

**Best Practices**

# **Using Contactless Smart Cards for Secure Applications**

Classification: Public (Info Level 1)  
Document No.: LA-11-005d-en  
Edition: 2010

# 1 Introduction

**Background** Contactless smart card technology is enjoying an increasing popularity as a proven, reliable and cost efficient mean for identification for many years. In particular, the functionality and convenience of contactless smart cards have made this technology in many areas the preferred choice for a credential also in security related applications in the corporate, recreational or payment world. Its major applications include physical access control, cashless payment and related multi-applications such as electronic locks, printing, parking, time & attendance and transport to name a few.

While some of the applications, for example parking or time & attendance, tend to focus more on the organisational, process automation or convenience benefits, others use contactless smart cards also as a security element to protect facilities or other assets from unauthorized access or use.

As for every technology used for security purposes, the well known principle that an absolute security does not exist also applies to contactless smart cards. The compromising of a security technology is always a question of time, expense and technological progress. Nevertheless, the risk of compromising a contactless smart card system can be minimised by applying a set of "Best Practices".

This document provides best practices on what should be followed when evaluating, installing and operating contactless smart card systems based on LEGIC technology. It helps to identify the security elements that have to be considered in order to ensure a maximum system security.

The selection of security measures depends on the system application and the security requirements thereof. For example, the requirements to control the access to a parking lot are in most of the cases much less sensitive than securing the access to a company building.

Please note that there may be additional appropriate best practices which are not contained in this document.

**Target audience** This document is targeted to all parties applying, integrating or using contactless smart card systems. This incorporates system integrators, consultants, end-users and application manufacturers. The document can be used in different phases of a system's life cycle: Evaluation, planning, installation and operation.  
If you are an end-user, please coordinate the system security with your system integrator or system supplier.

## Change history

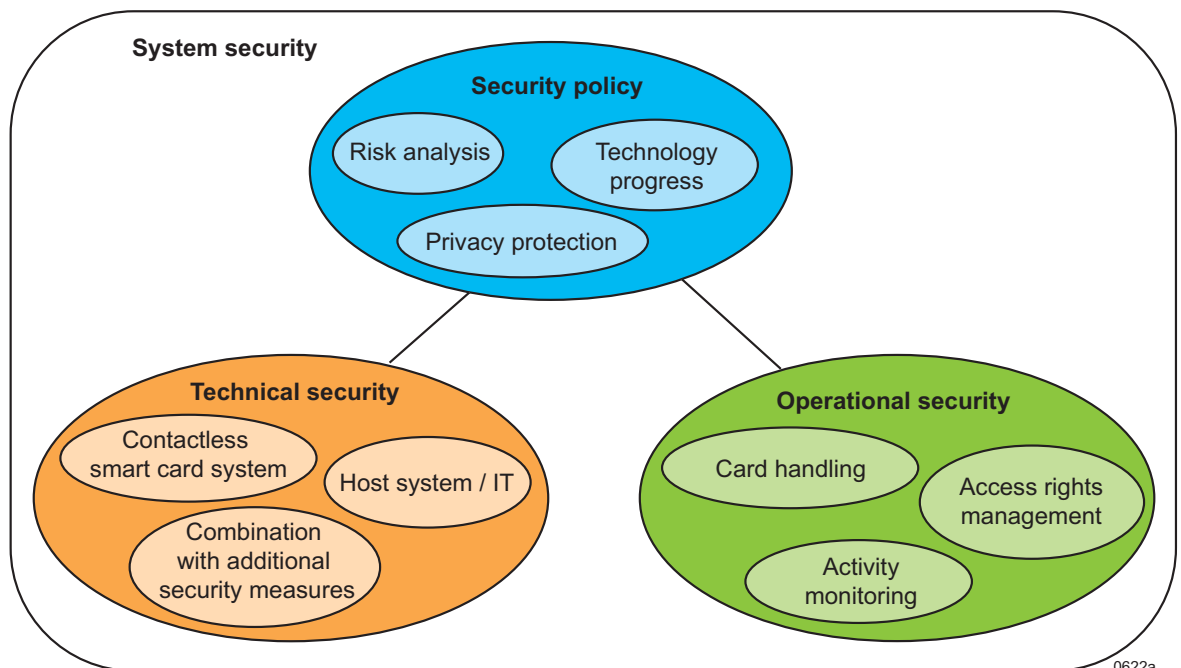
Change	Edition
New edition	07.2008
Minor text corrections	01.2010

## 2 Securing a contactless smart card system

**Overall system security** To ensure a maximum security of the contactless smart card system, different security measures have to be considered. This includes technical measures such as data encryption or tamper proof enclosures as well as operational measures such as card personalisation processes or guidelines on how to wear the employee badge.

The overall system security can be divided into three areas:

- **Security policy** (What are the system's security requirements?)
- **Technical security** (Which technical measures are required?)
- **Operational security** (Which processes have to be defined?)



The best system security is achieved if as many measures as possible are applied, with attention to the required security level. With applying all these measures, a system is significantly less vulnerable to being compromised.

Also, it is important to assess the role and respective measures of the contactless smart card system in the overall concept. It might be much easier to enter a facility through the window or to break into the cash box of a vending machine than attacking the smart card system. Respectively, it might be as important for an effective security to define adequate detection measures or intruder alarms.

**LEGIC system security** LEGIC Identsystems Ltd offers a wide product portfolio which is oriented to the different customer demands such as security, flexibility, convenience or cost sensitivity. Since the beginning, LEGIC has paid great attention to the system security and has implemented additional elements which are incorporated in a multi-layer security concept. The LEGIC advant technology covers e.g.:

- Technical measures such as authentication between reader and card, encrypted data transmission and data storage or secure reading of UID
- Master-Token System Control (physical token based authorisation)
- Organisational measures such as restricted and adequate distribution of product information

### 3 Security policy

To ensure the overall system security, it is recommended to define a security policy. Each operator of a contactless smart card system should consider the security requirements for his system. The access to banks or airports for example normally requires higher security standards than the access to a parking lot or to a skiing region.

#### Setting up a security policy

A security policy typically covers the following issues:

- A risk analysis helps to identify the potential risks and provides the basis for defining the technical and operational security measures.
- It's also essential to consider the privacy and data protection. The handling of sensitive data has to comply with the needs of card holders, the enterprise and with local regulations.
- To be prepared for the future and to comply with the technological progress, a regular system assessment is highly recommended. Based on this assessment appropriate measures for the future development of the contactless smart card system can be derived (see also next paragraph).
- A security policy should also cover issues such as physical and logical access rights for all card holders or the connection to the enterprise IT system.

Derived from the security policy, the technical and operational security measures are defined.

#### Technological progress

To be prepared for the future, continuous attention to the technological development in the security industry should be given. It is recommended to define a road map for corporate security development. This road map helps to protect the investment and leads to a migration path for the contactless smart card system.

One scenario can contain measures such as e.g. the step-by-step change from one reader generation to the next or to provide an upgrade possibility for each reader (e.g. firmware upgrades, enabling multi RF standard interfaces).

#### Example for migration scenario

*The following example sequence shows a smooth migration scenario from a LEGIC prime system to a LEGIC advant system:*

1. *Replace LEGIC prime Master-Tokens by LEGIC advant Master-Tokens. Use exclusively LEGIC advant Master-Tokens for issuing new cards.*
2. *Replace LEGIC prime readers step by step by LEGIC advant readers.  
Replace LEGIC prime cards step by step by LEGIC advant cards.*
3. *Where required use microcontroller based smart cards (with LEGIC all-in-one area).*

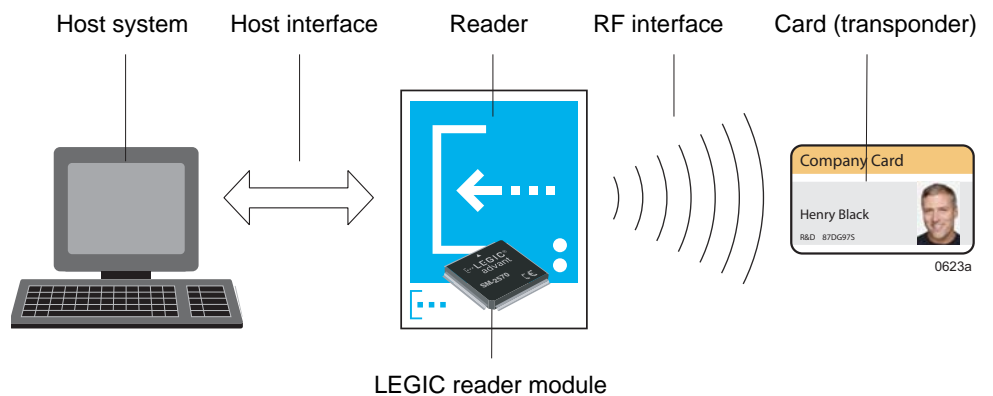
## 4 Technical security

To optimally secure a contactless smart card system a combination of different technical security measures is required. The measures are chosen in accordance with the security policy and the requirements of the application.

Besides the security elements already implemented in the LEGIC advant products (authentication, encryption) optional elements such as read/write protection or stronger encryption (DES, 3DES, AES) may be activated. This section gives best practice hints on using the individual security elements.

### End-to-end security in a contactless smart card system

The following illustration shows the components of a contactless smart card system for a better understanding of the security elements.



In order to choose the right protection measures, the full data path in the system has to be considered. This starts from the data stored in the card on the "front end", continues then over the air interface and reader and its wiring to the host system in the "back end". Respectively, the right component (reader, card, host system) and connections (RF interface, host interface) as well as the respective use of security elements in the contactless system have to be chosen.

### Card (transponder) types

Selecting the card type should be done in correspondance to the security requirements. When ranking the technologies, cards with LEGIC advant transponder chips (ATC...) support advanced security features compared to cards with LEGIC prime transponder chips (MIM...). For high security demands use microcontroller based smart cards with a LEGIC all-in-one area (AFS...).

### Securing the reader hardware

Especially for outdoor readers it is common practice to provide measures for securing the reader enclosure. A tamper proof enclosure (e.g. recessed mounting, special screws, tamper detect mechanism) or the use of a remote antenna can resist physical attacks.

In special cases it might also be appropriate to use a shielding for focussing the RF field in order to avoid eavesdropping of data in the stay field.

### Using LEGIC security elements

LEGIC advant reader modules already offer a comprehensive range of implemented security elements such as data integrity check on RF and host interface (MAC, CRC), data integrity check of card data (read after write), authentication between reader and card, encrypted data transmission on RF interface and encrypted data on card. These security elements are always active and provide a high protection against unauthorised data manipulation and eavesdropping.

To optimally adapt the system security to the requirements of the application, optional security elements can be activated:

- The LEGIC Master-Token System Control controls the access rights for issuing and personalising of cards. Due to this unique physical token based authorisation system only authorised persons who possess the required Master-Token can create card data segments.
- Sensitive card data can be read/write protected in such a way that only authorised readers can access these data (reader authorisation with physical token, independent of application software).
- If the host interface requires a protection against eavesdropping or data manipulation, a DES or 3DES encryption and/or an authentication may be applied.
- For cashless payment applications, a set of functions for secure cash transactions is provided (LEGIC cash standard).
- With LEGIC advant readers, which are configured to read only the card's serial number (UID), the LEGIC SafeID function should be used in any case. It enables a secure reading of the UID of ISO14443 A and ISO15693 compliant LEGIC cards (Background: The pure ISO14443 A standard provides here a disclosed serial number).

#### **Using host security elements**

If the contactless smart card system is connected to a host system, an appropriate configuration can strengthen the overall system security considerably.

- Most important is the monitoring of the system activity (e.g. for an access control system). This can detect unusual activities such as multiple entries of a person or other irregularities.
- To prevent the loss or manipulation of card data is common practice to backup the card data on the host system.
- To protect the host system data (e.g. access control data) it is recommended to use a secure server for the host system and to provide a firewall between host system and corporate IT systems.

#### **Combining security measures**

In many cases, an appropriate combination of security mechanisms can strengthen the system security of a contactless smart card system:

- For a stronger identification of the card holder, multiple authentication methods such as card with PIN or biometrics are recommended. Another common measure is the combination with CCTV monitoring.
- To avoid unwanted remote reading of card data in principle, also the wearing of the card when not in use can be considered. A shielded card case is a common measure. To complicate the forgery of the card design, holograms or other design security features are possible.
- To secure sensitive sites or buildings, also the mechanical security should be considered (security doors and windows, fences, person singling, scales).

## 5 Operational security

Besides the technical security also the definition and observance of processes is an important part of the overall system security. It is essential to define controlled processes, to train the involved staff and to audit processes and staff regularly.

- All employees should know how to handle the card. This may include e.g. wearing only inside the company, keeping in shielded case or hiding while not in use, reporting in case of loss.
- Special attention should be paid on the card issuing and card disposal process (personalisation of cards for new employees, withdrawal of cards from employees who left the company). This also includes the handling of lost or replaced cards.
- The Master-Token System Control is a very strong and unique LEGIC security feature. It is essential to define processes for secure handling and storage of all Master-Tokens (e.g. responsibilities and authorizations, access and handling rights, logging).
- Consider also the processes for installing and replacement of readers. They might contain encryption keys.
- Defining the process for updating the access rights in offline readers is recommended.

## 6 Appendix

**Recommended literature** The following document provides general recommendations on how to secure a RFID system:

- [1] National Institute of Standards and Technology (NIST),  
Guidelines for Securing Radio Frequency Identification (RFID) Systems,  
[http://csrc.nist.gov/publications/nistpubs/800-98/SP800-98\\_RFID-2007.pdf](http://csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf)