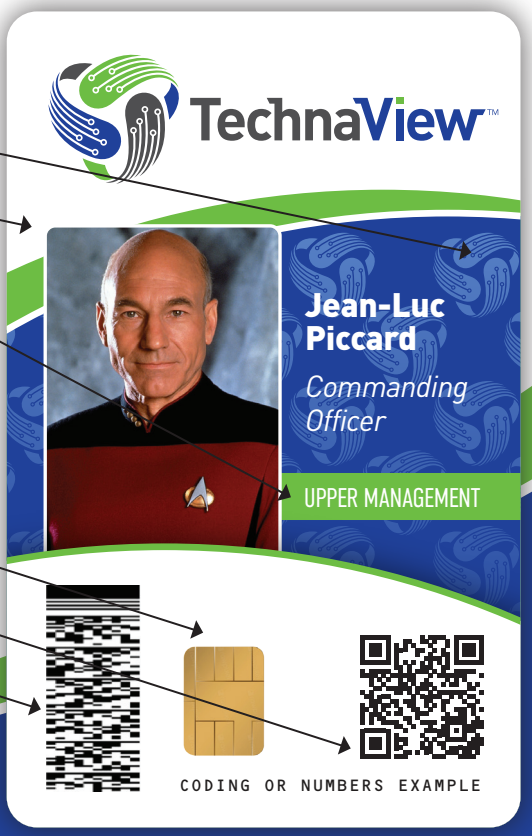
TechnaView™

SECURE CREDENTIAL

New Credential Features:

- Unreproducible Holographic Overlay
- Large High Definition Photograph of Individual
- Department Identification Color Coded Banner
- Radio and Smart Technologies
- 13.56 MHz and 125kHz Unjoined Receivers
- Java Enabled Card with DESFire EV3
- Contact Smart Chip
- QR Code for AI Scanners or Cameras
- Barcode for Scanners



Purpose:

- Cost effectively elevates security while using existing systems the county currently has in place.
- Unifies individual elements within daily operations and existing infrastructure, with added elements to “bridge the gap” between current and future security technologies.
- Privately maintained encryption key by the county, that allows use of any vendor or supported appliance for service.

Practical Use Applications:

- Authorized Individual Identification
- Building Access
- Computer Access
- Time Clock Login
- Vending and Concessions
- Elections Worker/Volunteer Validation

TechnaView.com

TechnaView™

VISITOR CREDENTIAL

New Credential Features:

- Unreproducible Holographic Overlay
- Radio and Smart Technologies
- 13.56 MHz and 125kHz Unjoined Receivers
- Java Enabled Card with DESFire EV3
- QR Code for AI Scanners or Cameras
- Contact Smart Chip
- Barcode for Scanners

Purpose:

- Cost effectively elevates security while using existing systems the county currently has in place.
- Unifies individual elements within daily operations and existing infrastructure, with added elements to “bridge the gap” between current and future security technologies.
- Privately maintained encryption key by the county, that allows use of any vendor or supported appliance for service.

Practical Use Applications:

- Authorized Visitor / Volunteer Validation
- Easy to verify identity via mobile device
- Specialized Visitor Computer Access
- User Data log entry via QR code or Barcode

TechnaView.com

Secure Credential

By

New Credential Features:

- Large High Definition Photograph of Individual
- Department Identification Color Coded Banner
- Holographic Unduplicatable Overlay
- Barcode for Scanners
- QR Code for AI Scanners or Cameras
- Unjoined Radio and Smart Technologies
- 13.56 MHz and 125kHz Receivers
- Contact smart chip
- Java enabled Card with DESFire EV3

Purpose:

- Develop overall security procedure and align identification credentials (badges) to that.
- Cost effectively elevates security while using existing systems.
- Unifies individual elements within daily operations and existing infrastructure, with added elements to “bridge the gap” between current and future security technologies.
- Privately maintained encryption key by the county, that allows use of any vendor or supported appliance for service.

Practical Use Applications:

- Authorized Individual Identification
- Building Access
- Computer Access
- Time Clock Login
- Shipping & Receiving Documentation
- Elections User Validation
- Payment System

Physical Access Control Explained:

Physical access control systems (PACS) are designed to prevent unauthorized individuals from entering a building or restricted area while allowing authorized personnel easy access. They work by creating barriers and using authentication methods to verify a person's identity and authorization.

Components of a PACS:

- Access points: These are the physical entry points like doors, turnstiles, or gates.
- Credential readers: These devices read identification credentials, such as key cards, fobs, or biometric data.
- Control panel: The control panel manages access based on the information received from the readers and determines whether to grant or deny entry.
- Access control server: This server manages user information, access rights, and audit logs.

Examples of Physical Access Controls:

- Locks and keys: Traditional locks and keys are a basic form of physical access control.
- Key cards and fobs: RFID cards or key fobs store electronic credentials that are read by card readers.
- Biometric systems: These systems use unique physical characteristics like fingerprints or facial recognition to verify identity.
- Security cameras: Surveillance systems monitor entry points and can be integrated with access control systems.
- Visitor management systems: These systems manage visitor access and track their movements within a facility.
- Security guards: Human security personnel can monitor entry points and control access.
- Metal detectors: These devices are used to detect metallic objects that may pose a security risk.
- Electronic access cards:These cards contain electronic data that is read by card readers to verify identity and grant access.
- Door sensors: These sensors detect when a door is opened or closed, triggering alarms or other security measures if necessary.
- Turnstiles: These devices control the flow of people and restrict access to authorized individuals.

Logical Access Control Explained:

Logical access control is a security measure that regulates and manages user access to computer systems, networks, and data. It ensures that only authorized individuals can access specific resources and perform designated actions. This is achieved through various methods like authentication, authorization, and accountability mechanisms.

Key aspects of logical access control:

- Identification: Verifying the user's identity, often through usernames or other identifiers.
- Authentication: Confirming the user's claimed identity, typically using passwords, biometrics, or other security tokens.
- Authorization:Granting or restricting access to specific resources based on the user's role and permissions.
- Accountability:Tracking user actions and access for auditing and security purposes.

Logical access control differs from physical access control, which focuses on securing physical spaces and devices. Logical access controls are used for virtual or digital resources, such as computer systems, networks, and data within those systems.

Examples of logical access control measures:

- Passwords: A common method for identifying and authenticating users.
- Multi-factor authentication (MFA): Requiring multiple forms of verification, like a password and a code from a mobile device, to enhance security.
- Biometrics: Using unique physical characteristics, like fingerprints or facial recognition, for authentication.
- Access Control Lists (ACLs): Defining specific permissions for users or groups to access certain files, folders, or network resources.
- Role-Based Access Control (RBAC): Assigning permissions based on job roles within an organization.
- Discretionary Access Control (DAC): Allowing users to control access to resources they own.
- Mandatory Access Control (MAC): Enforcing access restrictions based on system-defined rules.

Java Card Explained

- Java Card is a technology that allows small Java-based applications called applets to run securely on smart cards.
- It provides a platform-independent environment for developing and deploying secure applications on smart cards.
- Java Card technology is widely used in various smart card applications, including:

  SIM cards: Used in mobile phones for authentication and network access.

  Payment cards: Used for contactless payment transactions.

  ID cards: Used for physical and logical access control.

  Healthcare cards: Used for storing patient information.

  Passports: Used for electronic passports.

NFC Explained:

:

- NFC is a short-range wireless communication technology that allows devices to exchange data when brought close together (typically within a few centimeters).
- It operates at a frequency of 13.56 MHz and uses electromagnetic fields for communication.

NFC is commonly used for:

- Contactless payments: Enabling payments by tapping a card or mobile device on a payment terminal.
- Data transfer: Allowing quick exchange of data between devices.
- Access control: Used for unlocking doors or accessing restricted areas.
- Pairing devices: Simplifying the process of connecting devices via Bluetooth or Wi-Fi.

How Java Card and NFC work together:

- Java Card applets can be designed to handle NFC communication.
- For example, an NFC-enabled payment card can use a Java Card applet to securely store payment information and handle contactless transactions when brought close to an NFC reader.
- The NFC technology provides the communication channel, while the Java Card applet provides the secure logic for handling the transaction.

In essence, Java Card provides the secure processing environment, and NFC provides the wireless communication channel, making them a powerful combination for secure and convenient applications in various industries.

Proximity Cards Explained:

RFID Technology:
Proximity cards utilize radio-frequency identification (RFID) to wirelessly transmit data to a reader.

125 kHz Frequency:
The standard frequency for these cards is 125 kHz.

Access Control:
A common application is in access control systems, where the card's unique ID is read by a reader to unlock doors or grant entry.

Other Applications:

Proximity cards are also used for other purposes such as:

- Tracking: Monitoring the location of people or assets.
- Time and Attendance: Recording when employees clock in and out.
- Point of Sale: Used for payments and loyalty programs at retail locations.

Card Types:
Proximity cards come in various formats, including standard, clamshell, and composite cards.

Barcodes Explained:

Barcodes are machine-readable representations of data in the form of parallel lines and spaces of varying widths. They are used to encode information, like product identification, inventory tracking, and more, that can be quickly read by barcode scanners or even smartphone apps.

How Barcodes Work:

1. Encoding Data:

Barcodes convert numbers, letters, and characters into a series of bars and spaces. These patterns represent binary digits (0s and 1s), which are interpreted by scanners.

2. Scanning:

A barcode scanner uses a laser or camera to read the barcode symbol.

3. Decoding:

The scanner translates the patterns into digital data, which can then be processed by a computer or other device.

4. Applications:

Barcodes are widely used in retail, inventory management, logistics, and various other industries to automate identification and data capture.

QR Code Explained:

A QR code, or Quick Response code, is a type of two-dimensional barcode that can be scanned by a smartphone or other digital device to quickly access information or trigger actions. It appears as a square pattern of black and white squares and can store a large amount of data both horizontally and vertically.

- Two-dimensional barcode: Unlike traditional barcodes that store information in one direction (horizontally), QR codes store information in both horizontal and vertical directions, allowing for more data storage.
- Quick access: When scanned by a device, a QR code provides instant access to information or triggers an action, such as opening a webpage, connecting to a Wi-Fi network, or making a payment.
- Commonly used: QR codes are now widely used for various purposes, including marketing, product information, event registration, and digital payments.

How it works:

1. . Data encoding: The QR code encodes data in a matrix of black and white squares (pixels).
2. Scanning: A camera or QR code reader scans the code, recognizing the pattern of squares.
3. Decoding: The device decodes the binary information stored in the code, converting it into usable data (e.g., a URL, text, or contact information).
4. Action: The decoded information is then used to trigger an action, such as opening a webpage or displaying text.

Key features:

- Position markers: The three large squares in the corners of the QR code help the scanner identify the code's orientation and ensure accurate reading.
- Error correction: QR codes have built-in error correction capabilities, allowing them to be scanned even if they are partially damaged or obscured.
- Variety of data types: QR codes can store various types of data, including text, URLs, contact information, and even more complex data formats.

PKOC Explained:

PKOC, which stands for Public Key Open Credential, is a specification for a secure, interoperable, and vendor-agnostic access control credential. It leverages the concept of public key cryptography to allow devices like smartphones or plastic cards to generate and manage their own encryption keys, eliminating the need for centralized key management systems. This approach enhances security, simplifies access control, and promotes interoperability between different systems.

- Secure Credentials: PKOC uses public-key cryptography, where a private key is kept securely on the device (phone or card) and a public key is shared with access control systems.
- Interoperability: PKOC is designed to be vendor-neutral, meaning it can work with various access control systems and devices, promoting a more flexible and open ecosystem.
- Simplified Key Management: PKOC eliminates the need for complex key distribution and management infrastructure typically associated with traditional access control systems, as the private key never leaves the device.
- Cost-Effective: Because PKOC is open and vendor-neutral, it can significantly reduce the costs associated with proprietary access control solutions.
- Mobile-Friendly: PKOC is well-suited for mobile credentials, allowing users to utilize their smartphones for access control.
- Bring Your Own Credential (BYOC): PKOC supports the "Bring Your Own Credential" concept, where users can manage their own credentials without relying on a central issuer.

PKOC's design is based on industry standard X.509.

- PKI stands for Public Key Infrastructure and PKOC utilizes a portion of PKI that is better stated as PK, or PKI without the I.
- The only key that is shared is the public key.
- The public key is the credential, just like any present access card number.
- The access card number needs to be available to put into an access control system.
- X.509 is a process that defines the creation of a key pair, a public key and a private key.
- The public key is shared as the credential number.
- The private key is never shared. It is stored in a vault of the device where it was created.
- The public key and the private key are different, thus asymmetric keys.

MIFARE DESFire EV3 Explained:

MIFARE DESFire EV3 is a contactless smart card technology, the latest in the MIFARE DESFire family, offering enhanced performance, security, and features compared to its predecessors. It's designed for various applications like transportation, access control, and payment systems. Key improvements include faster transaction speeds, greater operating distance, and robust security features like a Transaction Timer to prevent man-in-the-middle attacks.
Here's a more detailed breakdown:

Enhanced Security:

- AES Encryption:DESFire EV3 utilizes AES128 for encryption and includes features like random UIDs, pick master keys, and file encryption keys.
- Secure Dynamic Messaging (SDM): SDM provides advanced data protection within standard NDEF read operations, ensuring secure data exchange.
- Transaction Timer: This feature limits the time for a transaction, mitigating risks associated with man-in-the-middle attacks.
- Mutual Authentication:Both the card and reader authenticate each other using cryptographic keys before data transfer.
- Common Criteria EAL5+ Certification:The IC hardware and software are certified to this high security standard.
- Transaction MAC: This feature helps prevent fraudulent attacks by providing proof of executed transactions.
- Improved Performance: Faster Transaction Speed: The EV3 offers faster transaction speeds compared to previous generations, enhancing overall system efficiency and user experience.
- Greater Operating Distance: The EV3 provides a larger read range compared to earlier versions.
- NFC Forum Tag Type 4 Compliant: This allows for seamless integration with NFC-enabled devices.

Other Key Features:

- Multi-Application Support: DESFire EV3 can hold multiple applications, allowing for flexible and versatile use.
- Flexible File System: Users can define application structures and files within the card, offering customization for different needs.
- Backwards Compatibility:The EV3 is designed to be backward compatible with older MIFARE DESFire systems.
- AppXplorer Platform: This platform allows for applications to be loaded onto cards by the cardholder using a mobile app.

In essence, MIFARE DESFire EV3 is a powerful and secure smart card technology that combines enhanced security features, improved performance, and multi-application capabilities, making it suitable for a wide range of applications.