White paper

Who’s guarding access to your access control system?

Authors: John Harvey, Leon Rose, Carl Fenger,
LEGIC Identsystems

LEGIC Master-Token System-Control (MTSC): providing companies and institutions with security independence

Summary

When it comes to managing who is allowed entrance to critical infrastructure, the most vulnerable point of attack is not the access control system itself, encryption used, nor physical media such as employee badges – it’s how the cryptographic keys embedded in door locks get there to begin with.

Access control systems can be compromised even before installation is completed

For government buildings, schools, offices, airports, and private residences, the importance of secure access control is growing to protect against theft and crime, as well as against physical access to sensitive information. In healthcare settings such as hospitals or care homes, effective and contactless access control is crucial for preventing the spread of pathogens such as COVID.

Fortunately, modern IT technology has developed to the point where the automated authentication of individuals and secure management of smartcard-based personal credentials is virtually bullet-proof. Most access control systems employ symmetrical encryption based on techniques such as Advanced Encryption Standard (AES, or "Military Grade Encryption") meaning smartcard (badge) access to infrastructure equipped with this technology is largely secure, *once implemented.*

Security: as strong as the weakest link
We all have daily experience with today's smartcard-based access control technology – most of us use it when entering our offices or university campus buildings using a badge as credential. The basis of security is the guarantee that no one can gain access to the encryption key (also referred to as "password, PIN, etc.") stored in the door lock's secure memory. For AES encryption, this is simply a 128-, 192-, or 256-bit number.

Modern semiconductor technology in the form of a "Secure Element" prohibits physical or electrical access to this encryption key once it is stored in electronic door locks, even by the most sophisticated hacker.

One weakness, however, still exists.

How are encryption keys installed?
When it comes to managing access to buildings, rooms and storage areas, the most vulnerable point of attack is not the access control system itself, encryption used, nor physical media such as employee badges – it's how the cryptographic keys embedded in door locks get there to begin with. A breach at this most fundamental level of access security can render the entire access control deployment vulnerable.

Disadvantages of factory programming
One way to ensure that cryptographic keys are securely installed in door locks is to do so during the manufacturing stage – "factory programming" of each lock before it leaves the production line. This ensures that encryption keys are safely embedded in the lock before delivery to customers. Three fundamental problems, however, exist:

1) Compromised security ownership
Having electronic locks pre-programmed at an external vendor immediatley puts security ownership at risk. How many third-party suppliers, IT and logistics staff have had access to encryption keys during manufacturing and delivery before the lock is installed ? The answer is – you don't know. Security processes at external suppliers are defined, controlled and audited within their own four walls, and processes are not 100% transparent to end-customers. For this reason, factory programming of encryption keys, with the exception of specific limited cases, should be avoided and the end-customer must be able to (re-) configure their access infrastructure with encryption keys which they own and control themselves.

2) Logistics
Electronic door lock manufacturers produce millions of locks for thousands of customers each year. So long as locks are delivered as "blanks" configurable by the end-customer at the final stage, logistics can be kept simple – one product fits all.

As soon as factory-programmed locks are created, what once was a single product suitable for many customers becomes a customer-specific product, with all the associated storage and logistics issues associated with administering thousands of different variants. This adds significantly to the cost of the lock while introducing risks for over- or under-production, as well as error.

3) Change of ownership
Businesses close, move, and change ownership on a regular basis. To prevent previous owners from accessing infrastructure that they vacated, each door lock must be re-programmed by the new owner

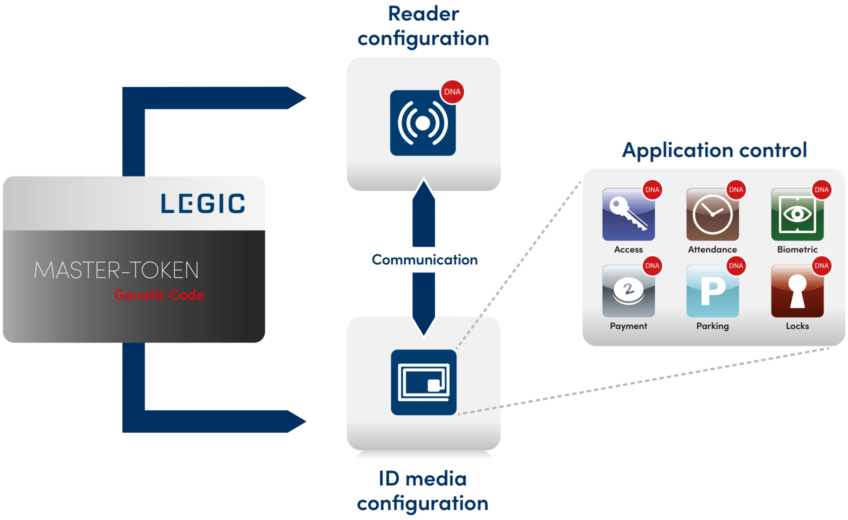
with new encryption keys. This negates the benefits of factory programming.

Physical onsite programming
If door locks are installed in a "blank" state (no key installed), they cannot be programmed over a network due to lack of encryption – encryption is only possible once the encryption (decryption) key is installed. The person installing the key onsite is also a risk factor if the unencrypted key is visible – the key can be easily copied, remembered or photographed.

When most access control installations are initialized, security personnel are tasked with physically installing encryption keys on each door lock using a dedicated device. To prevent leakage of the key during lock initialization, LEGIC's unique "Master-Token System-Control" Key and Authorization Management solution (MTSC) has been designed to provide companies and institutions with absolute independence and control over their organization's access security including cards and readers.

A secret shared is no longer a secret
The main security feature of MTSC is the deliberate omission of secrets shared among installation and security administration staff such as encryption keys or passwords. Authorizations instead are granted using non-human readable physical tokens in the form of uncopiable, contactless smartcards.

Companies who use a visible password-based security system are not usually aware of how easily they can be compromised. Visible passwords can be leaked at any time, completely undetected. MTSC does not use passwords, which gives better control over security in contactless smart card applications. MTSC is based on a unique, invisible "genetic code," embedded within contactless smartcards. The genetic code within this technology guarantees that all the necessary credentials are unique.



LEGIC Master-Token System-Control (MTSC)

The code is transferred via contactless RFID during badge initialization and to readers during system configuration. The use of a physical token also allows administrators to securely manage their badge population and easily add or withdraw applications as required (i.e., access control, time & attendance, secure printing, vending & canteen ePayment, etc. – up to 127 applications can be hosted on a single card). Additionally, the ownership of an own physical token grants Security Officers full autonomy in selecting trusted suppliers, should they choose to do so.

Independent ownership vs. delegation to 3rd parties
Although 100% ownership of security deployment for access control systems is important for a company headquarters, delegation of encryption key deployment to trusted 3rd parties in remote field offices or external card reader manufacturers is often convenient. This is easily done with a "limited initialization card".

Owners of an MTSC system do not have to permanently hand over a system-wide password or encryption key but can give external card reader and of course card manufacturers a physical token which is limited in the number of reader and credential configurations they can perform. This allows outsourced access security services to be tightly controlled, traceable, revocable and auditable ("Hierarchical Rights Delegation").

Ensuring security through organizational structure and processes
By keeping encryption keys hidden from human eyes, overall system security is safeguarded by the physical protection of the Master-Token which resides on a smartcard, like storing gold in a safe. By adhering to simple and basic measures, card reader initialization and card production is secured through an appropriate level of security and authorized personnel. Master-Tokens can only be removed using a documented workflow with corresponding approval levels and, among other techniques, according to the four-eyes principle.

LEGIC Master-Token used for secure initialization of cards and readers via RFID

When using systems that rely on human-readable secrets such as visible passwords, once the key is removed from the "safe", it remains in the memory of at least one person. With an MTSC Master-Token, there is no such "knowledge" in the hands of any individual.

Enabling auditable processes
Due to the fact that the encryption key is locked in the token and cannot be read by a person, nor exchanged over digital networks, it becomes easy to implement basic and auditable organizational measures to ensure a high level of security for the Master-Token. Protection is similar to that which is provided for physical objects such as cash or precious metals.

The same process for human-readable information, or information exchanged over a network is far more complex, with many more security risks. MTSC thus enables the easy implementation of auditable processes such as those described in ISO-27001, "Annex A.9 Access Control" which describes best practices for safeguarding access to information and ensure that employees can only access information that's relevant to their work.

MTSC use case: Frankfurt Airport, Germany

MTSC use case: Frankfurt Airport
Frankfurt am Main Airport is Germany's largest commercial airport. The airport employs around 81,000 people in various locations around the world. To manage access control security for its employees and contractors, the airport authorities have implemented a multi-level MTSC security concept for the numerous functions, processes, and applications. Part of this is a uniform access control system for employees and contractors based on contactless ID cards as identification medium. Read about the deployment "Frankfurt Airport: how do you protect an access control system in an audit-proof manner?

For more information about how to take full control of an access control system with LEGIC MTSC, visit https://www.legic.com/mtsc.

About LEGIC
For over 30 years, Swiss-based LEGIC Identsystems has enabled companies from around the world to deploy solutions with demanding security requirements. Based on key management, trusted services and secure, contactless semiconductors, the LEGIC Security Platform provides end-to-end security for smartphone- and smartcard-based access, mobility, shared resource and industrial IoT applications.

Author: John Harvey, Leon Rose , Carl Fenger

November 2022