LEGIC

Success Story

# Frankfurt Airport


## How do you protect an access control system in an audit-proof manner?

**System security begins with procurement**

If you want to manage who comes and goes in your buildings, the most vulnerable point of attack is neither the access control system itself, nor physical identification media such as employee badges; it is the cryptographic keys that are used to configure and manage your system.

In offices, factories, warehouses, universities, hotels, utilities, and airports, this most fundamental level of access security is thus of paramount importance.

Frankfurt am Main Airport is Germany's largest commercial airport. In terms of passenger volume, it was the fourth largest European airport in 2019 with 70.6 million passengers and is in 15th place worldwide. The company 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 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.

**Who is monitoring the administrator?**

In order to give Frankfurt Airport full control over its own smart-card-based airside access control solution for employees and contractors, the end-to-end security platform from LEGIC was selected. The system is based on LEGIC's Master Token System Control (MTSC), a unique key and authorization management solution from LEGIC.

The patented system is designed to give end users complete independence and control over the security of their business, including cards and readers.

The main feature of MTSC is the deliberate avoidance of shared secrets such as passwords. Authorizations are granted using physical tokens in the form of contactless smart cards. Organizations that use a password-based security system usually have no idea how easily they can be compromised. MTSC technology is based on a unique "genetic code" contained in contactless smart cards. The genetic code within this technology guarantees that all required credentials are unique. The code is transmitted to the reader during initialization of the ID card and during configuration.

In combination with the physical token, administrators can securely manage their ID population and, if necessary, easily add or remove applications (e.g., access control, time recording, secure printing, cashless payment at machines and in the canteen, etc.). In addition, having their own physical token grants security officers full autonomy in choosing trustworthy suppliers.

**Advantages of MTSC in practical use**

The following practical insights into the advantages of MTSC at Frankfurt Airport come from an interview with Mr. Roman Falke, Senior Delivery Manager for Security Systems in the Department Airside Security and Video Management Systems at Fraport AG (Fraport AG is one of the largest global airport businesses which also operates Frankfurt Airport).

Further information on how you can take full control of your access control system with LEGIC MTSC can be found at

www.legic.com/mtsc or contact LEGIC at www.legic.com/contact

**LEGIC: Where do you generally see the greatest potential security gaps in airside access systems such as Frankfurt Airport operates?**
Fraport: „You can avoid the biggest security gaps if you think BEFORE the introduction of HOW the ID is programmed and in which environment it is produced. For the planning, it is highly advisable to consult experienced specialists from the beginning."

**LEGIC: What are the main advantages of using the MTSC Key and Authorization management solution from LEGIC?**
Fraport: „Limited sets of tokens can be created on the basis of LEGIC MTSC. This allows us to retain full control over our ID card structure and decisively minimize any possible security risk. With these individually defined Sub-tokens, responsibility can be assigned and withdrawn at any time!"

**LEGIC: How should such an access system be introduced and operated in a controlled manner?**
Fraport: "After we decided on MTSC, we received extensive training on how to handle and take responsibility for smart-card-based master tokens. The entire route of these security elements from LEGIC to the recipient at the airport must be prepared and carried out in a tightly controlled manner.

On one hand, internal ID card production can be secured in terms of appropriate workspace and personnel; the smart-card master tokens, on the other hand, must be stored with strict physical protection. They can only be removed from secure storage using a documented workflow with different approval levels and, among other things, according to the four-eyes principle. Of course, this also applies to the use of each token. When using a system that works with passwords or shared secrets, for example, the key that has been removed from a safe remains in a person's memory. With a smart-card-based physical token, there is no permanent knowledge in the hands of a single person."

**LEGIC: Can an auditable handling of tokens be implemented?**
Fraport: „The structured, documented planning of the specified workflow of how tokens are dealt with is crucial for this. Every use of a token, regardless of the purpose, follows strict guidelines. Only in this way can the security level be kept high from the beginning, and auditable security be implemented."

**LEGIC: According to which internal and / or external security requirements did you have the mentioned procedure assessed?**
Fraport: "Of course, we meet requirements such as those published in Annex 9 of ISO-27001. This is continuously monitored via internal audits conducted by our own, independent departments. The MTSC concept supports us in meeting these demanding requirements according to practical process descriptions."

**LEGIC: How important is direct contact with LEGIC for Fraport AG?**
Fraport: "Direct and immediate information from LEGIC on questions and topics is crucial for operation. In addition, direct contact offers us timely planning for upcoming security developments."