

Best Practices

Kontaktlose Smart Card Anwendungen sicher implementieren

Klassifikation: Öffentlich (Info Level 1)
Dokument-Nr.: LA-11-005d-de
Ausgabe: 2010

1 Einleitung

Hintergrund Die kontaktlose Smart Card Technologie erfreut sich seit vielen Jahren stetig wachsender Beliebtheit als bewährte, zuverlässige und kosteneffiziente Technologie für Identifikationszwecke. Insbesondere die Funktionalität und die komfortable Anwendung machten diese Technologie in vielen Bereichen zur bevorzugten Wahl für Identifikationsmedien - so auch für sicherheitsrelevante Anwendungen in Unternehmen, im Freizeitbereich und im Zahlungsverkehr. Die wichtigsten Anwendungen dieser Technologie umfassen die Personen-Zutrittskontrolle, das bargeldlose Bezahlen sowie damit zusammenhängende Applikationen, wie elektronische Türschlösser, Drucker, Parksysteme, Zeiterfassung, Transport und viele andere.

Während bei einigen Anwendungen, z.B. beim Parken oder der Zeiterfassung, das Hauptaugenmerk auf den organisatorischen Vorteilen, dem Nutzen durch Prozessautomatisierung oder gesteigerten Komfort liegt, werden kontaktlose Smart Cards von anderen Anwendern auch als Sicherheitselement zum Schutz von Anlagen und Einrichtungen gegen Zugang oder die Nutzung durch Unbefugte eingesetzt.

Wie bei jeder Technologie für Sicherheitszwecke gilt auch für kontaktlose Smart Cards das bekannte Prinzip, dass es keine absolute Sicherheit gibt. Die Überwindung einer Sicherheitstechnologie ist immer eine Frage von Zeit, Kosten und technologischem Fortschritt. Dennoch lässt sich das Risiko einer Umgehung der Sicherheit eines kontaktlosen Smart Card-Systems durch eine Reihe von "Best Practice" Massnahmen (beste Anwendungspraxis) minimieren.

Im vorliegenden Dokument werden Best Practises vorgestellt, die bei der Evaluation, Installation und dem Betrieb kontaktloser Smart Card Systeme basierend auf der LEGIC Technologie herangezogen werden sollten. Die daraus ermittelten Sicherheitselemente können zur Gewährleistung maximaler Systemsicherheit beitragen.

Welche Sicherheitsmassnahmen letztendlich eingesetzt werden, hängt von der Systemanwendung und den mit ihr zusammenhängenden Sicherheitsanforderungen ab. So sind zum Beispiel die Anforderungen an die Zugangskontrolle zu einem Parkhaus in den meisten Fällen weniger streng als an die zuverlässige Beschränkung des Zutritts zu einem Unternehmen.

Anzumerken ist, dass es zusätzlich zu den hier genannten Best Practices womöglich noch weitere geeignete Massnahmen geben kann, die im Einzelfall abzuwägen sind.

Zielgruppe Das vorliegende Dokument richtet sich an alle Personen oder Unternehmen, die kontaktlose Smart Card Systeme herstellen, integrieren oder anwenden. Dazu zählen Systemintegratoren, Berater, Endanwender und Hersteller von Anwendungen. Das Dokument kann in verschiedenen Lebenszyklen eines Systems genutzt werden: Evaluierung, Planung, Installation und Betrieb.

Als Endanwender sollten Sie sich mit Ihrem Systemintegrator oder Systemanbieter über die Systemsicherheit verständigen.

Änderungsgeschichte

| Änderung | Ausgabe |
|--------------------------|---------|
| Neu erstellt | 07.2008 |
| Kleinere Textkorrekturen | 01.2010 |

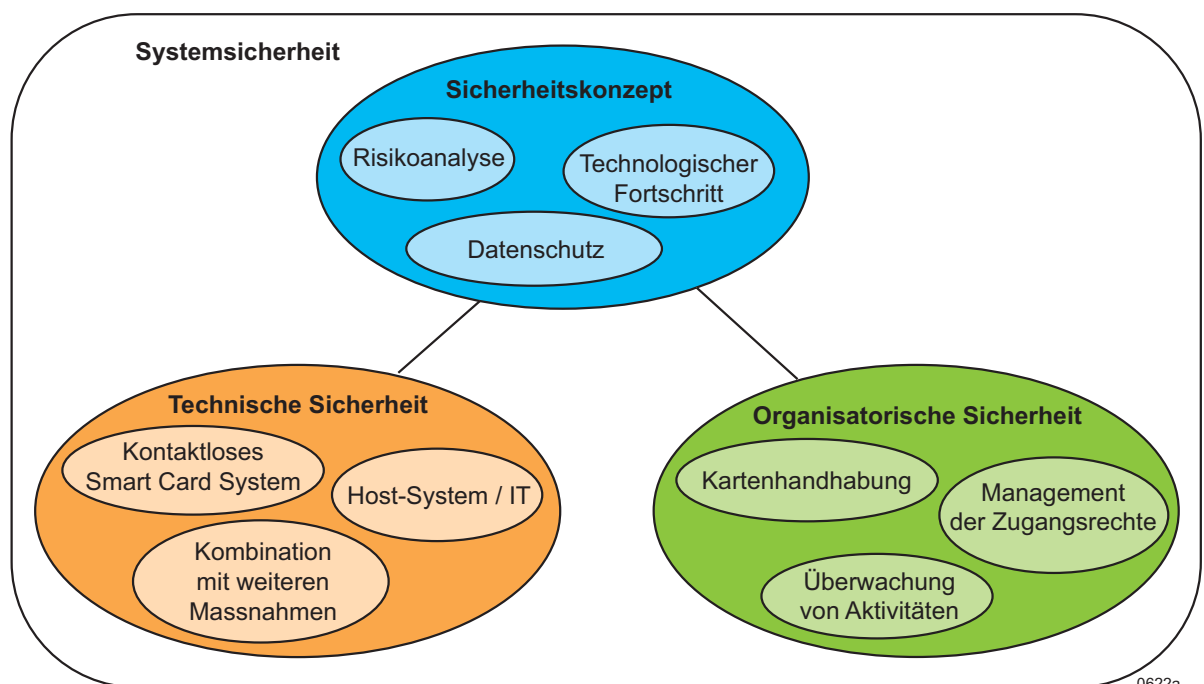
2 Die Sicherung eines kontaktlosen Smart Card Systems

Gesamtsicherheit des Systems

Um die maximale Sicherheit eines kontaktlosen Smart Card Systems zu gewährleisten, müssen verschiedene Sicherheitsmassnahmen in die Überlegungen einbezogen werden. Darunter fallen technische Massnahmen wie Datenverschlüsselung oder manipulationssichere Gehäuse, aber auch organisatorische Massnahmen wie Karten-Personalisierungsprozesse oder Richtlinien zum korrekten Tragen des Mitarbeiterausweises.

Die Gesamtsicherheit des Systems lässt sich in drei Bereiche unterteilen:

- **Sicherheitskonzept** (Welche Sicherheitsanforderungen gelten für das System?)
- **Technische Sicherheit** (Welche technischen Massnahmen sind erforderlich?)
- **Organisatorische Sicherheit** (Welche Prozesse müssen festgelegt werden?)



Die beste Systemsicherheit lässt sich erreichen, wenn so viele Massnahmen wie möglich, abgestimmt auf das erforderliche Sicherheitsniveau, umgesetzt werden. Bei Umsetzung all dieser Massnahmen ist es erheblich aufwendiger, ein System zu kompromittieren.

Des weiteren ist es wichtig, die Rolle des kontaktlosen Smart Card Systems im Gesamtkonzept zu bewerten und daraus entsprechende Massnahmen abzuleiten. So könnte es gegebenenfalls viel einfacher sein, durch ein Fenster in eine Anlage einzudringen oder die Geldkassette eines Automaten aufzubrechen, statt direkt das Smart Card System anzugreifen. Entsprechend kann es für ein effektives Sicherheitskonzept ebenso wichtig sein, geeignete Überwachungsmaßnahmen oder Alarmanlagen festzulegen.

- LEGIC Systemsicherheit** LEGIC Identsystems AG bietet ein breites Produktportfolio, das sich an unterschiedlichen Kundenanforderungen wie Sicherheit, Flexibilität, Komfort oder Kosten-Nutzen-Überlegungen orientiert. Seit Beginn seiner Tätigkeit hat LEGIC dem Thema Systemsicherheit grosse Aufmerksamkeit gewidmet und zusätzliche Elemente als integrale Bestandteile eines mehrschichtigen Sicherheitskonzepts implementiert. Die LEGIC advant Technologie deckt z.B. folgende Komponenten ab:
- Technische Massnahmen wie die Authentifizierung der Karte durch den Leser (LEGIC SafeID) und/oder verschlüsselte Datenübertragung und Datenspeicherung
 - Master-Token System Control (Autorisierung mittels physikalischer Tokens)
 - Organisatorische Massnahmen wie die restriktive und gezielte Weitergabe von Produktinformationen

3 Sicherheitskonzept

Zur Gewährleistung der Gesamtsicherheit des Systems ist es empfehlenswert, ein übergreifendes Sicherheitskonzept zu definieren. Jeder Betreiber eines kontaktlosen Smart Card Systems sollte die Sicherheitsanforderungen seines Systems beurteilen. So sind zum Beispiel für den Zugang zu Banken oder Flughäfen in der Regel höhere Sicherheitsstandards erforderlich als für den Zugang zu einem Parkplatz oder einer Skiregion.

- Aufsetzen eines Sicherheitskonzepts** Ein Sicherheitskonzept deckt üblicherweise die folgenden Aspekte ab:
- Eine Risikoanalyse hilft dabei, die möglichen Risiken zu identifizieren und stellt die Grundlage zur Festlegung der technischen und organisatorischen Sicherheitsmassnahmen dar.
 - Ein wesentlicher Aspekt ist ebenso die sorgfältige Betrachtung der Elemente Datenschutz und Datensicherheit. Der Umgang mit sensiblen Daten muss mit den Bedürfnissen der Karteninhaber und des Unternehmens und mit den geltenden Bestimmungen in Einklang gebracht werden.
 - Um auf zukünftige Entwicklungen vorbereitet zu sein und den technologischen Fortschritt angemessen berücksichtigen zu können, sind regelmässige Bewertungen des Systems unbedingt zu empfehlen. Aus dieser Bewertung können dann geeignete Massnahmen für die zukünftige Entwicklung des kontaktlosen Smart Card Systems abgeleitet werden (siehe auch nächsten Abschnitt).
 - Ein Sicherheitskonzept sollte auch Aspekte wie die physikalischen und logischen Zugangsrechte für alle Karteninhaber oder die Verbindung zum IT-System des Unternehmens abdecken.

Ausgehend vom Sicherheitskonzept werden die technischen und organisatorischen Sicherheitsmassnahmen definiert.

- Technologischer Fortschritt** Aufmerksame Beobachtung der technologischen Weiterentwicklung in der Sicherheitsbranche ist eine Voraussetzung, um auf die Zukunft vorbereitet zu sein. Abgeleitet aus dem Fortschritt der Technologie, empfiehlt es sich eine Roadmap ("Fahrplan") für die Sicherheitsentwicklung des Unternehmens festzulegen. Diese Roadmap hilft, die geleisteten Investitionen zu schützen, und gibt den Migrationspfad für das kontaktlose Smart Card System vor. Ein Szenario kann Massnahmen wie z.B. den Übergang von einer Leser-Generation zur nächsten oder das Vorsehen einer Möglichkeit zur Softwareaktualisierung für jeden Leser enthalten (z.B. Firmware-Upgrades, Einschalten der Multi-RF-Standard-Schnittstellen).

Beispiel für ein Migrationsszenario

Die folgende Beispielsequenz zeigt ein nahtloses Migrationsszenario von einem LEGIC prime System zu einem LEGIC advant System:

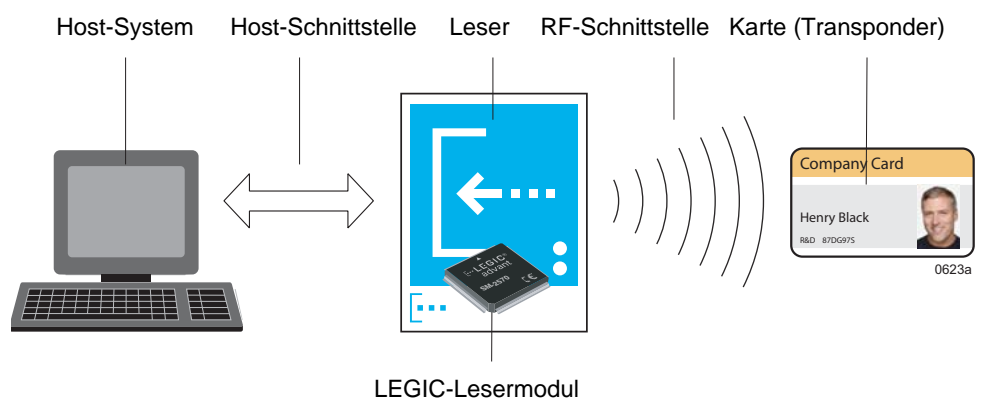
1. LEGIC prime Master-Tokens durch LEGIC advant Master-Tokens ersetzen. Ausschliesslich LEGIC advant Master-Tokens für die Ausgabe neuer Karten verwenden.
2. LEGIC prime-Leser Schritt für Schritt durch LEGIC advant-Leser ersetzen. LEGIC prime-Karten Schritt für Schritt durch LEGIC advant-Karten ersetzen.
3. Wo erforderlich, Smart Cards auf Mikrocontroller-Basis einsetzen (mit LEGIC all-in-one-Bereich).

4 Technische Sicherheit

Um ein kontaktloses Smart Card System optimal zu sichern, ist eine Kombination unterschiedlicher technischer Sicherheitsmassnahmen erforderlich. Die Auswahl der Massnahmen richtet sich nach dem Sicherheitskonzept und den Anforderungen der Anwendung. Neben den Sicherheitselementen, die bereits in den LEGIC advant Produkten implementiert sind (Authentifizierung und Verschlüsselung) können auch optionale Elemente wie Lese-/Schreib-Schutz oder stärkere Verschlüsselung (DES, 3DES, AES) aktiviert werden. Der folgende Abschnitt enthält Hinweise zur besten Verwendung der einzelnen Sicherheitselemente.

Durchgehende "Ende zu Ende"-Sicherheit in einem kontaktlosen Smart Card System

Zum besseren Verständnis der Sicherheitselemente zeigt die folgende Abbildung die Komponenten eines kontaktlosen Smart Card Systems.



Um die richtigen Schutzmassnahmen zu wählen, sollte der gesamte Datenpfad im System betrachtet werden. Er beginnt bei den auf der Karte gespeicherten Daten am "Frontend" und setzt sich dann über die drahtlose Schnittstelle und dem Leser über die Verbindung zum Host-System am "Backend" fort. Entsprechend werden dann einerseits die jeweils richtige Komponente (Leser, Karte, Host-System) und andererseits die richtigen Verbindungen (RF-Schnittstelle, Host-Schnittstelle) sowie die entsprechenden Sicherheitselemente im kontaktlosen System gewählt.

Kartentypen (Transponder)

Die Auswahl des Kartentyps muss in Abstimmung mit den Sicherheitsanforderungen erfolgen. Stuft man die Transpondertypen ein, so verfügen LEGIC advant Karten (ATC...) über fortgeschrittenere Sicherheitsmerkmale verglichen mit LEGIC prime Transponder-Karten (MIM...). Für hohe Sicherheitsanforderungen sollten Smart Cards auf Mikrocontroller-Basis mit einem LEGIC all-in-one Bereich (AFS...) genutzt werden.

Sicherung der Leser-Hardware Insbesondere bei Lesern im Aussenbereich ist es üblich, Massnahmen zum Schutz des Leser-Gehäuses einzusetzen. Ein manipulationssicheres Gehäuse (z. B. Unterputzmontage, Spezialschrauben, Sabotagekontakt) oder eine abgesetzte Antenne kann physische Angriffe verhindern.
In Sonderfällen kann es auch angebracht sein, mit einer Schirmung zur Bündelung des RF-Felds zu arbeiten, um ein Abhören der Daten im Streufeld zu verhindern.

Der Einsatz von LEGIC Sicherheitselementen LEGIC advant Leser bieten bereits eine umfassende Palette implementierter Sicherheitselemente, z. B. Datenintegritätsprüfung auf RF- und Host-Schnittstelle (MAC, CRC), Datenintegritätsprüfung der Kartendaten (Lesen nach Schreiben), Authentifizierung zwischen Leser und Karte, verschlüsselte Datenübertragung auf RF-Schnittstelle und verschlüsselte Daten auf der Karte. Diese Sicherheitselemente sind immer aktiv und bieten leistungsstarken Schutz gegen unbefugte Datenmanipulation und Abhören.

Um die Systemsicherheit optimal auf die Anforderungen der Anwendung anzupassen, können optionale Sicherheitselemente aktiviert werden:

- Mit dem LEGIC Master-Token System Control werden die Zugangsrechte für die Ausgabe und Personalisierung von Karten vergeben und kontrolliert. Dank dieses einzigartigen Autorisierungssystems auf Grundlage physikalischer Tokens können nur autorisierte Personen, die das erforderliche Master-Token besitzen, Datensegmente auf dem Transponder erstellen.
- Sensible Kartendaten können lese-/schreib-geschützt sein, dass nur autorisierte Leser auf diese Daten zugreifen können (Autorisierung des Lesers durch physikalisches Token unabhängig von der Anwendungssoftware).
- Wenn an der Host-Schnittstelle ein Schutz gegen Abhören oder Datenmanipulation erforderlich ist, können eine DES- oder 3DES-Verschlüsselung und/oder eine Authentifizierung zum Einsatz kommen.
- Für Anwendungen zur bargeldlosen Zahlung werden einige Funktionen für sichere Bezahltransaktionen angeboten (LEGIC cash Standard).
- Bei LEGIC advant Lesern, welche so konfiguriert sind, dass ausschliesslich die Seriennummer des Kartenmediums (UID) ausgelesen wird, sollte unbedingt die LEGIC SafeID-Funktion zum Einsatz kommen. Sie ermöglicht ein sicheres Lesen der UID von LEGIC-Karten, die ISO 14443 A und ISO 15963 entsprechen (Hintergrund: die reine Norm ISO 14443 A sieht hier eine offengelegte Seriennummer vor).

Einsatz von Host-Sicherheitselementen Falls das kontaktlose Smart Card System mit einem Host-System verbunden ist, kann die Gesamtsicherheit durch eine optimal geeignete Konfiguration erheblich gesteigert werden.

- Am wichtigsten ist die Beobachtung der Systemaktivität (z. B. für ein Zugangskontrollsystem). So können ungewöhnliche Aktivitäten wie der mehrfache Zugang der gleichen Person oder andere Unregelmässigkeiten entdeckt werden.
- Um den Verlust oder die Manipulation von Kartendaten zu verhindern, ist es allgemein üblich, eine Sicherung der Kartendaten auf dem Host-System vorzunehmen.
- Um die Daten des Host-Systems zu schützen (z. B. Zugangskontrolldaten), ist der Einsatz eines sicheren Servers für das Host-System und die Einrichtung einer Firewall zwischen Host-System und den übrigen IT-Systemen des Unternehmens zu empfehlen.

Kombination von Sicherheitsmassnahmen In vielen Fällen kann eine angemessene Kombination von Sicherheitsmechanismen die Systemsicherheit eines kontaktlosen Smart Card Systems steigern:

- Für eine eindeutigere Identifikation des Karteninhabers werden mehrfache Authentifizierungsverfahren wie eine Karte plus PIN oder biometrische Daten empfohlen. Eine weitere übliche Massnahme ist die Kombination mit Videoüberwachung (CCTV).
- Um ein unerwünschtes Fernablesen der Kartendaten grundsätzlich zu verhindern, kann man beim Tragen der Karte bei Nichtverwendung eine abgeschirmte Kartenhülle verwenden. Um die Fälschung des Kartendesigns zu erschweren, sind Hologramme und weitere Design-Sicherheitselemente möglich.

- Um sensible Standorte oder Gebäude zu sichern, sollte auch die mechanische Sicherheit berücksichtigt werden (Sicherheitstüren und -fenster, Zäune, Personenvereinzelnung, Waagen).

5 Organisatorische Sicherheit

Neben der technischen Sicherheit ist auch die Festlegung und Einhaltung von Prozessen ein wichtiger Bestandteil der Gesamtsicherheit des Systems. Es ist erforderlich, kontrollierte Prozesse festzulegen, die beteiligten Mitarbeiter zu schulen und die Prozesse und Mitarbeiter regelmäßigen Überprüfungen zu unterziehen.

- Alle Mitarbeiter müssen über den Umgang mit der Karte unterrichtet sein. Dazu kann zum Beispiel zählen, die Karte nur innerhalb des Unternehmens zu tragen, sie in einer geschirmten Hülle aufzubewahren oder bei Nichtverwendung zu verbergen und den Verlust der Karte umgehend zu melden.
- Besondere Aufmerksamkeit sollte auf den Prozess der Ausstellung und Rücknahme der Karte gelegt werden (Personalisierung der Karten für neue Mitarbeiter, Einziehung der Karten von Mitarbeitern, die das Unternehmen verlassen). Darunter fällt auch der Umgang mit dem Verlust und dem Austausch von Karten.
- Das Master-Token System Control ist ein einzigartiges, äusserst leistungsstarkes Sicherheitsmerkmal von LEGIC. Es ist unabdingbar, Verfahren für die sichere Handhabung und Aufbewahrung aller Master-Tokens festzulegen (z. B. Zuständigkeiten und Autorisierungen, Zugangs- und Handhabungsrechte, Protokollierung).
- Auch zu den Verfahren für Installation und Austausch von Lesern sind sorgfältige Überlegungen erforderlich. Leser könnten Schlüssel oder andere Geheimnisse enthalten.
- Empfohlen wird auch die Festlegung eines Prozesses zur Vergabe der Zugangsrechte in Offline-Lesern.

6 Anhang

Empfohlene Dokumente Das folgende Dokument enthält allgemeine Empfehlungen zur Sicherung eines RFID-Systems:

- [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