C·CURE IQ

Modern Physical Access Control and Credential Security Strategies – ISSA Sacramento Chapter

September 18, 2026

Matt Varvais

Area Sales Manager – CA, NV, HI

Software House

Johnson Controls

About Me

Experience

- Started in physical security industry in 2006
- Worked for Sacramento-based systems integrator from 2006 to 2022
- Joined Software House as Area Sales Manager in 2022

Hobbies and Interests

- Baseball, movies, outdoors

What is Access Control?

NIST
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

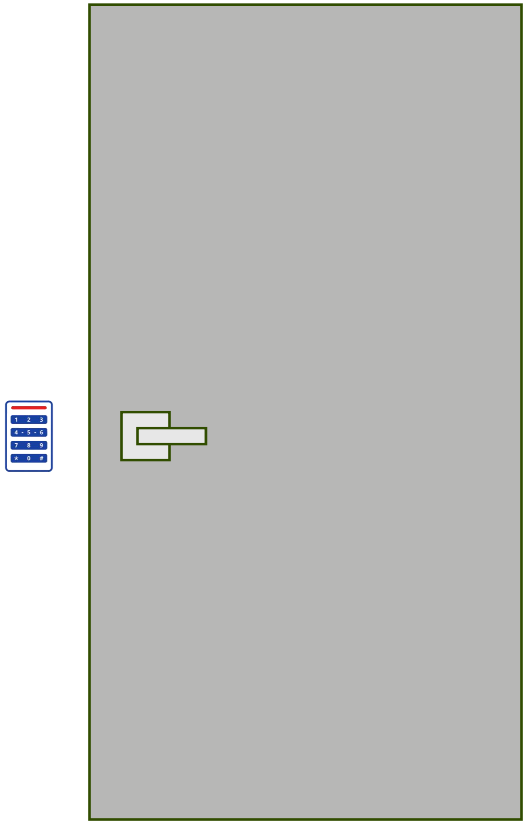
physical access control system

Definition:
An electronic system that controls the ability of people or vehicles to enter a protected area by means of authentication and authorization at access control points.

Also Known As

PACS

ACS



Integrated Security Ecosystem

Open Platforms and Protocols

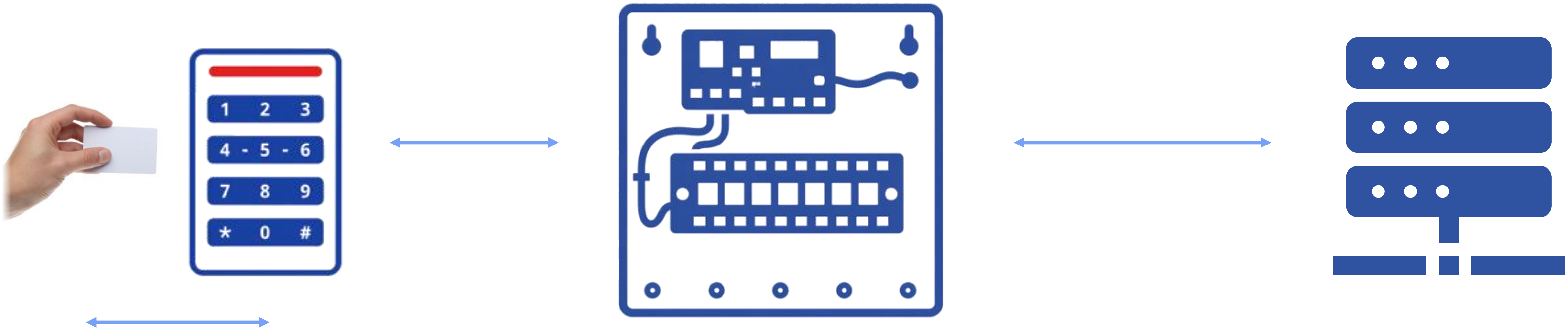
- Utilizing open protocols to allow for solutions to share important data between systems easily
- Open APIs allow for customized integrations and deep data management through multiple end points
- Streamline operations for efficiencies

C·CURE IQ

The natural evolution of C•CURE and victor into a modern, unified security platform

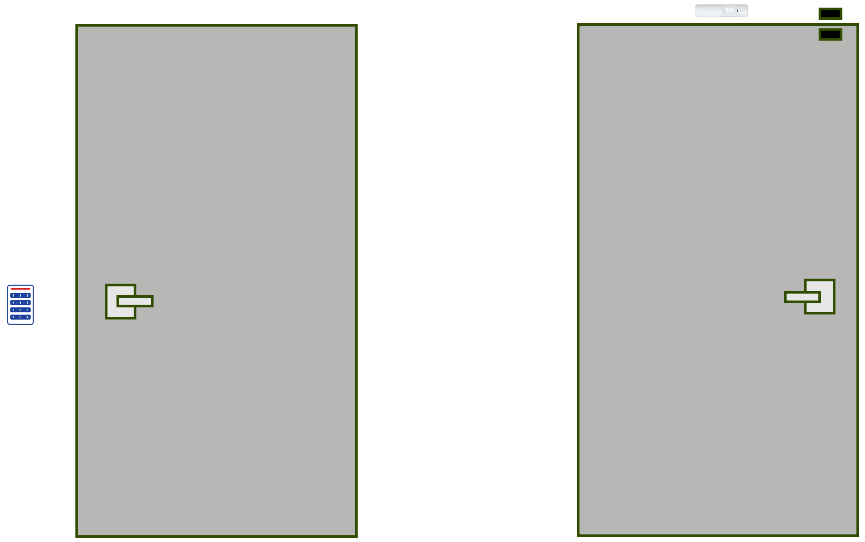
Johnson Controls

Credential Transaction Path Vulnerability Areas



Other PACS Basic Door Components

- **Door Position Switch –** A device used to monitor the open/close status of the door and send it back to the PACS control panel.
- **Request to Exit Sensor –** A device that detects a person exiting through a door and sends an authorized exit signal to the access control system, preventing false "Door Forced" alarms.
- **Electrified Lock –** An electronically controlled locking device that interfaces with an access control system to secure a door and allow authorized access through credential presentation, remote commands, or programmed schedules.



Non-Secure Side **Secure Side**

Door Position Swich

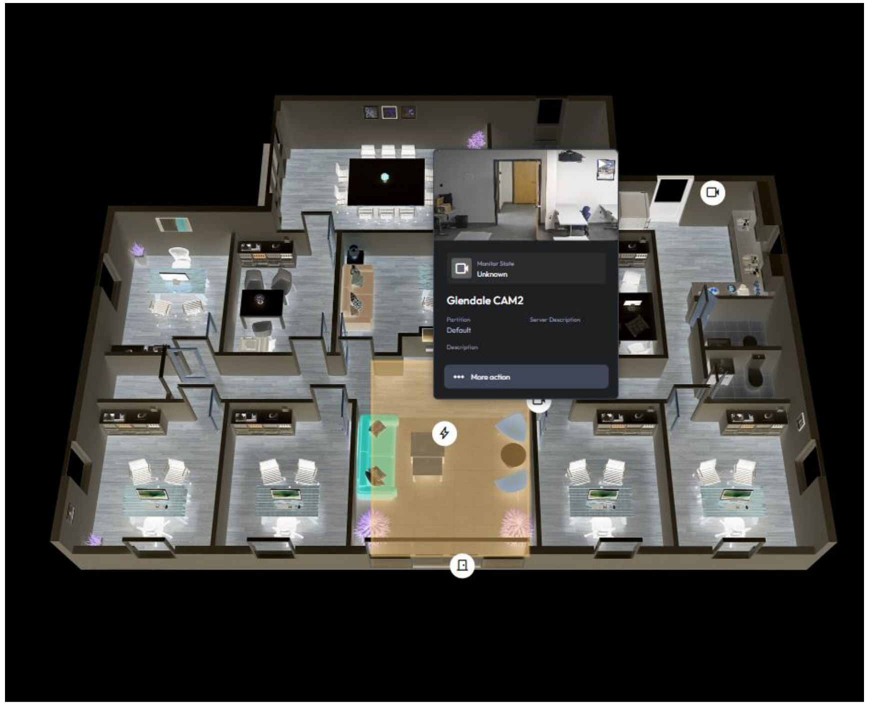
Request to Exit

Electrified Lock

Standard Door Status Types Explained

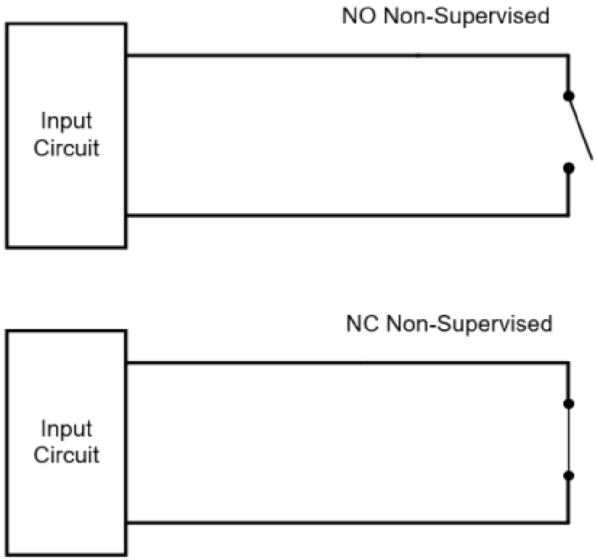
- **Door Closed –** The door position switch (DPS) indicates the door is closed and secured.
- **Door Open –** The DPS indicates the door is physically open. No alarm state is indicated.

- **Door Forced Open –** The DPS indicates the door is physically open. An alarm generated when a secured door is opened without a valid credential, authorized request-to-exit, or scheduled unlock action.
- **Door Held Open –** The DPS indicates the door is physically open. Door was opened properly but remained open longer than the configured time limit.
- **Alarm Fault/Trouble –** A trouble condition indicates that the system can no longer reliably monitor a device or circuit.
  - Examples:
    - Dead Short
    - Open Circuit (wire cut or broken)
    - Incorrect wiring/ incorrect resistance value



Why Supervision is Important

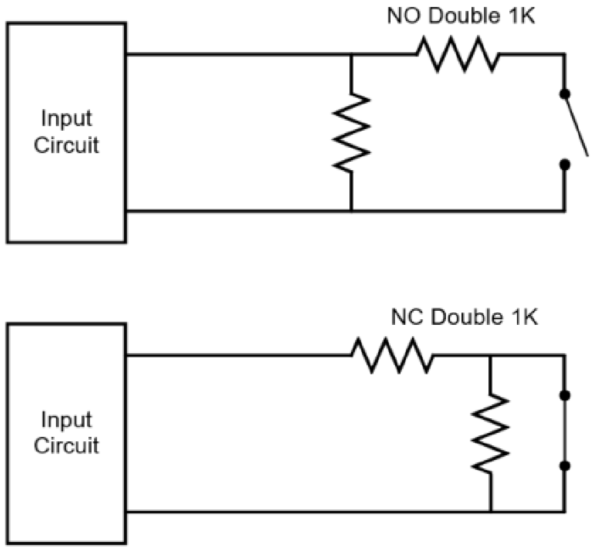
Figure 22: Non-supervised NO and NC



This method reports:

- Short.
- Open (>30K)

Figure 18: NO/NC Double EOL 1K Supervision



This method reports:

- Short
- Alert (500 ohms)
- Normal (1K)
- Alert (2K)
- Line Fault (Any unexpected value. This is usually due to incorrect value resistors or faulty resistors).
- Open (>30K)

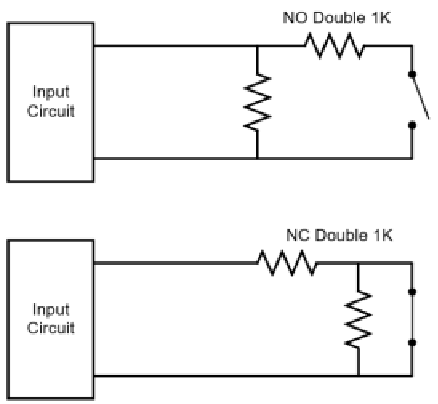
How Door Position Switch Works

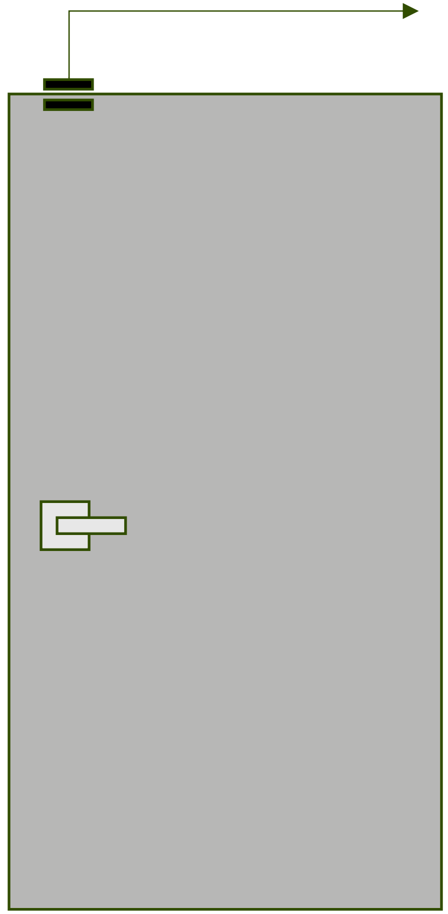
Also Known As

Door Contact

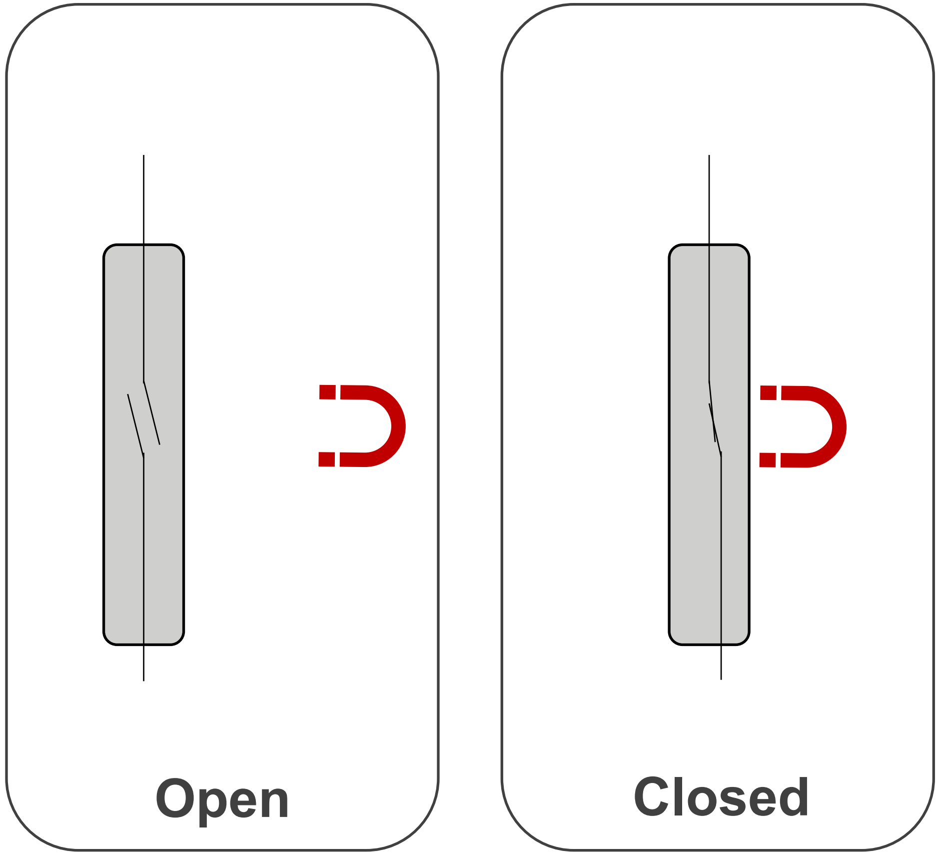
DPS (Door Position Switch)

Figure 18: NO/NC Double EOL 1K Supervision





Reed Switches Explained

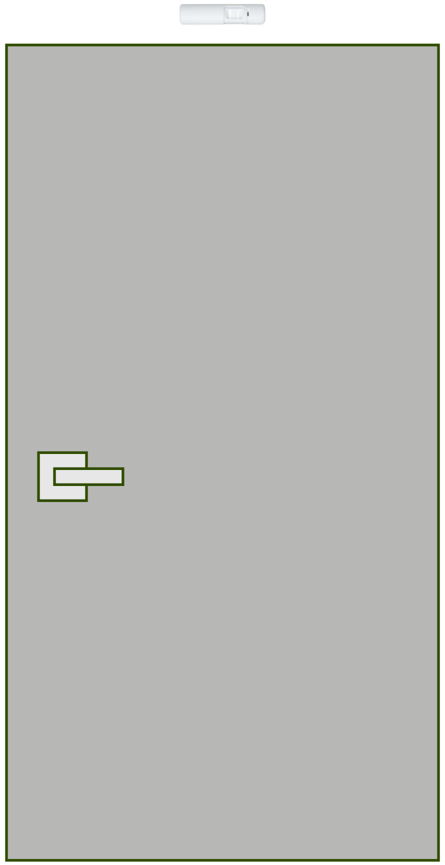


How Request to Exit Sensor Works

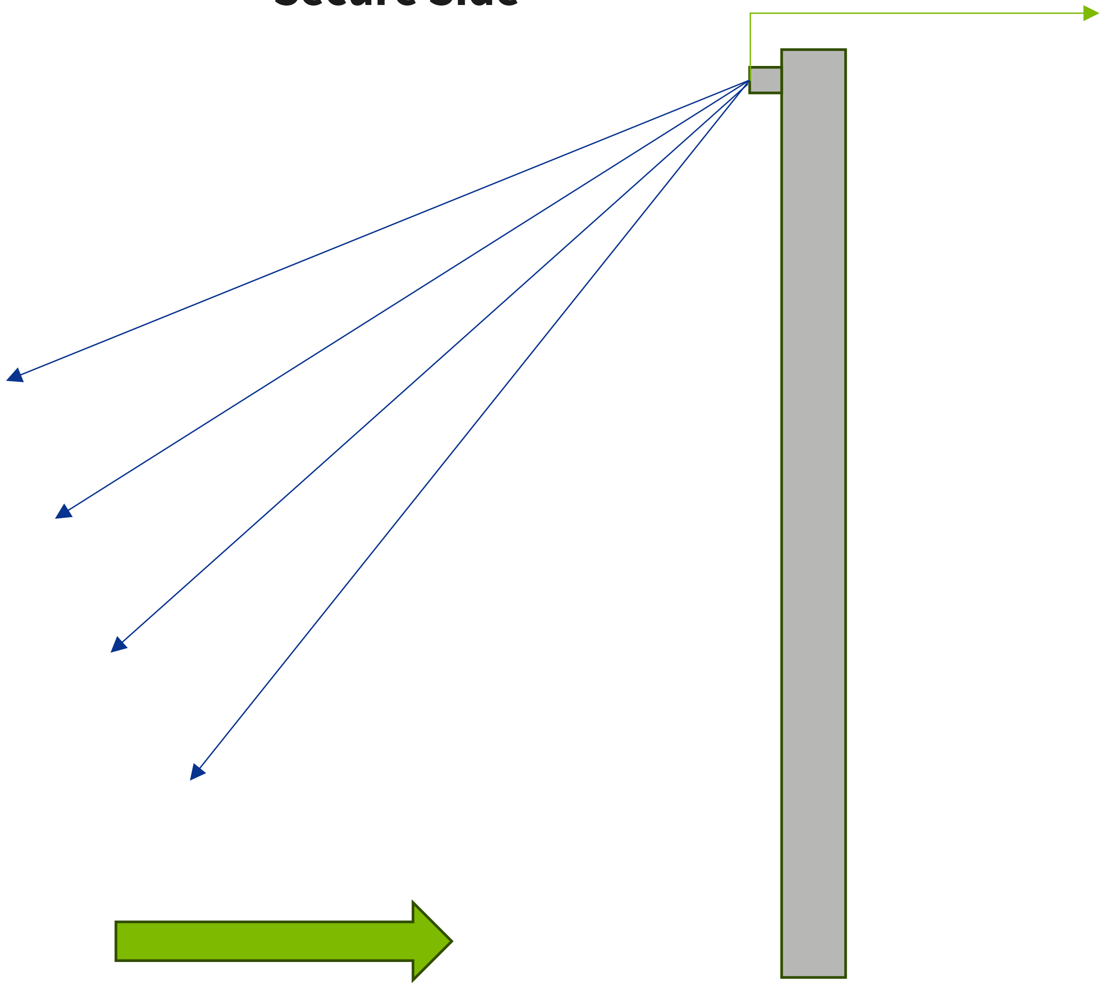
Also Known As

REX

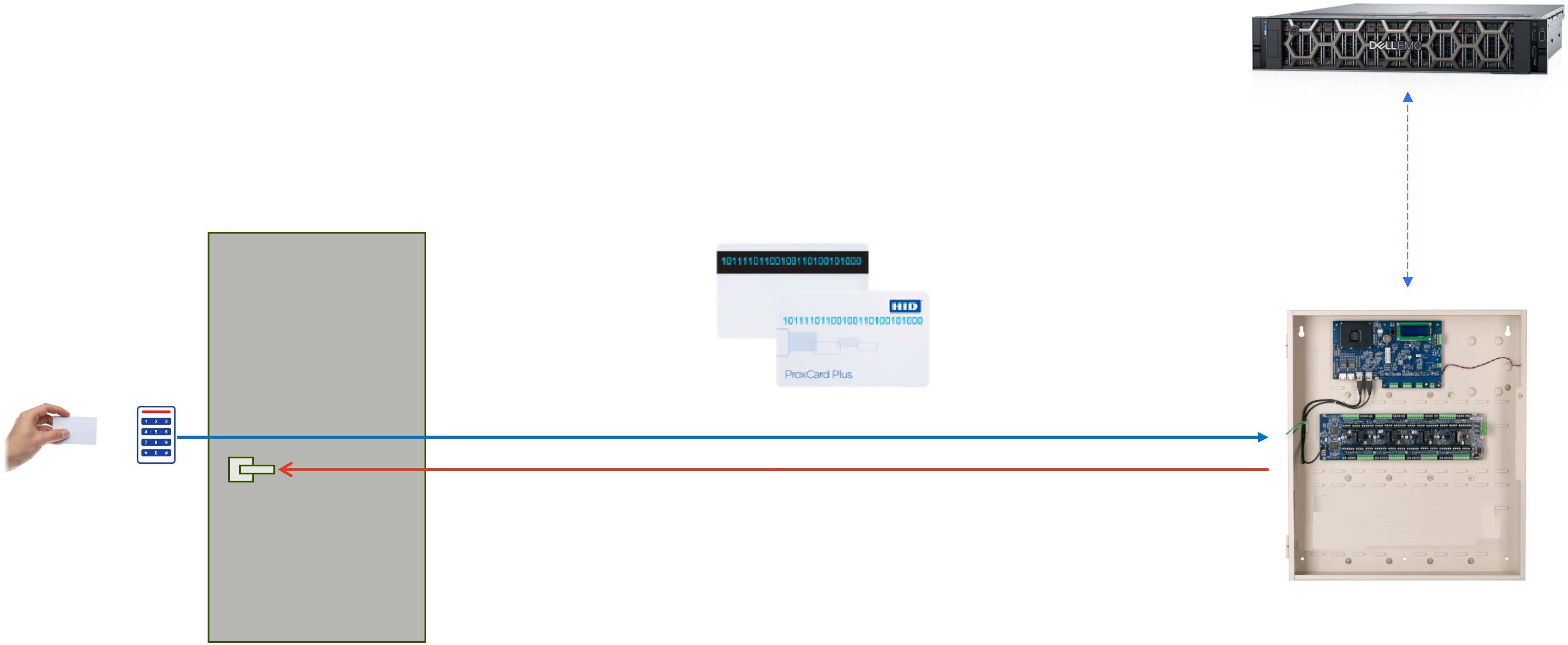
RTE



Secure Side



PACS Transaction Path



How Raw Credential Data Works

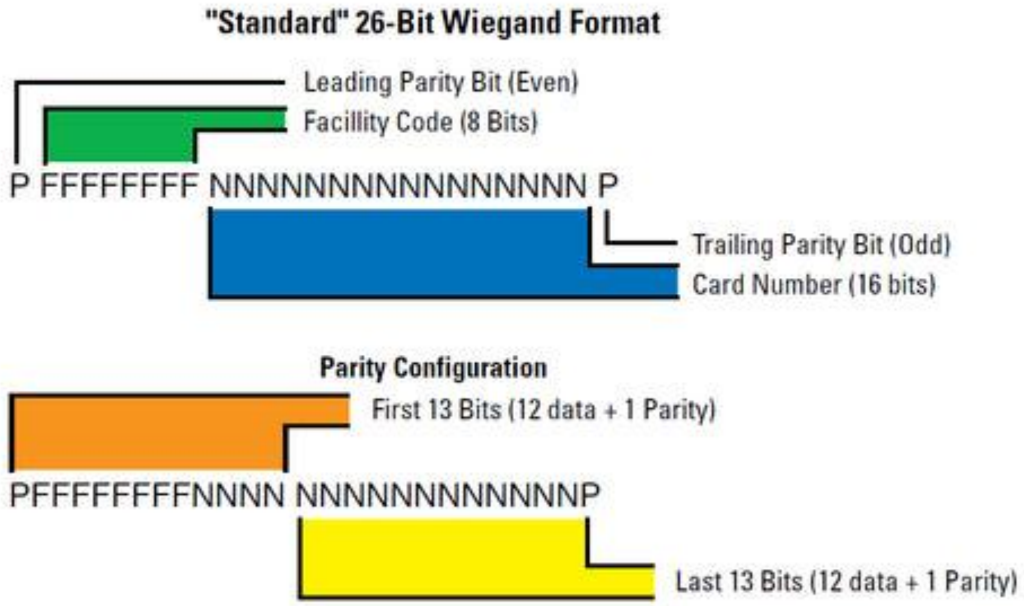
Classic 26-Bit Structure (example for simplicity)

- The 26 bits transmit sequentially as: P + AAAAAAAA + BBBBBBBBBBBBBBBB + P
- P (Parity): 1 leading odd parity bit and 1 trailing even parity bit.
- A (Facility Code): 8 bits, allowing for codes ranging from 0 to 255.
- B (Card Number): 16 bits, providing a unique ID range from 0 to 65,535 per facility code.

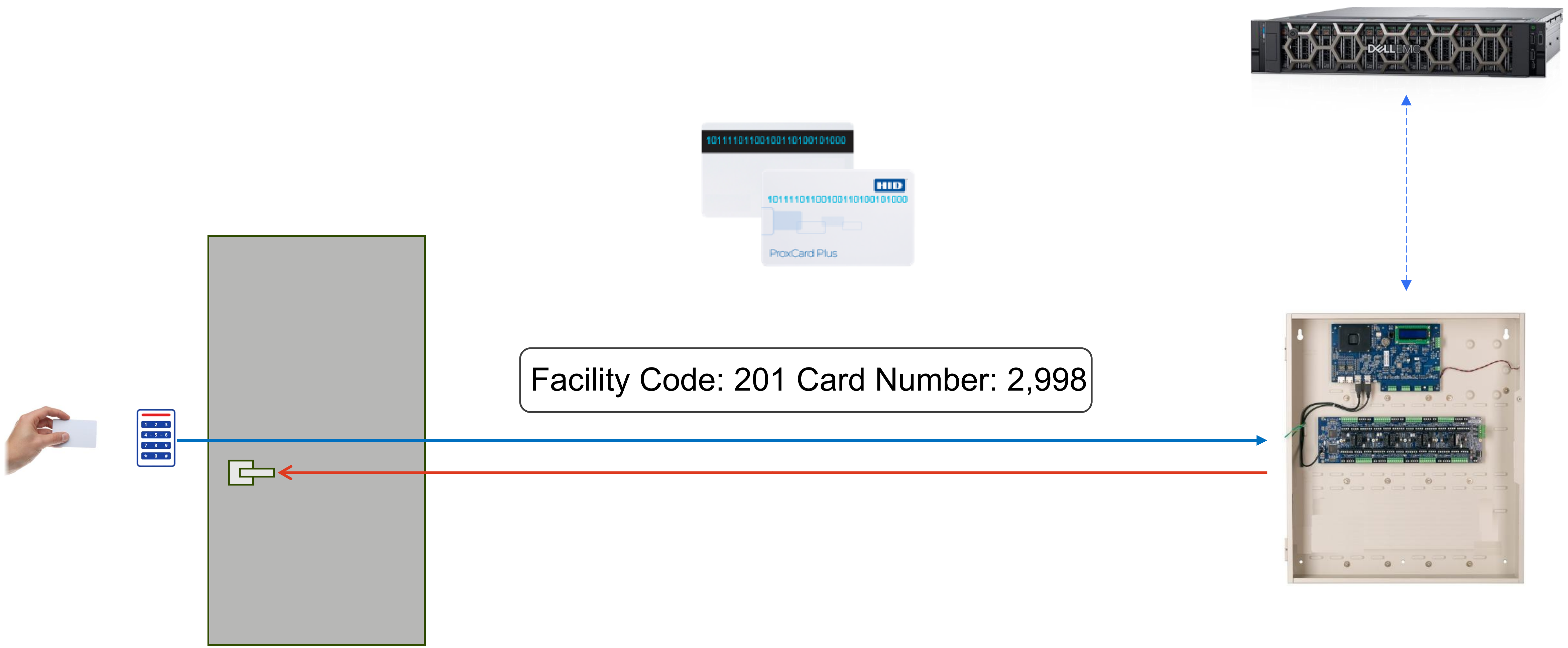
- When broken down by the system:

  11001001000010111011011 0

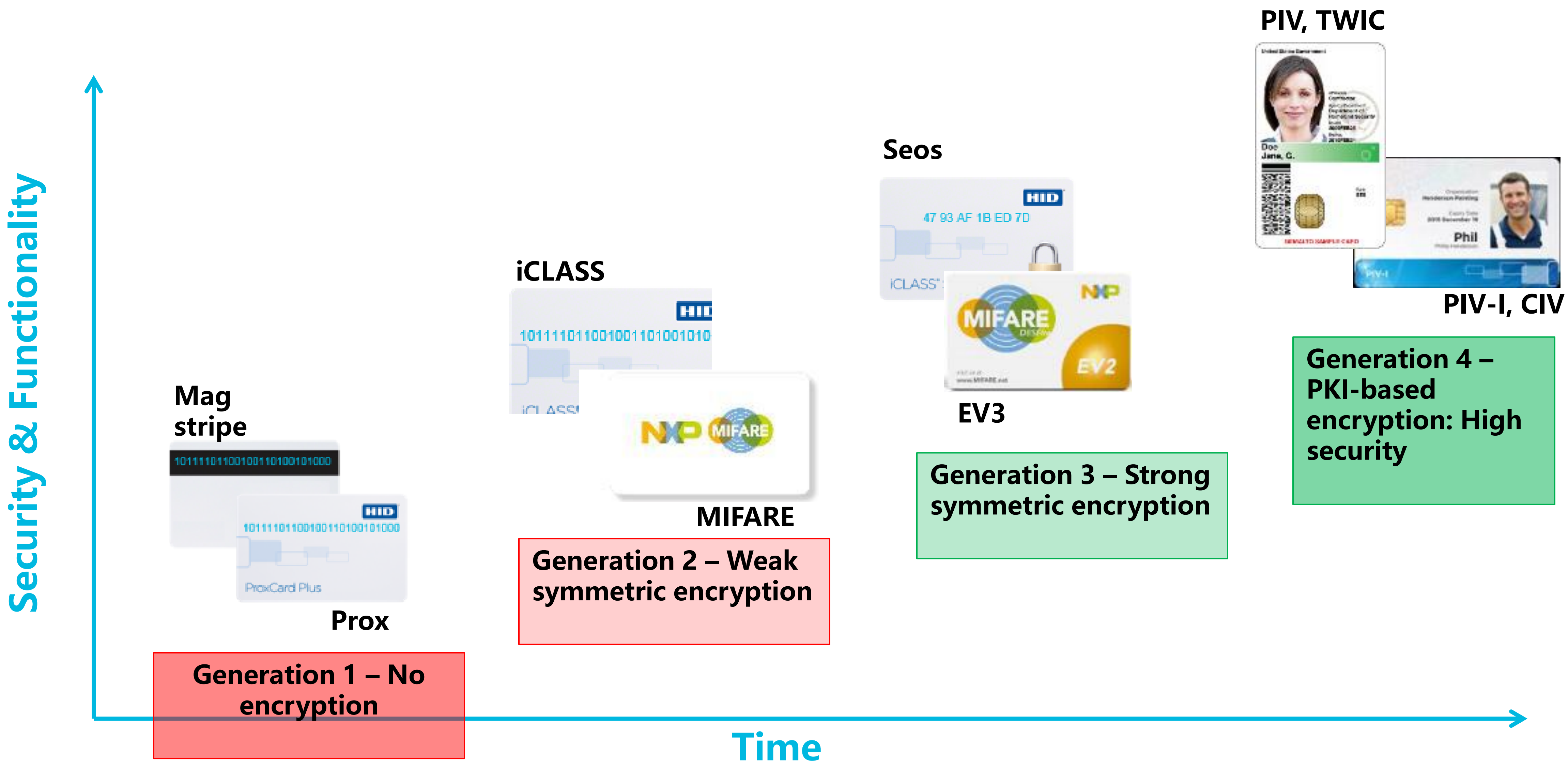
- Facility Code: 11001001 (Binary) = 201
- Card Number: 0000101110110110 (Binary) = 2,998



PACS Transaction Path

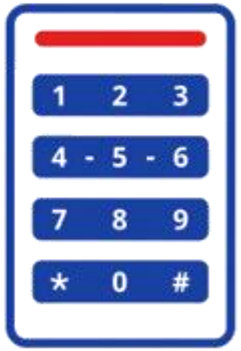


Personnel identification is constantly being upgraded

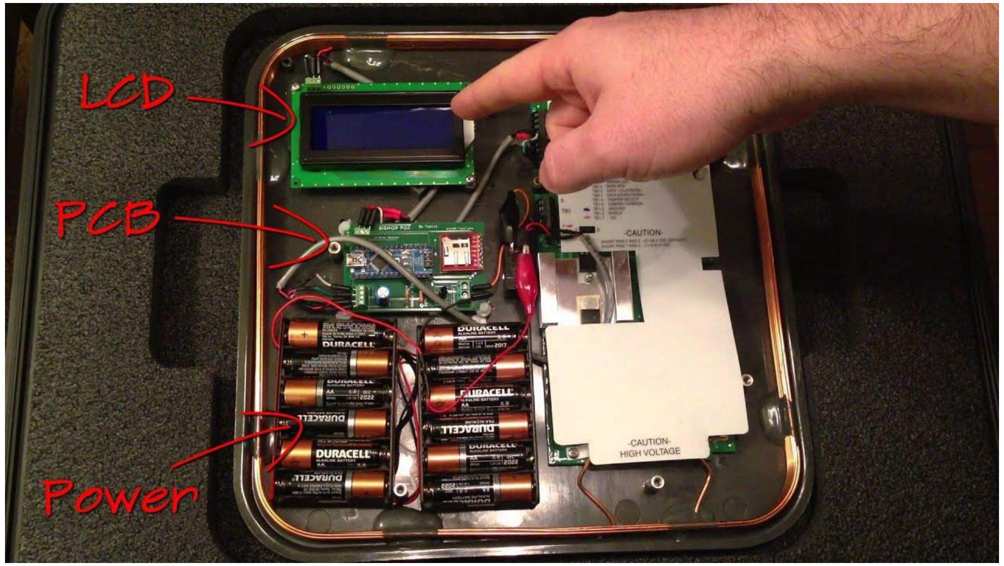


Low Frequency (125 kHz) Credentials Explained

1011110110010011010010100 0



- **With Low Frequency prox:**
  - Reader energizes credential and asks for data
  - Card sends identifier
  - Access system compares number to database
- **The credential does not authenticate the reader**
- **The reader does not authenticate the credential**
- **The same number is transmitted every time**

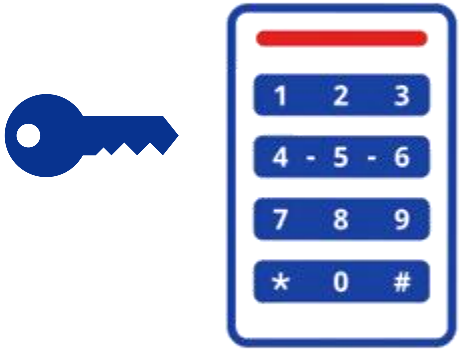


How High Frequency (13.56 MHz) Encryption Works

- **With High Frequency credentials:**
  - Reader and card exchange cryptographic challenges
  - The credential proves it possesses a secret key
  - Simply copying the card number is insufficient
- **Reader will only accept access attempts from credentials using correct encryption key**

10111101100100110100101000

- AES-128/2TDEA cryptographic algorithms for data protection
- Mutual authentication protocol with generation of diversified session key to protect each card session (using secure messaging)



Credential Options (in Private Sector)

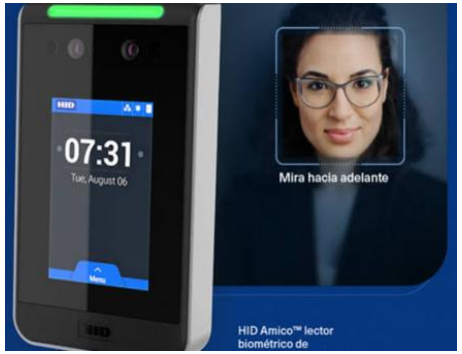
Classic Card

- Multi-tech options for low frequency and high frequency
- Options for logical access

Mobile

- Options for NFC and BLE (NFC being more secure)
- Can support phones, wearables, etc.

Biometric



Options for:

- Fingerprint
- Hand
- Palm Vein
- Iris
- Facial authentication

FIDO2

- Still uses same high frequency technology for physical access
- FIDO2 sector used for logical access

Benefits of High Frequency Credentials

Stronger Encryption

- Many high-frequency credential technologies support cryptographic authentication.
- Makes card cloning significantly more difficult than standard 125 kHz proximity cards.

Mutual Authentication

- The card and reader can verify each other's authenticity before exchanging data.
- Helps prevent credential cloning.

Unique Secure Keys

- Credentials can contain secure keys that are difficult to extract or duplicate.

User Experience Benefits

Mobile Credential Support

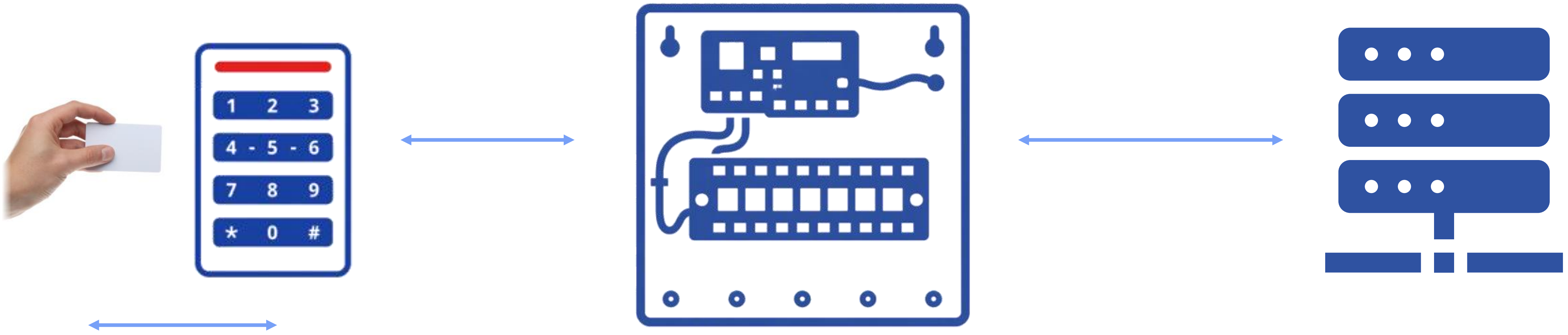
- The same reader platform can often support smartphones via NFC or Bluetooth.
- Enables digital badges and reduced dependence on physical cards.

Multi-Application Capability

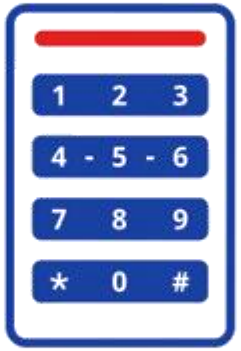
One credential can support:

- Building access
- Secure Printing
- Time and attendance
- Cashless payments
- Parking

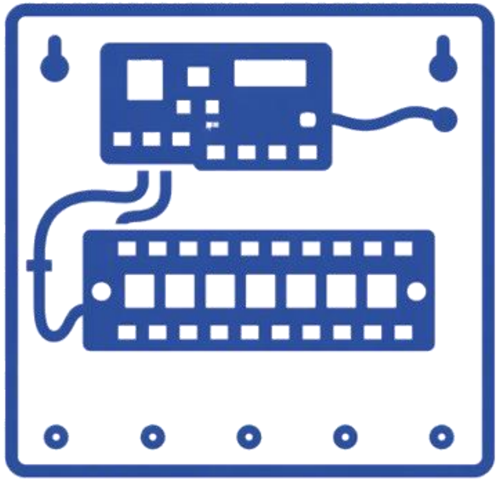
Card Transaction Path Vulnerability Areas



How Reader Data is Transmitted (Legacy Tech)

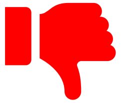


10111101100100110100101000

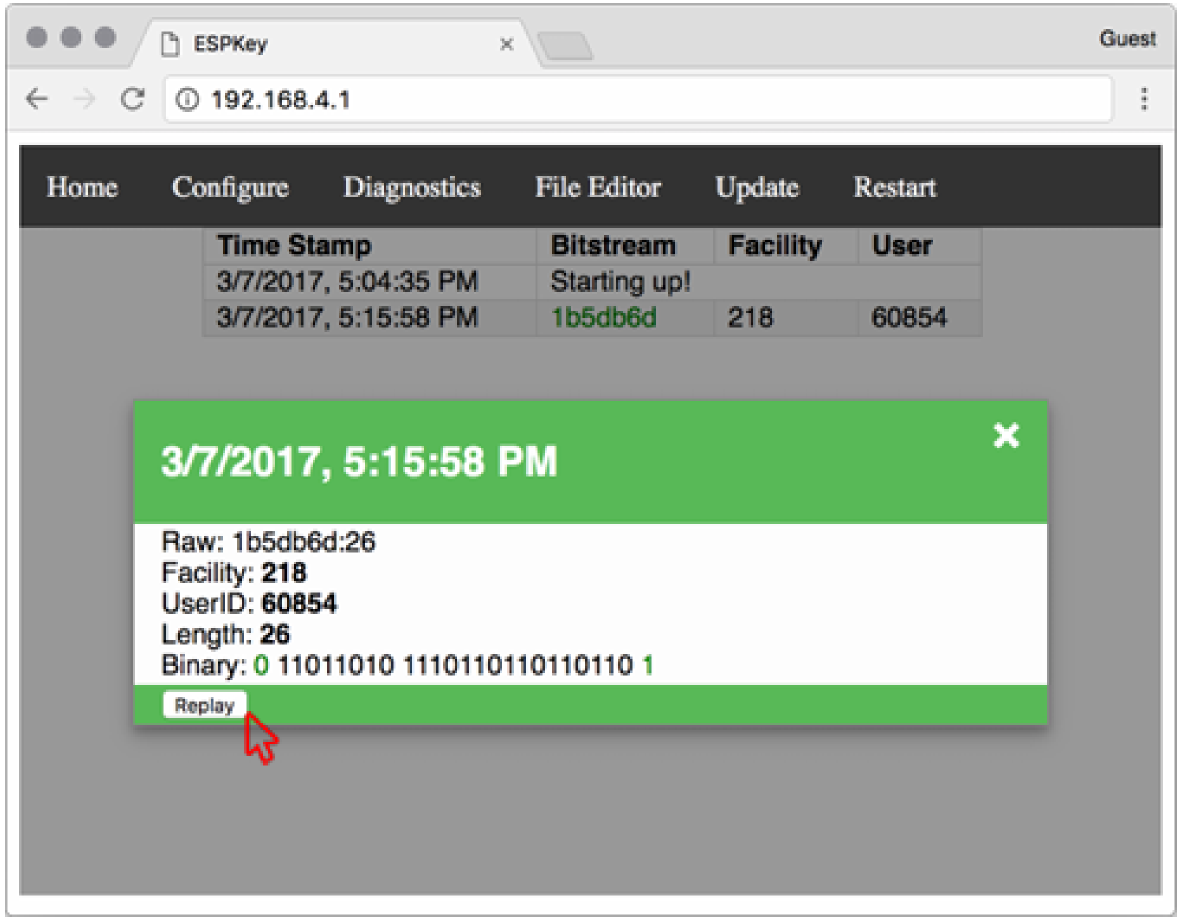


Weigand
(Legacy Technology)

- Most Common
- Uni-Directional data transmission
- Unprotected raw data transmission



How ESP Key Works



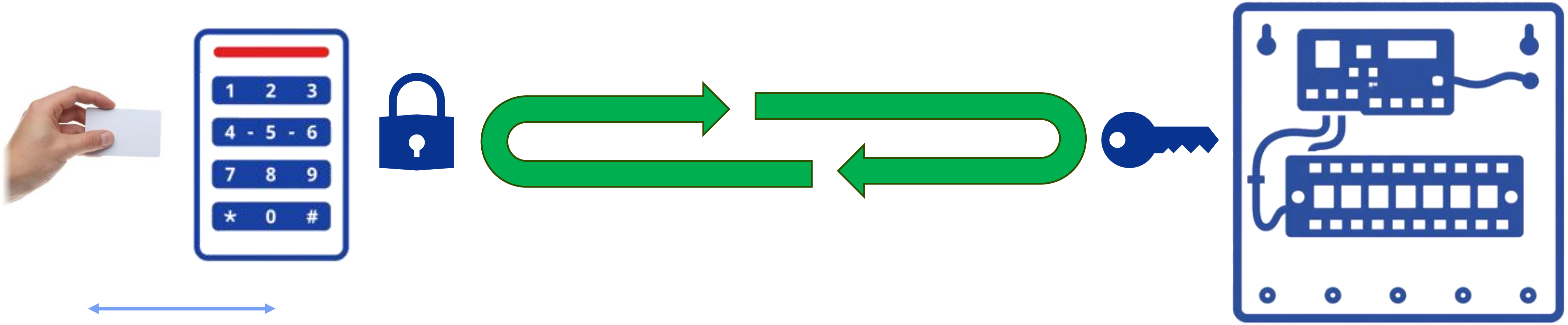
- Device connects to reader power and data circuits.
- When a badge is presented, the reader sends credential data to the controller.
- Device can observe and record that data stream while remaining transparent to normal operation.
- Device can save credential data to onboard memory or replay the transaction.

How Reader Data is Transmitted (OSDP)

10111101100100110100101000

OSDP
(Open Supervised Device Protocol)

- Modern and recommended deployment method
- Bi-Directional Communication
- AES 256 Encryption



Benefits of OSDP

Improved Security

- Encrypted communication between reader and controller using Secure Channel.
- Protects against credential data interception and replay attacks.
- More secure than unencrypted Wiegand communications.

Simplified Installation

- Uses a single 4-conductor RS-485 communication bus instead of multiple conductors required by Wiegand.
- Reduces cable complexity and installation costs.
- Supports longer cable runs.

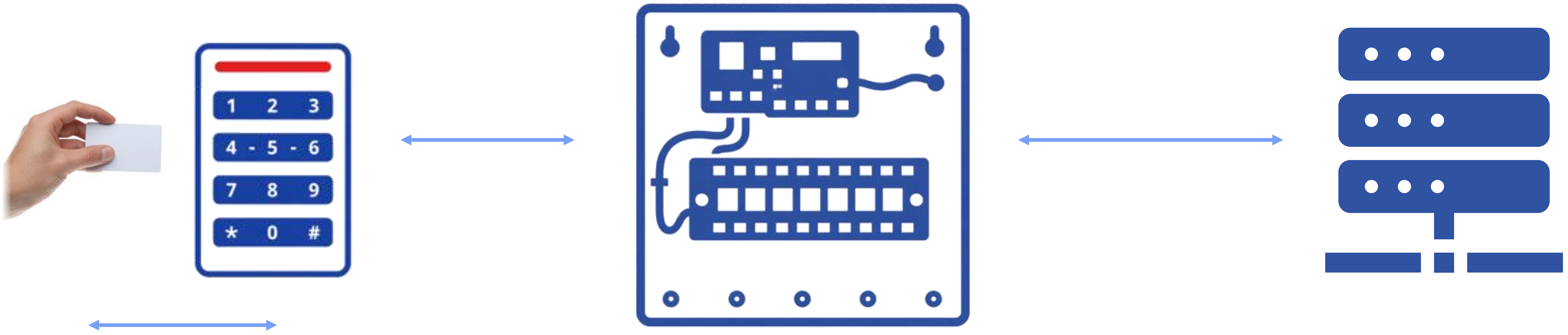
Two-Way Communication

- Controllers can communicate with readers and readers can communicate back.
- Enables:
  - Remote reader configuration
  - Reader diagnostics
  - Health monitoring
  - Firmware updates

Better Maintenance & Troubleshooting

- Remote diagnostics reduce service calls.
- Administrators can identify:
  - Reader failures
  - Wiring issues
  - Communication problems
  - Tamper events

Card Transaction Path Vulnerability Areas



Trusted Execution Environment (TEE)

TEE – a secure, isolated, trusted environment **within the main processor**

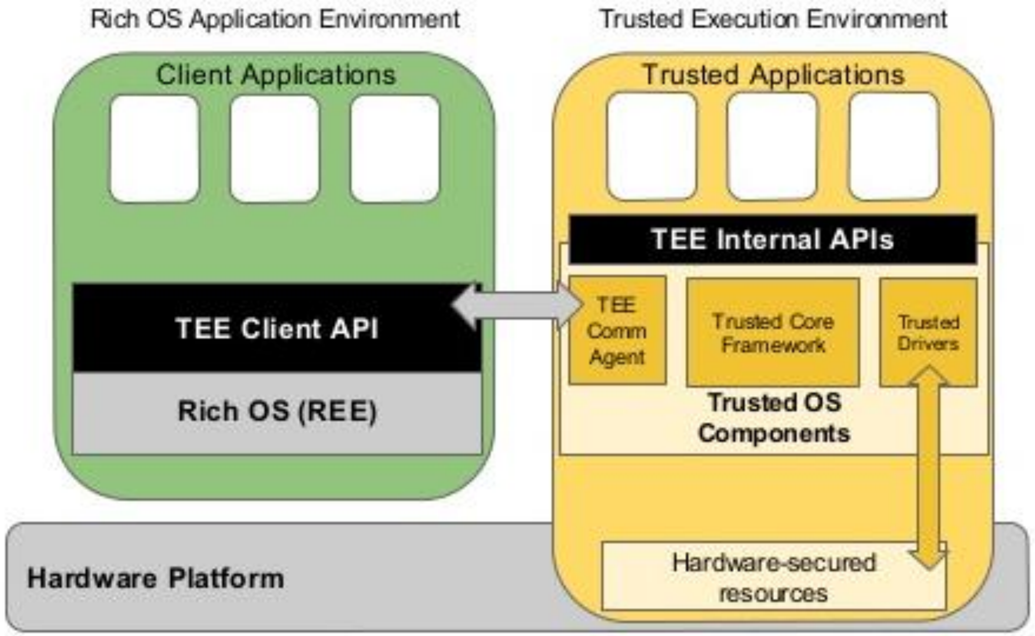
Does not rely on a separate less flexible Trusted Platform Module (TPM)

1. Main Operating System

- Runs the access control application
- Handles networking
- Processes cardholder transactions
- Communicates with C•CURE 9000

2. Trusted Execution Environment (TEE)

- Runs in parallel to the main OS
- Isolated from the Linux environment
- Protects critical code and security-sensitive data
- Uses hardware and software protections to maintain confidentiality and integrity of that data



The Benefits of Secure Hardware Using TEE

Advanced hardware-based cybersecurity

Secure Manufacture from Inception – Personalized and secured with a proper, established chain of trust

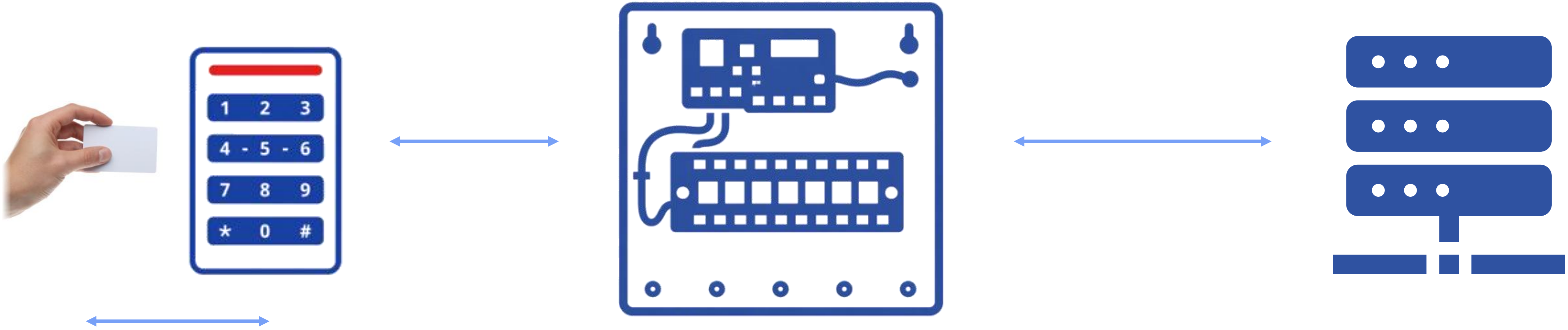
Secure Boot – Entire boot sequence authenticated

Secure Operation – Each command authenticated

Secure Update – Device will only update using software that is considered trusted

Card Transaction Path Secured

- ✓ Use High Frequency/ encrypted credentials and readers
- ✓ Use unique encryption keys any time possible
- ✓ Utilize OSDP encrypted comms between reader and controller
- ✓ Encrypt data at rest and in transit between controller and server



Questions?

Matt Varvais
Area Sales Manager
CA, NV, HI
916.502.3675
matt.varvais@jci.com

Johnson Controls