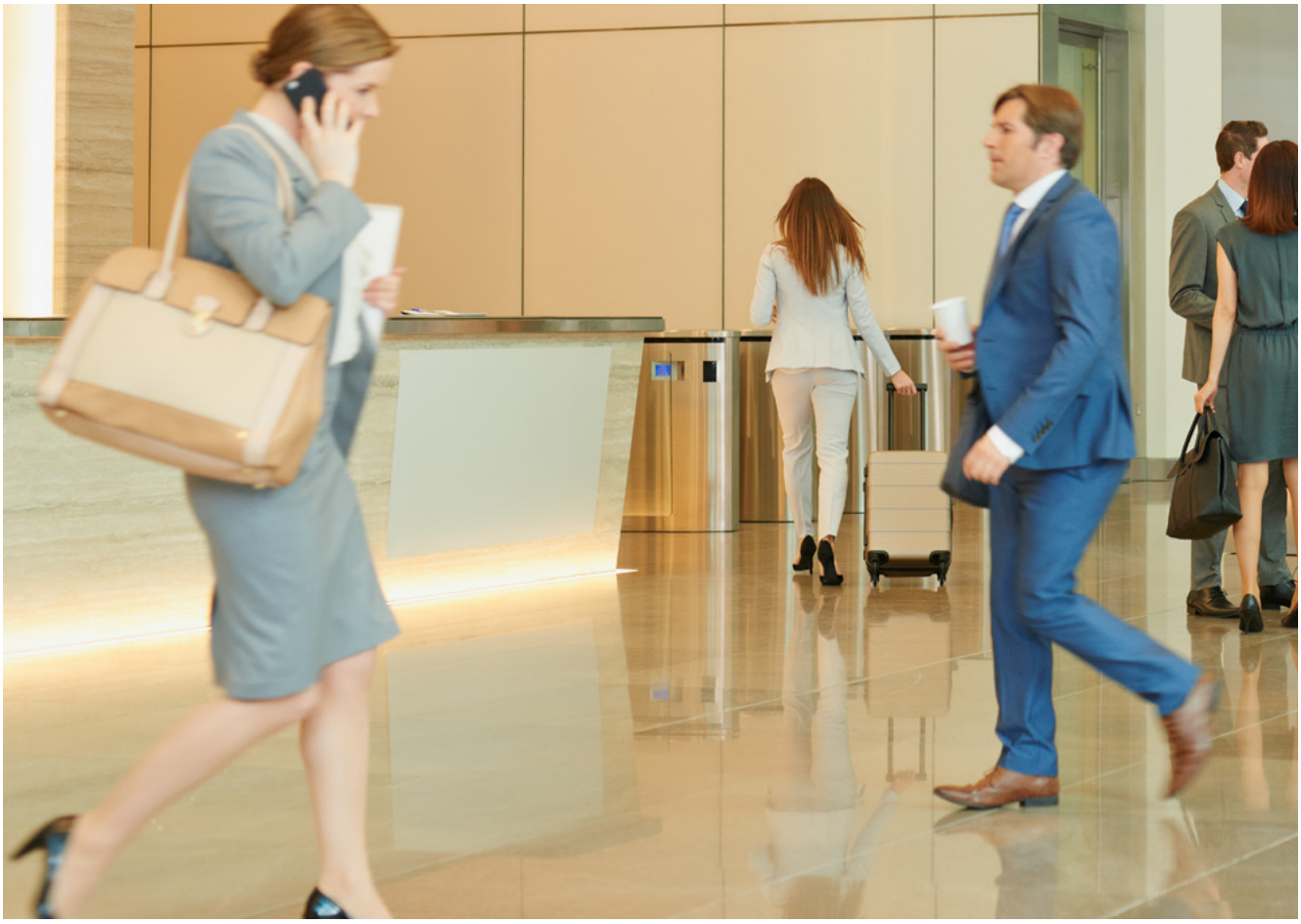
Use Case: Simple and Secure Credential Management of Multi-Site Access Management Systems



Enterprise-scale access management solutions, which involve large numbers of people across multiple sites and distributed buildings, can be hard to protect and difficult to scale. NXP's MIFARE DUOX IC is tailored for use in these situations, bringing high levels of security and easy expansion to multi-site access management solutions.

Target Applications

- Business
- Education
- Hospitality
- Manufacturing
- Medical
- Government
- Multi-tenant office buildings

Challenge

Large organizations, such as corporations, universities, resorts, production sites and medical facilities, often operate across multiple buildings, offices and locations and manage access for thousands of people, with varying levels of authorization. Granting staff access to geographically dispersed offices with a single card significantly increases the complexity of the physical access control system. It necessitates effective and secure key management and distribution processes, along with various other tasks.

The access management solutions employed by these organizations must uphold a high level of security, even when scaled to accommodate large numbers of users and various stakeholders such as building owners, building operators, access control owners, access control operators, and other related parties. The method used to protect, encrypt and interact with access credentials can influence the solution's ability to meet this need.

Maintaining security at scale

Nowadays, access management solutions mostly rely on symmetric encryption, such as Advanced Encryption Standard (AES). However, symmetric cryptography might not be the optimal fit for complex, multi-party access solutions. While symmetric encryption is robust, fast and efficient, it is still subject to its own set of limitations when utilized within complex multi-party access management systems with large-scale use. This is because they depend on the secure exchange of symmetric keys, which can present challenges. Additionally, the risk of secret key leakage from the reader terminal can lead to credential cloning. If the secret master key is compromised, several attack scenarios are possible. For example, access credentials may be copied and issued to additional users for unauthorized use, or fraudsters may start issuing new cards containing new valid credentials for unauthorized use.

Symmetric key encryption uses one key for both encrypting and decrypting data, which means both the sender and receiver must have the same key. Keeping this key confidential and secure at all times is crucial, so it should never be shared publicly. Efficient management of the key, including its generation, storage, distribution, rotation and revocation, is essential for maintaining security. Though managing symmetric keys works well with a small number of parties within a strong security system, it becomes more complicated as more entities get involved. In complex systems involving multiple organizations, preventing key compromise or leakage is challenging. The entire system's integrity can be jeopardized if even one party mishandles the symmetric key, leading to potentially severe consequences.

On the other hand, asymmetric cryptography, such as Elliptic Curve Cryptography (ECC), offers higher flexibility when compared to symmetric cryptography. That's because asymmetric cryptography involves keypairs which consist of two keys, one private and one public. The private key is kept secret and never shared. The public key can be freely distributed and shared with all involved parties. Even if the public key, which is required to encrypt data, is revealed, the encrypted data remains safe, since the private key, which is required to decrypt the data, is still unknown. Each authorized device or smartcard used as an access credential is provided with a unique digital certificate signed by a Trusted Root and Certificate Authority (CA). This certificate acts as proof of authentication, adding an additional layer of security to the process, and making it more difficult for unauthorized parties to access the system.

Solution

To enhance the robustness and security of access credentials used in complex multi-party access management systems, a number of industry groups involved in access management have issued guidelines and standards that specify the integration of symmetric and/or asymmetric encryption.

Aliro, a specification created by the Connectivity Standards Alliance (CSA), defines a standardized communication protocol between the access reader and the user device. It requires asymmetric cryptography and asymmetric authentication for access control systems, offering secured, convenient and consistent user experience when using smartphones, wearables or other user devices to unlock doors.

The FiRa Consortium, which is dedicated to use cases that employ Ultra-Wideband (UWB), including access control on mobile phones, is driving specifications that use ECC and PKI-based mutual authentication for access control applications in various different sectors, as well as other areas like indoor navigation, smart ranging scenarios and location services.

LEAF is a universal standard that unites physical and digital credentials across a single comprehensive platform. The LEAF Community is a global initiative that connects technology providers, integrators, and enterprises to ensure seamless interaction between credentials and access control devices.

MIFARE DUOX: Combining symmetric and asymmetric cryptography

To support the deployment of asymmetric cryptography in big, complex and geographically dispersed access management systems and to address industry needs and standards, NXP offers the MIFARE DUOX, a contactless smartcard IC that combines asymmetric and symmetric cryptography in a single chip, enabling simplified key management and fast asymmetric authentication for access management applications.

MIFARE DUOX is designed to support industry specifications. Compliance with these standards and guidelines facilitates the deployment of access control reader firmware that enables seamless interaction between access control devices and various user credentials, including mobile devices, wearables or MIFARE DUOX-powered smartcards.

Furthermore, the MIFARE DUOX credential addresses potential threats posed by quantum computers by implementing AES-256 as an initial step towards post-quantum cryptography. This field of cryptographic science aims to develop algorithms that are resistant to quantum computer attacks. Implementing this approach provides organizations with security measures for identity and access management that are designed to be robust against future technological advancements. Using the extended key size of 256-bit for AES addresses current security needs in identity and access management while also preparing for future challenges.

MIFARE DUOX is Common Criteria EAL 6+ certified and offers additional features for enhanced security. The **Transaction Signature** feature generates a secure signature for each executed transaction between the reader and the smartcard, to ensure data hasn't been altered and for generating a secure transaction proof in a multi-party environment. The **Proximity Check** feature protects against relay attacks, making sure the communication between reader terminal and MIFARE DUOX-based smartcard is not being relayed by malicious attackers.

In addition to physical access control, MIFARE DUOX can also be used in logical access control scenarios by serving as a multi-factor authentication (MFA) device. For example, when logging in to a work computer, internal office network, device or secured application, the user needs to provide their identity along with proof of authenticity. Besides entering a traditional password, the MIFARE DUOX-based device can function as a second-factor device to generate a secure one-time password (OTP) that can be sent to the system to uniquely identify and authenticate the user.

"MIFARE DUOX empowers our customers to solve issues traditionally tied to sharing symmetric keys in complex multi-party environments. With MIFARE DUOX and the chip's integration of partial backwards-compatibility to MIFARE DESFire EV3, post-quantum ready AES-256 cryptography, asymmetric cryptography based on ECC, and the Safetrust ecosystem, customers can seamlessly transition to an asymmetric identity management system using their existing MIFARE DESFire reader infrastructure. This enables supply chain management through digital certificates and a chain of trust, eliminating the need to share sensitive keys with vendors. Customers can now trust, generate, and revoke supplier access without the risks of potentially compromised symmetric keys."

Jason Hart, CEO & Co-founder, Safetrust

Summary

MIFARE DUOX enables large-scale organizations to issue smartcards that support multiple applications across various locations. This allows end-users to benefit from additional services beyond access control, such as in-house micropayments, elevator access, follow-me printing services, PC logon, second-factor authentication, parking access, onsite EV charging, and more.

Learn more

Visit the MIFARE DUOX product page to find comprehensive application notes to be used with MIFARE solutions, as well as detailed design tools, software, trainings and more.

nxp.com

Document Number: MIFAREDUOXACCESSMGMTFS REV 1