



NEWSLETTER

FEBRUAR 2010

Sehr geehrter Kunde/Partner,

es ist soweit! Die „Mifare-Attacke“ stand im Mittelpunkt unseres 6. Kundentages 2008 und war Thema heftiger Diskussionen. Unter Kunden und Partnern wurde schon damals über die Sicherheit von LEGIC prime spekuliert. Die Vertreter von LEGIC hatten bereits zu diesem Zeitpunkt auf unserem Kundentag darauf hingewiesen, dass es keine 100%ige Sicherheit gibt. Jetzt haben wir die Gewissheit. Durch eine Untersuchung des Chaos Computer Clubs und einer – nach unserem Geschmack zu einseitigen – Reportage des ARD-Politikmagazins Kontraste ist klar: „LEGIC prime ist nicht mehr sicher“.

Was bedeutet das für Sie als Kunde und Partner? Grundsätzlich gilt, dass Sicherheit ein Ergebnis aus einer Vielzahl von unterschiedlichen technischen und organisatorischen Komponenten ist. Allein die Tatsache, dass ein LEGIC prime Chip kompromittiert werden kann, bedeutet nicht automatisch, dass das gesamte System unsicher ist. Dies ist auch der Grund, weshalb wir die Darstellung des ARD-Magazins als sehr einseitig und „medienwirksam“ einstufen.

Panik ist nicht angesagt. Abhängig vom Gefährdungspotential Ihrer Organisation kann eine erneute Sicherheitsanalyse jedoch sinnvoll sein. Auf einige Gegenmaßnahmen wollen wir in unserem Newsletter hinweisen.

Als LEGIC Partner stehen wir Ihnen für weitere Fragen gerne zur Verfügung.

Mit besten Wünschen

Ihr vps-Team

Die absolute Sicherheit!?

Anlässlich einer Fachtagung des Chaos Computer Clubs in Berlin Ende Dezember 2009 präsentierte eine Expertengruppe neueste Erkenntnisse zum Reverse Engineering von LEGIC prime und anderen Transponder Chips. Im Rahmen dieser Präsentation wurde unter anderem die Aussage gemacht, dass die Anfang der 90er Jahre entwickelte LEGIC prime Technologie damals eine Pionierleistung darstellte. Heute sei die Sicherheit von LEGIC prime jedoch schwach und könne größtenteils überwunden werden. Bereits im Dezember 2007 hatte der CCC den in Zusammenarbeit mit der University of Virginia durchgeführten „Mifare Hack“ vorgestellt.

Die absolute Sicherheit gibt es nicht! Dieses Prinzip gilt grundsätzlich für jede Sicherheitstechnologie. Kontaktlose Smartcards mit LEGIC Technologie machen hier keine Ausnahme. Die Überwindung einer Sicherheitstechnologie ist immer eine Frage von Zeit, Kosten und technologischem Fortschritt.

Entsprechend den 1992 verfügbaren technischen Möglichkeiten für RFID IC's verwendet Prime ein festes Chiffrierverfahren. Die Sicherheit dieses Verfahrens basiert auf der Geheimhaltung der verwendeten Algorithmen. Heute favorisierte Verfahren basieren auf offenen Algorithmen und geheimen Schlüsseln. Im Vergleich mit heutigen Verfahren werden ältere Methoden häufig als kritisch beurteilt.

Mit MIFARE DESfire und LEGIC advant gibt es neue Technologien, die auf diesen Standards aufbauen. MIFARE DESfire wurde 2004 eingeführt. LEGIC advant ist bereits seit fünf Jahren auf dem Markt. advant unterstützt eine Verschlüsselung bis AES sowie den Einsatz von derzeit hochsicheren mikroprozessorbasierten Karten.

Ein kontaktloses Smartcardsystem besteht aus mehreren Komponenten wie Ausweise, Leser und Hostsystem. Um die maximale Sicherheit eines kontaktlosen Smartcardsystems zu gewährleisten, muss das gesamte System umfassend betrachtet und es müssen verschiedene Sicherheitsmaßnahmen in die Überle-

gungen mit einbezogen werden. Darunter fallen z.B. technische Maßnahmen wie Datenverschlüsselung oder manipulationssichere Gehäuse, aber auch organisatorische Maßnahmen wie Prozesse zur Ausweisbeantragung, Personalisierung und Verwaltung, oder Richtlinien zum korrekten Tragen der Ausweise.

Jede Anwendung eines kontaktlosen Smartcardsystems hat spezifische Anforderungen bezüglich des Gefährdungspotentials und daraus resultierende Sicherheitsanforderungen. Gängige Praxis ist es, ein Sicherheitskonzept zu erstellen, in dem die Sicherheitsanforderungen an das System festgelegt und daraus die notwendigen technischen und organisatorischen Maßnahmen abgeleitet werden.

Die Sicherheit von LEGIC prime ist gebrochen. Was ist zu tun? Grundsätzlich bietet sich der Umstieg auf LEGIC advant an. Dieser Schritt wird auch vom Chaos Computer Club empfohlen und ist für Prime User sicherlich der einfachste und zukunftssicherste Weg.

Da dieser Schritt bei bestehenden Installationen mit zusätzlichen Kosten verbunden ist, muss sicher von Fall zu Fall, abhängig von der Sicherheitsanalyse entschieden werden. Neben der Migration auf LEGIC advant bietet sich auch die Kombination mit zusätzlichen Sicherheitsmerkmalen (wie z.B. PIN, Biometrie) an.

Inhalt:	Seite
Migration von LEGIC prime auf LEGIC advant	2
Unterstützung von LEGIC Hybrid-Ausweisen	2
Besuchen Sie uns auf der....	2

Migration von LEGIC prime auf LEGIC advant

Unter dem Begriff Migration versteht man die schrittweise Umstellung des kontaktlosen Smartcardsystems von einer Technologieplattform auf eine andere. In diesem Fall der Umstieg von LEGIC prime auf LEGIC advant mit dem Ziel, die Sicherheit des Gesamtsystems zu erhöhen.

Bei der Migration müssen die drei zentralen Komponenten des LEGIC Systems koordiniert und kosteneffizient abgelöst werden. Dies sind:

- Master-Tokens und Initialisierungsstationen
- LEGIC-Ausweise, Schlüsselanhänger, Tokens
- Leser (inkl. Applikationssoftware)

Die Komponenten werden typischerweise Schritt für Schritt migriert, um den reibungslosen Betrieb des Systems jederzeit gewährleisten zu können. Für die Reihenfolge der Migration gibt es unterschiedliche Modelle. Dabei müssen die folgenden Überlegungen angestellt werden:

- Wie kann die Sicherheit am schnellsten gewährleistet werden?
- Welches sind die technischen Möglichkeiten (ein LEGIC advant Leser kann LEGIC prime Transponder lesen, umgekehrt kann ein LEGIC prime Leser keine LEGIC advant Transponder lesen)?
- Welches ist die kosteneffizienteste Lösung?

Beispiel:

Die Migration kann in den folgenden 3 Stufen erfolgen:

- *Phase 1: Master-Token auf LEGIC advant umstellen*
- *Phase 2: Leser auf LEGIC advant umstellen*
- *Phase 3: Ausweise nach und nach auf LEGIC advant umstellen.*

Die *IDExpert*[®] Produkte unterstützen Sie optimal in den einzelnen Phasen dieser Migration.

Als LEGIC Partner beraten wir Sie gerne über die notwendigen Schritte, zugeschnitten auf Ihre individuellen Anforderungen und Ihre Systemkonfiguration.

Ihr Ansprechpartner:

Rudi Noé

Telefon: +49 (0)7243 5488 0
E-Mail: rnoe@vps.de

Unterstützung von LEGIC Hybrid-ausweisen

Unter einem LEGIC Hybridausweis versteht man einen Ausweis, der sowohl einen LEGIC prime Chip, als auch einen LEGIC advant Chip enthält.

vps entwickelt aktuell eine Lösung für die *IDExpert*[®] Produkte, welche die Personalisierung und Verwaltung solcher Hybrid-Ausweise einfach ermöglicht. Die Personalisierung dieser Ausweise erfolgt wie gewohnt in einem Arbeitsschritt.

Durch den Einsatz dieser Ausweise ist ein Mischbetrieb von LEGIC prime und LEGIC advant Lesern und Ausweisen, unter Berücksichtigung erhöhter Sicherheitsanforderungen, im Unternehmen möglich.

- *In den sicherheitsrelevanten Bereichen werden jeweils die LEGIC prime Leser durch LEGIC advant Leser ausgetauscht.*
- *Diese Leser werden so konfiguriert, dass nur LEGIC advant Transponder akzeptiert werden. Damit wird die Sicherheit speziell für diesen Bereich wesentlich erhöht.*
- *Nur bei den Personen, welche Zugang zu diesen Sicherheitsbereichen benötigen, werden die LEGIC prime Ausweise durch Hybrid-Ausweise ersetzt.*

Die Lösung ist ab Ende Februar 2010 in den *IDExpert*[®] Produkten verfügbar und wird neben anderen Produktneuigkeiten auf der CeBIT 2010 vorgestellt.

Besuchen Sie uns auf der....



CeBIT 2010
2. – 6. März 2010
Stand B25 Halle 11
Hannover



Identity Conference 2010
5. – 8. Mai 2010
München