WHAT IS XSECURE?

Xsecure is the XPR encryption and credential solution. Access control systems can use this data for user identification instead of a built-in Card Serial Number (CSN). The concept uses native AES encryption of the Mifare DESFire cards, combined with a key diversification algorithm, additional data encryption, and data validity checking. Key sets and encryption processes are known only to the secure reader.

Xsecure

WHY IS CREDENTIAL SECURITY IMPORTANT?

Credentials are the most exposed component of RFID access systems. The most popular hacking method of an access control system is to clone RFID cards or Card Serial Number (CSN) simulations to obtain unauthorised access.
With the proper equipment, a user's card can be read when it is in their wallet or pocket without realising it.
Securing user credentials is the first step in any security upgrade for the access control system.

WHY XSECURE?

The **Xsecure** concept uses Mifare DESFire EV3 credentials. Above that, each credential access key (key to read data on the credential) is unique, resulting from **a non-reversible diversification process**. Furthermore, the credential's data is encrypted and sealed, with error checking to prevent spoofing. This process is limited to the reader and credential encoding system in production. To prevent duplicates, credentials are solely encoded by XPR that controls the issued IDs.

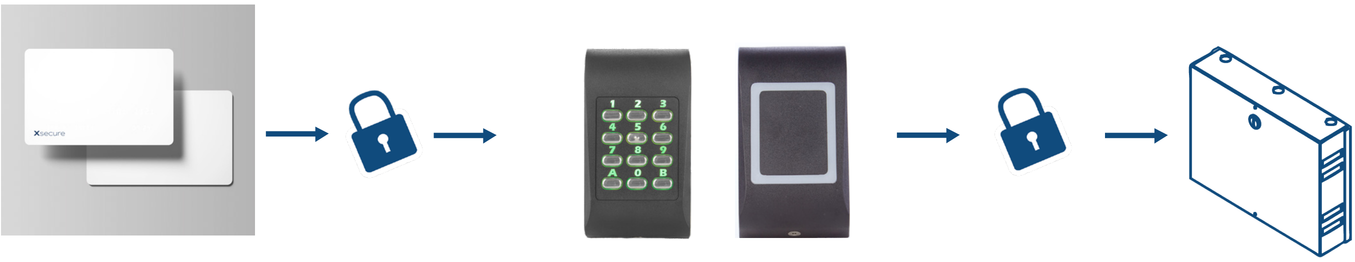
XSECURE CARD FEATURES

ISO card	
Type	MIFARE® DESFire® EV3
Common Criteria certification	EAL5+ (Hardware and Software)
Operating Frequency	13.56 MHz
Communication Protocol standard	ISO14443A-4
Communication Speed	Up to 848 kbps
Memory	2 K
Data Retention	25 years
Xsecure ID	7 bytes. Use minimum of 4 LSB bytes guarantee uniqueness of the ID
Printing	One side (blank) and other side with Xsecure logo and ID card number on the bottom
Material	PVC
Operating Temperature	-35°C to + 50°
Standards compliance	ISO14443A-4, ISO/IEC 7816-4, ISO/IEC 24727-3:2008
Compatible readers	Xsecure readers

HOW DOES IT WORK?

XPR creates cards with a **unique ID** protected by a **different key** for each card.

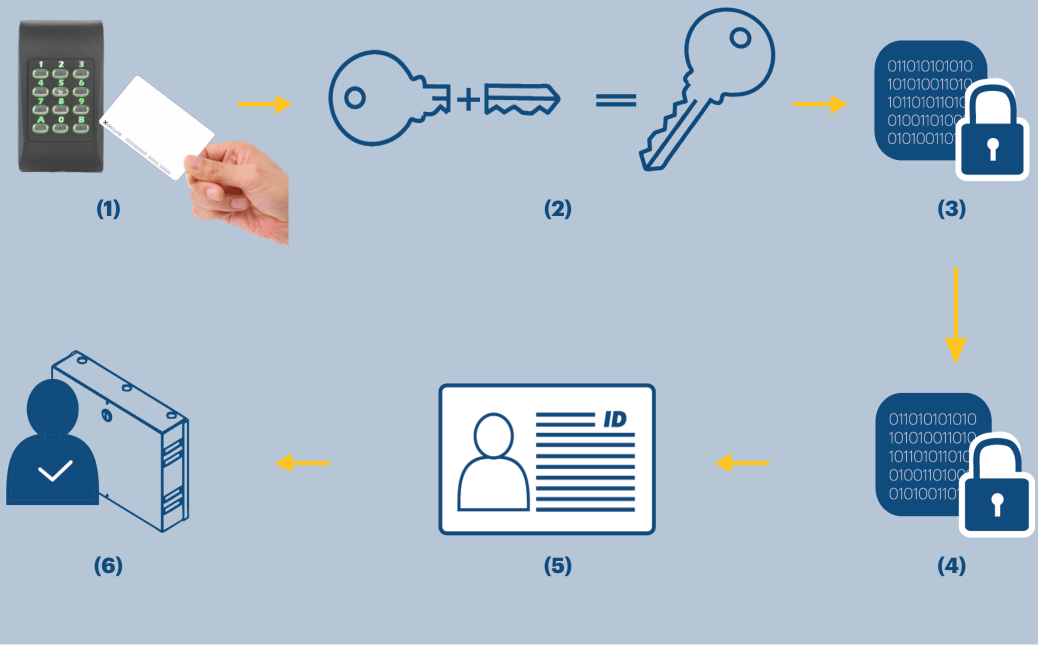
Configuring a secure reader to read only **Xsecure** cards by the installer or end user.



Secure Communication
AES & Key Diversification

Communication Protocols
Wiegand, RS-485, OSDP

When the reader detects a card **(1)**, it assembles the card access key (unique for each card) **(2)**, reads the card content **(3)**, decrypts the card content **(4)**, extracts the ID **(5)**, and sends it to the controller **(6)**.


(1)
+
=
(2)
011010101010
101010011010
101101011010
010011010010
010100110
(3)
011010101010
101010011010
101101011010
010011010010
010100110
(4)
ID
(5)
(6)