 cards
- Cards are authenticated using advanced hardware-based encryption
- Ensures secure transaction and verification of card identity

Messages (2) Pending Messages (2)

See All Messages>>

Meeting Room
Central Meeting Room Alarm Report
2022-01-25 18:52 2022-01-25 19:01

Main Entrance
Gate II Alarm Report
2022-01-26 16:42 2022-01-26 20:03

Access Alert Emergency
Connected
192.168.134.102
2022-0326 8:05:52

Access Alert Important
Connected
192.168.134.102
2022-0326 8:05:52

Access Alert General
Connected
192.168.134.102
2022-0326 8:05:52

Access Alert Prompt
Connected
192.168.134.102
2022-0326 8:05:52

ARMATURA

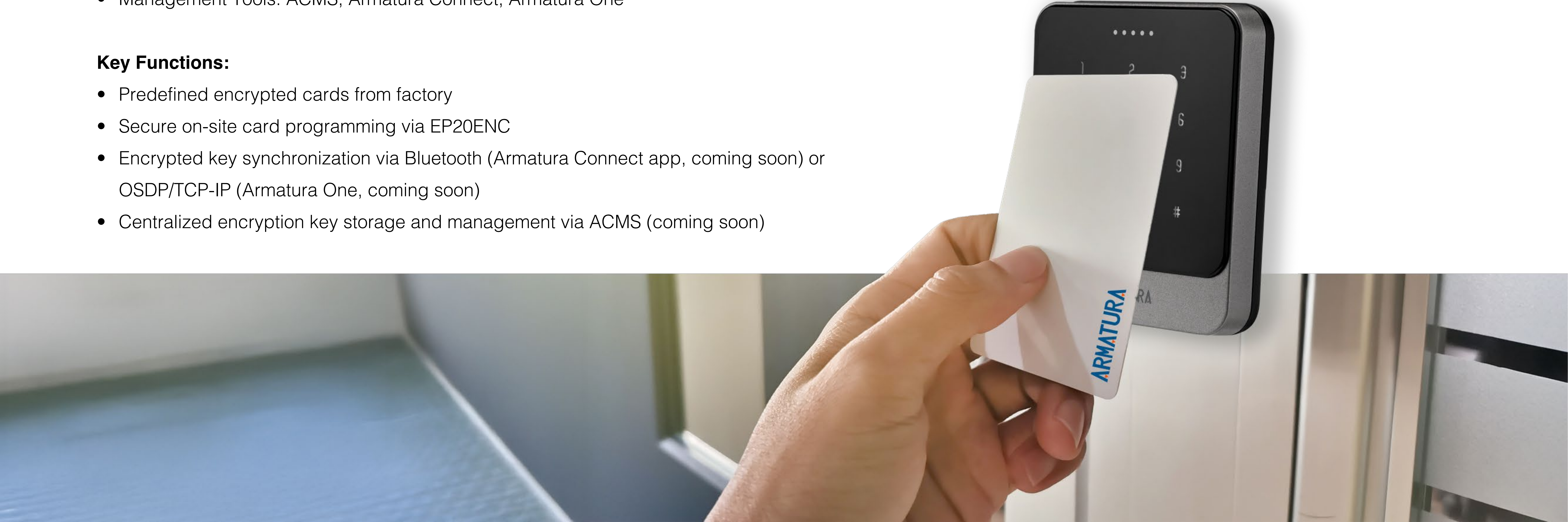
Architectural & Engineering Overview (Highlights)

Components Supported:

- Cards: MIFARE DESFire EV1, EV2, EV3
- Readers & Enrollers: EP10C, EP20 Series, EP30CF, VG10CKQ, OmniAC20/30, FT10CMQ
- Encryption: 3DES, AES, 3K3DES
- Management Tools: ACMS, Armatura Connect, Armatura One

Key Functions:

- Predefined encrypted cards from factory
- Secure on-site card programming via EP20ENC
- Encrypted key synchronization via Bluetooth (Armatura Connect app, coming soon) or OSDP/TCP-IP (Armatura One, coming soon)
- Centralized encryption key storage and management via ACMS (coming soon)



ARMATURA

Key Benefits of the Armatura Encrypted Card Solution

1. Multi-Layered Data Protection

Armatura's solution leverages strong encryption standards such as 3DES, AES, and 3K3DES to safeguard sensitive card data. The encryption keys are securely generated, stored, and synchronized across the ecosystem using the ACMS platform, preventing unauthorized duplication and access.

2. Simplified and Secure Card Issuance

Organizations can order factory-preconfigured encrypted cards with predefined security settings, eliminating manual errors. For customized setups, the EP20ENC enroller enables administrators to securely program encryption parameters and issue cards on-site with ease.

3. Flexible and Centralized Key Management

Encrypted keys can be securely distributed to readers and terminals through:

- Armatura Connect
  Bluetooth-based mobile application for device configuration and key distribution. (Coming Soon)
- Armatura One
  OSDP for readers and TCP/IP for terminals. (Coming Soon)
- ACMS (Armatura Card Management System)
  All keys are centrally managed via ACMS, ensuring consistent and synchronized deployments across all endpoints. (Coming Soon)

ARMATURA

Key Benefits of the Armatura Encrypted Card Solution

4. Scalable System Management

Whether managing one site or hundreds, the ACMS platform acts as the centralized brain of the system. It supports real-time updates, key rotation, and user management while providing complete visibility and control to system integrators or administrators.

5. High-Speed Performance for Large Deployments

Armatura's solution ensures fast authentication and transaction speeds below 100 milliseconds. This makes it ideal for enterprise-grade and high-traffic environments where user experience and speed are critical.

6. Long-Term Reliability and Endurance

MIFARE DESFire cards used in this solution are made with industrial-grade materials that withstand daily wear-and-tear. Their durability and long read/write lifecycle reduce the need for frequent card replacement.

7. Seamless Integration with Existing Systems

All hardware and cards are compliant with ISO/IEC 14443 A, making them compatible with most international systems. Readers like OmniAC20, OmniAC30, and FT10CMQ support encrypted formats out of the box, making integration fast and effortless.

Supported Products

Armatura's encrypted card solution is built on a robust product ecosystem that supports secure issuance, encryption, and management across a wide range of environments.

Readers & Terminals

- EP10C*: High-performance outdoor access readers
- EP20 Series*: Supports both standard and encrypted cards
- EP30CF*: Multi-function access controller with encryption compatibility
- VG10CKQ*: Versatile reader with secure authentication engine
- Standalone Terminals: OmniAC20*, OmniAC30*, FT10CMQ* with full encrypted card support (Coming Soon)

Enroller

- EP20ENC*: Secure, intelligent enroller for card cloning and encryption configuration

Software & Platforms

- ACMS (Armatura Card Management System):
  Central hub for key management and encryption policies. (Coming Soon)
- Armatura One:
  Software suite for access control configuration and encrypted key distribution (Coming Soon)
- Armatura Connect:
  Mobile app for Bluetooth-based device configuration and key sync (Coming Soon)

* Only the RNI and SFMH versions of products marked with an asterisk (*) support Desfire EV3, including DES, 3DES, and 3K3DES encryption formats.

ARMATURA

ARMATURA

Address:190 Bluegrass Valley Parkway Alpharetta, GA 30005
Phone: +1-650-4556863
Email: sales@armatura.us
Website: www.armatura.us