WHO'S GUARDING ACCESS TO YOUR ACCESS CONTROL SYSTEM?

John Harvey, Leon Rose and Carl Fenger of LEGIC Identsystems detail the benefits offered by the company's MTSC solution

For government buildings, schools, offices, airports and 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 hospitals or care homes, effective and contactless access control is crucial for preventing the spread of pathogens such as COVID.

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

"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."

Security is as strong as the weakest link

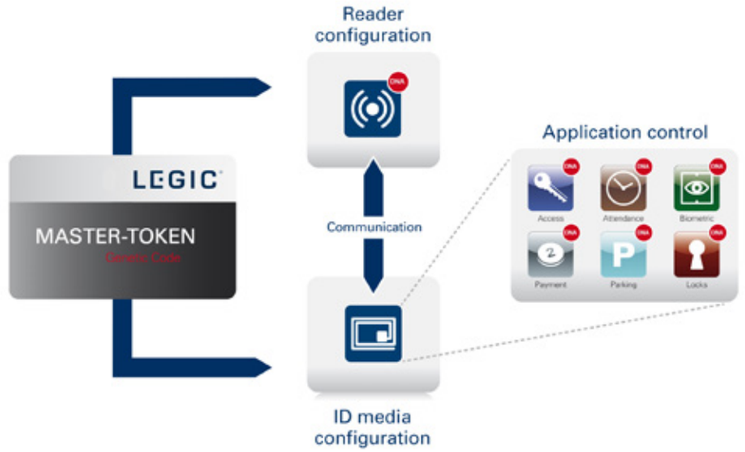
We all have daily experience with smartcard-based access – most of us use it when entering our workplaces using a badge as a personal credential.
The basis of security is the guarantee that no one can gain access to the encryption key (also referred to as "password") stored in the door lock's secure 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.

Physical onsite programming

If door locks are installed in a "blank" state, they cannot be programmed over a network - encryption is only possible once the encryption key is installed. The person installing the key onsite is also a risk – a visible key can be easily copied, remembered or photographed.



To prevent leakage of the key during lock initialisation, LEGIC's unique "Master-Token System-Control" Key and Authorisation Management solution (MTSC) has been designed to provide companies and institutions with absolute independence and control over their organisation's access security including cards and readers.

"Companies using a visible password-based system are often unaware of how easily they can be compromised."

A secret shared is no longer a secret

The main feature of MTSC is the deliberate omission of secrets shared among security staff. Authorisations are granted using non-human readable physical tokens in the form of uncopiable, contactless smartcards. Companies using a visible password-based system are often unaware of how easily they can be compromised. MTSC does not use passwords, which gives better control over security in contactless smartcard applications.

MTSC is based on a unique, invisible "genetic code", embedded within a Master Token. The code is transferred via contactless RFID during badge initialisation and to readers during system configuration. This allows administrators to securely manage their badge population and easily add or withdraw applications as required.

Ensuring security through organisational structure

By keeping encryption keys invisible, system security is ensured by the physical protection of the Master-Token, like storing gold in a safe. By adhering to basic measures, card reader initialisation and card production is secured through an appropriate level of security and authorised personnel. Master-Tokens can only be removed using a documented workflow with corresponding approval levels (e.g., the four-eyes principle).

Enabling auditable processes

With MTSC it becomes easy to implement basic and auditable organisational 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 process for human-readable information 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".

For more information visit https://www.legic.com/mtsc.

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. 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.

2. Logistics: So long as locks are delivered as "blanks", 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. 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. To prevent previous owners from accessing infrastructure that they vacated, each door lock must be re-programmed by the new owner which negates the benefits of factory programming.