LEGIC

Whitepaper

Wie ist der Zugang zu Ihrem Zutrittskontrollsystem geschützt?

Autoren: John Harvey, Leon Rose, Carl Fenger,
LEGIC Identsystems AG

LEGIC Master-Token System-Control (MTSC): Sicherheit in den eigenen Händen für Unternehmen und Institutionen

Zusammenfassung

Bei der Frage: „Wer hat Zutritt zu kritischer Infrastruktur und wie lässt sich dieser verwalten?“ ist der anfälligste Angriffspunkt weder das Zutrittskontrollsystem selbst, noch die verwendete Verschlüsselung oder physische Medien wie Ausweise. Problematisch ist in diesem Fall, wie die in die Türschlösser integrierten kryptografischen Schlüssel überhaupt dorthin gelangen.

Zutrittsskontrollsysteme können bereits vor Abschluss der Installation in Gefahr sein

Für Regierungsgebäude, Schulen, Büros, Flughäfen und Privathäuser bzw. -wohnungen wird eine sichere Zutrittskontrolle immer wichtiger, um sich vor Diebstahl und Kriminalität sowie vor dem physischen Zugriff auf sensible Daten zu schützen. In Einrichtungen des Gesundheitswesens wie Krankenhäusern oder Pflegeheimen ist eine wirksame und berührungslose Zutrittskontrolle von entscheidender Bedeutung, um etwa die Verbreitung von Krankheitserregern wie COVID zu verhindern.

Glücklicherweise hat sich die moderne Technologie so weit entwickelt, dass die automatisierte Authentifizierung von Personen und die sichere Verwaltung von Smartcard-basierten persönlichen Credentials praktisch unangreifbar ist. Die meisten Zutrittskontrollsysteme verwenden eine symmetrische Verschlüsselung, die auf Techniken wie AES („Verschlüsselung nach Militärstandard") basiert. Das bedeutet, dass der Zutritt zu Infrastrukturen, die mit dieser Technologie ausgestattet sind, mit Smartcards (Ausweisen) weitgehend sicher ist, aber erst nach seiner Implementierung.

Sicherheit nur so stark wie das schwächste Glied

Wir alle gehen Tag für Tag mit der heutigen Smartcard-basierten Technologie für die Zutrittskontrolle um. Die meisten von uns nutzen sie, wenn sie mit einem Ausweis als Credential ihren Arbeitsplatz oder das Universitätsgelände betreten. Die Sicherheit basiert darauf, dass niemand Zugang zum Verschlüsselungscode hat (auch „Passwort" genannt), der im sicheren Speicher des Türschlosses gespeichert ist. Bei der AES-Verschlüsselung handelt es sich beim Code um eine 128-, 192- oder 256-Bit-Zahl. Moderne Halbleitertechnologie in Form eines „Secure Element" verhindert den physischen oder elektrischen Zugang zu diesem Verschlüsselungscode, sobald er in elektronischen Türschlössern gespeichert ist, selbst für die raffiniertesten Hacker.

Ein Manko verbleibt allerdings.

Wie werden Verschlüsselungscodes installiert?

Bei der Frage: „Wer hat Zutritt zu Gebäuden, Räumlichkeiten und Lagerbereichen und wie lässt sich dieser verwalten?" ist der anfälligste Angriffspunkt weder das Zutrittskontrollsystem selbst, noch die verwendete Verschlüsselung oder physische Medien wie Ausweise. Problematisch ist in diesem Fall allerdings, wie die in die Türschlösser integrierten kryptografischen Schlüssel überhaupt dorthin gelangen. Ein Verstoss auf dieser fundamentalen Ebene der Zugangssicherheit kann die gesamte Zutrittskontrolle angreifbar machen.

Nachteile der werksseitigen Programmierung

Wie kann nun sichergestellt werden, dass kryptografische Schlüssel sicher in Türschlössern installiert sind? Eine Möglichkeit ist die „Programmierung ab Werk" eines jeden Schlosses, bevor es die Fertigungslinie verlässt. Diese Vorgehensweise sorgt dafür, dass die Verschlüsselungscodes vor der Auslieferung an die Kunden sicher in das Schloss integriert werden. Es gibt jedoch drei fundamentale Probleme bei dieser Vorgehensweise:

1) Externe Abhängigkeit

Werden elektronische Schlösser bei einem externen Anbieter vorprogrammiert, ist die Sicherheitseigentümerschaft unmittelbar gefährdet. Wie viele Drittanbieter, IT- und Logistikpersonal hatten während der Herstellung und Lieferung Zugang zu den Verschlüsselungscodes, bevor das Schloss eingebaut wurde? Die Antwort hilft gar nicht weiter – Sie wissen es nämlich nicht. Die Sicherheitsprozesse bei externen Lieferanten werden innerhalb ihrer eigenen vier Wände definiert, kontrolliert und geprüft, und die Prozesse sind für die Endkunden nicht zu 100 % transparent. Aus diesem Grund sollte die werksseitige Programmierung von Verschlüsselungscodes mit Ausnahme bestimmter begrenzter Fälle vermieden werden. Die Endkunden müssen in der Lage sein, ihre Zugangsinfrastruktur mit Verschlüsselungscodes (neu) zu konfigurieren, die in ihrem Eigentum sind und die sie kontrollieren.

2) Logistik

Die Hersteller elektronischer Türschlösser produzieren jedes Jahr Millionen von Schlössern für Tausende von Kunden. Solange die Schlösser als „Rohlinge" geliefert werden, die von den Endkunden in der Endphase konfiguriert werden können, kann die Logistik einfach gehalten werden – ein Produkt für alle. Sobald werksseitig programmierte Schlösser erstellt werden, wird aus einem einzigen Produkt, das für viele Kunden geeignet ist, ein kundenspezifisches Produkt, mit allen damit verbundenen Lager- und Logistikproblemen, die mit der Verwaltung Tausender verschiedener Varianten verbunden sind. Dies erhöht die Kosten des Schlosses erheblich und birgt das Risiko einer Über- oder Unterproduktion sowie von Fehlern.

3) Wechsel des Eigentümers

Unternehmen schliessen, ziehen um und wechseln immer mal wieder den Eigentümer. Um zu verhindern, dass frühere Eigentümer auf die von ihnen zurückgelassene Infrastruktur zugreifen, muss jedes Türschloss vom neuen Eigentümer mit neuen Verschlüsselungscodes umpro-

grammiert werden. Das macht die Vorteile der werksseitigen Programmierung zunichte.

Programmierung vor Ort

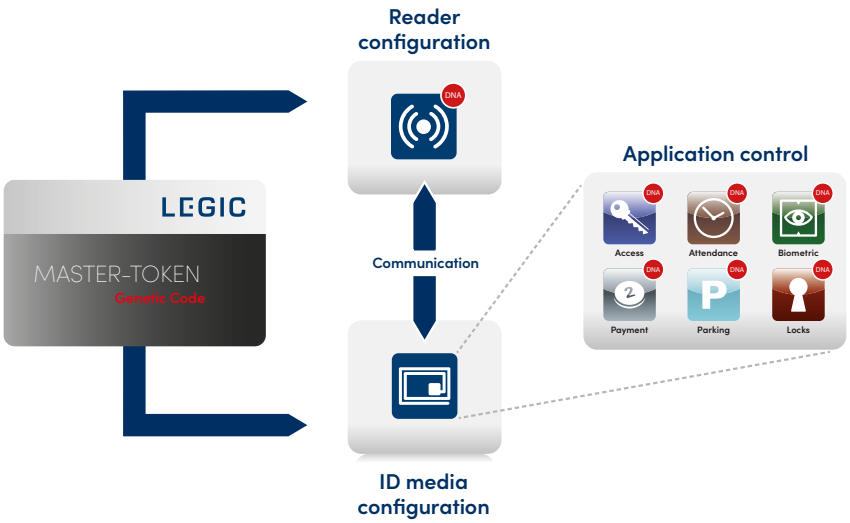
Wenn Türschlösser als Rohlinge (ohne vorprogrammierten Schlüsselcode) installiert werden, können sie aufgrund der fehlenden Verschlüsselung nicht über ein Netzwerk programmiert werden – eine Verschlüsselung ist nur möglich, sobald der Verschlüsselungscode installiert ist. Die Person, die den Schlüssel vor Ort installiert, stellt ebenfalls einen Risikofaktor dar. Falls der Schlüssel sichtbar ist, kann er leicht kopiert, ins Gedächtnis eingeprägt oder fotografiert werden.

Bei der Inbetriebnahme der meisten Zutrittskontrollsysteme muss das Sicherheitspersonal mit Hilfe eines speziellen Geräts jedes Türschloss mit entsprechenden Verschlüsselungscodes versehen. Um zu verhindern, dass der Schlüssel bei der Initialisierung des Schlosses offengelegt wird, hat LEGIC seine einzigartige Lösung „Master-Token System-Control" für Schlüssel- und Berechtigungsmanagement (MTSC) entwickelt. Damit erhalten Unternehmen und Institutionen absolute Unabhängigkeit und Kontrolle über die Zugangssicherheit ihrer Organisation, einschliesslich Karten und Lesegeräten.

Ein geteiltes Geheimnis ist kein Geheimnis mehr

Das wichtigste Sicherheitsmerkmal von MTSC ist der **bewusste Verzicht auf Geheimnisse (Secrets)**, wie Verschlüsselungscodes oder Passwörter, die mit dem Personal für Installation und Sicherheitsverwaltung geteilt werden. Die Berechtigungen werden stattdessen durch nicht von Menschen lesbare, physische Tokens in Form von unkopierbaren, kontaktlosen Smartcards erteilt.

Unternehmen, die ein Sicherheitssystem verwenden, welches auf sichtbaren Passwörtern basiert, sind sich in der Regel nicht bewusst, dass sie gefährdet sind und wie



LEGIC Master-Token System-Control (MTSC)

leicht Schaden für sie entstehen kann. Sichtbare Passwörter können jederzeit und völlig unbemerkt nach aussen dringen. MTSC verwendet keine Passwörter. Das ermöglicht eine bessere Kontrolle über die Sicherheit bei kontaktlosen Smartcard-Anwendungen. MTSC basiert auf einem einzigartigen, unsichtbaren „genetischen Code", der in kontaktlose Smartcards integriert ist.

Der Code wird bei der Initialisierung des Ausweises und bei der Systemkonfiguration per RFID kontaktlos an die Lesegeräte übertragen. Die Verwendung eines physischen Token ermöglicht es Administratoren ausserdem, ihre **Ausweispopulation sicher zu verwalten und Anwendungen nach Bedarf einfach hinzuzufügen oder zu entfernen** (z. B. Zutrittskontrolle, Zeit- und Anwesenheitserfassung, sicheres Drucken, elektronische Zahlungen für Verkaufsautomaten und Kantinen usw. Bis zu 127 Anwendungen können auf einer einzigen Karte untergebracht werden). Darüber hinaus gewährt das Eigentum eines physischen Token den Sicherheitsbeauftragten volle Autonomie bei der Auswahl vertrauenswürdiger Lieferanten, wenn sie dies wünschen.

Unabhängige Eigentümerschaft vs. Delegation an Dritte

Obwohl die hundertprozentige Eigentümerschaft an der Sicherheitsimplementierung für Zutrittskontrollsysteme für eine Unternehmenszentrale wichtig ist, kann die Delegation der Implementierung von Verschlüsselungscodes an vertrauenswürdige Dritte in entfernten Aussenstellen oder an externe Kartenleserhersteller oft zweckmässig sein. Dies lässt sich mit einer „begrenzten Initialisierungskarte" leicht realisieren.

Eigentümer eines MTSC müssen nicht ständig ein systemweites Passwort oder einen Verschlüsselungscode herausgeben, sondern können externen Installateuren und natürlich Kartenherstellern ein physisches Token geben, das die Anzahl der von ihnen durchführbaren Lesegerät- und Credential-Konfigurationen begrenzt. Dies ermöglicht, dass ausgelagerte Zugangssicherheitsdienste streng kontrollierbar, nachvollziehbar, und überprüfbar sind („Hierarchische Delegation von Rechten").

LEGIC Master-Token für die sichere Initialisierung von Karten und Lesegeräten über RFID

Sicherheit durch Organisationsstruktur und Prozesse

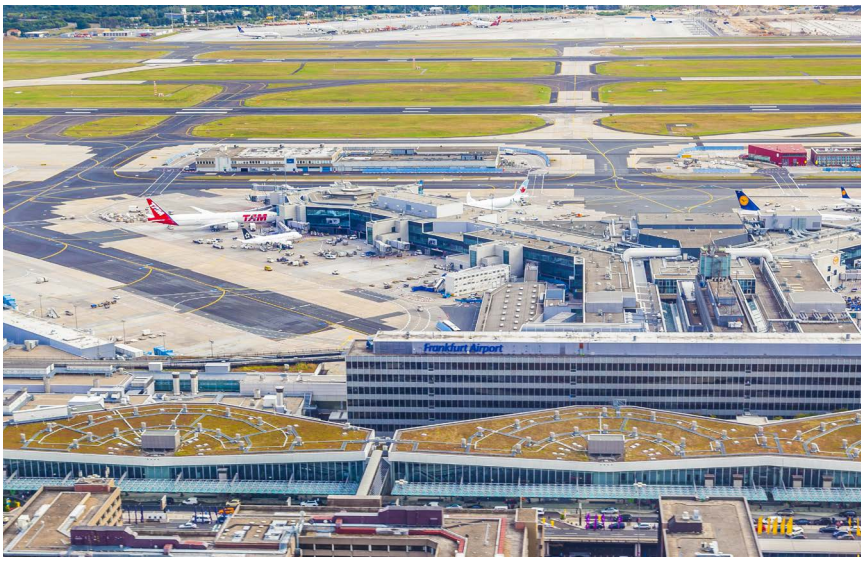
Die Sicherheit des Gesamtsystems wird durch den physischen Schutz der Master-Token sichergestellt, weil die Verschlüsselungscodes vor neugierigen Augen verborgen bleiben, ähnlich wie bei der Aufbewahrung von Goldbarren in einem Safe. Durch die Einhaltung einfacher und grundlegender Massnahmen ist die Initialisierung des Kartenlesegeräts und die Kartenproduktion durch ein angemessenes Sicherheitsniveau und autorisiertes Personal gesichert. Master-Token können nur über einen dokumentierten Workflow mit entsprechenden Genehmigungsstufen und unter anderem nach dem Vier-Augen-Prinzip entfernt werden.

Bei Systemen, die auf von Menschen lesbaren Secrets wie sichtbaren Passwörtern beruhen, verbleibt der Schlüssel, sobald er aus dem „Safe" entfernt wird, im Gedächtnis mindestens einer Person. Mit MTSC gibt es kein derartiges „Wissen" in den Händen von Einzelpersonen.

Überprüfbare Prozesse ermöglichen

Da der Verschlüsselungscode im Token eingeschlossen ist und weder von einer Person gelesen noch über digitale Netzwerke ausgetauscht werden kann, ist es einfach, grundlegende und überprüfbare, organisatorische Massnahmen zu implementieren. Das sorgt für ein hohes Sicherheitsniveau für das Master-Token. Der Schutz ist vergleichbar mit dem, der für physische Gegenstände wie Bargeld oder Edelmetalle erreicht wird.

Der gleiche Prozess für von Menschen lesbare oder über ein Netzwerk austauschbare Daten ist weitaus komplexer und birgt erheblich höhere Sicherheitsrisiken. MTSC ermöglicht somit die einfache Implementierung von überprüfbaren Prozessen, wie sie in ISO-27001, Annex A.9 Access Control beschrieben sind. Darin sind die Best Practices zur Sicherung des Zugangs zu Daten aufgeführt, und es wird sichergestellt, dass Mitarbeitende nur auf Daten zugreifen können, die für ihre Arbeit relevant sind.



MTSC Anwendungsbeispiel Flughafen Frankfurt, Deutschland

MTSC Anwendungsfall Flughafen Frankfurt

Der Flughafen Frankfurt am Main ist der grösste deutsche Verkehrsflughafen. Der Flughafen beschäftigt rund 81.000 Mitarbeitende an verschiedenen Standorten in der ganzen Welt. Um die Sicherheit der Zugangskontrollen für ihre Mitarbeitenden und Auftragnehmenden zu verwalten, haben die Flughafenbehörden ein mehrstufiges MTSC-Sicherheitskonzept für die zahlreichen Funktionen, Prozesse und Anwendungen eingeführt. Dazu gehört auch ein einheitliches Zutrittskontrollsystem für Mitarbeitende und Auftragnehmende, das auf kontaktlosen ID-Karten als Identifikationsmedium basiert. Lesen Sie mehr über die Implementierung „Flughafen Frankfurt: Wie schützt man ein Zutrittskontrollsystem so, dass es problemlos Audit-Prüfungen unterzogen werden kann?"

Weitere Informationen darüber, wie Sie mit LEGIC MTSC die volle Kontrolle über ein Zutrittskontrollsystem übernehmen können, finden Sie auf unserer Website.

About LEGIC

Seit über 30 Jahren ermöglicht LEGIC Unternehmen aus aller Welt die Implementierung von Lösungen mit anspruchsvollen Sicherheitsanforderungen. Auf der Grundlage von Schlüsselverwaltung, Trusted Services und sicheren, kontaktlosen Halbleitern bietet die LEGIC-Sicherheitsplattform End-to-End-Sicherheit für Smartphone- und Smartcard-basierten Zugriff, Mobilität, gemeinsam genutzte Ressourcen und industrielle IoT-Anwendungen.

Autoren: John Harvey, Leon Rose, Carl Fenger

November 2022