

Fälschungssicherheit von elektronischen Ausweisen

Über die Jahre hinweg sind sehr unterschiedliche Typen von elektronischen Ausweisen entstanden. Die heute verbreiteten, berührungslosen Kartentypen können etwa wie folgt – nach ihrer Fälschungssicherheit – kategorisiert werden.

Ausweistypen ohne Verschlüsselung

UID (Unique Identifier):

Dieser Ausweistyp gibt lediglich eine von Hersteller eingetragene Nummer aus. Da dies ohne weitere Sicherungsverfahren geschieht, ist diese Nummer von jedem Leser ähnlicher Bauart auslesbar und kann mit frei verkäuflichen Karten-Emulatoren simuliert werden. Zu dieser Gruppe zählen die meisten Systeme im Bereich 125 kHz, also z. B. Hitag, EM, HID ... aber auch Mifare-Systeme (13.56MHz) werden oft in dieser Betriebsart verwendet.

EPROM-Daten:

Im Gegensatz zum UID-Typ dienen hier vom Anlagenhersteller bei der Kartenausgabe in den Speicher der Karte (EPROM) eingetragene Daten als Identifikationsmerkmal. Sofern hierbei ohne Verschlüsselung gearbeitet wird, ist dies der am leichtesten zu fälschende Ausweistyp. Bereits mit einem recht einfach aufgebauten Leser, kann eine vorhandene Karte ausgelesen und auf eine weitere Karte des gleichen Typs geschrieben werden. In diese Gruppe fallen viele Mifare-Systeme, die die gleiche Karte für unterschiedliche Anwendungen (Zutritt, Gleitzeit, Kantine) nutzen.

Ausweistypen mit unzureichender Verschlüsselung

EPROM-Daten mit Anlagenschlüssel:

Dieses Verfahren ist eine Variante der EPROM-Karten. Hierbei werden ein oder mehrere Anlagenschlüssel erzeugt, die bei der Initialisierung (beim „Taufen“) auf die Karte aufgebracht werden. Dort dienen sie, möglichst gut gegen Auslesen geschützt, als Schlüssel zum Kryptieren der Datenübertragung. Typische und weitverbreitete Vertreter dieser Gattung sind Mifare (-Classic) und Legic.

In der Vergangenheit galten diese Systeme als ausreichend sicher. Neure Untersuchungen haben jedoch gezeigt, dass die Implementierung der zugehörigen Krypto-Algorithmen anfällig für spezialisierte Angriffe ist, die nunmehr publiziert sind. Seitdem müssen insbesondere Mifare (-Classic)- Karten und Legic- Karten trotz eingesetzter Verschlüsselung als unsicher gelten.

Ein weiterer Unsicherheitsfaktor ergibt sich aus der Tatsache, dass bei diesem Verfahren nur ein einziger Schlüssel für alle Karten existiert. Ein potentieller Angreifer muss dann nur die Schlüssel einer einzigen Karte knacken, um alle anderen Karten kopieren/fälschen zu können. Wenn, wie vielfach üblich, die Schlüssel in den Lesern gespeichert werden und nicht im Hintergrundsystem, ergeben sich weitere Angriffspunkte auf die Systemsicherheit.

Ausweistypen mit Authentisierung (Echtheitsprüfung)

Die Fälschungssicherheit eines elektronischen Ausweises, lässt sich durch den Einsatz von Prozessorchipkarten in Verbindung mit verbesserten Verschlüsselungsverfahren und vor allem für jede Karte separaten Schlüsseln, deutlich erhöhen.

Prozessorchipkarten:

Hier werden Karten mit eigenen CPUs eingesetzt, die nicht nur ausreichend Rechenleistung bereitstellen, sondern meist auch viel mehr flexibel einsetzbaren Speicherplatz bieten. Die erhöhte Rechenleistung ermöglicht unter anderem den Einsatz von Krypto-Verfahren, die in Fachkreisen allgemein als ausreichend sicher eingeschätzt werden. Hierzu zählen das altbewährte DES (Data Encryption Standard) sowie 3 DES und das deutlich neuere AES (Advanced Encryption Standard).

Prozessorchipkarten die auf diesen sichern Verschlüsselungsverfahren aufbauen, sind etwa die Telesec TCOS –Karte und die Mifare DESFire EV 1. Die Telesec TCOS -Karte ist von unabhängigen Instituten (z.B BSI) mit aufwendigen Verfahren auf die Stärke ihrer Sicherheitsmechanismen und Überwindungssicherheit überprüft. Daraus ergibt sich eine weltweit akzeptierte Einstufung auf einer absoluten Skala gemäß den sogenannten „Common Criteria“, z.B. „E4/Hoch“ für das Zertifikat der TCOS-Karte des Hersteller Telesec. Damit bietet die Telesec TCOS- Karte unter der Verwendung von DES/3DES eine verbürgte Sicherheit. Die Mifare DESFire EV 1 -Karte bietet unter Verwendung, der vom BSI empfohlenen bzw. für Neuanlagen geforderten AES Verschlüsselung, bei Authentisierung eine mindestens gleichwertige Fälschungssicherheit. Dieser Sicherheitsmechanismus beruht auf einer jeder Karte eigenen Schlüssel, der mit einer Zufallszahl überprüft wird. Dazu muss im Hintergrundsystem (Auswerteeinheit) eine Kopie des Schlüssels jeder einzelnen Karte aufbewahrt werden. Das Verfahren wird auf der folgenden Seite detailliert dargestellt.

Elektronische Ausweise

Der Authentisierungsmechanismus erfordert jedoch ein geeignetes Hintergrundsystem, das nicht nur die gleichen Krypto-Operationen wie die Karte ausführen kann, sondern die Kartenschlüssel auch sicher verwaltet. Darüber hinaus werden für diese Kartentypen spezielle Leser erforderlich, die transparent Daten von der Auswerteeinheit zur Karte und zurück übertragen können. Seit einiger Zeit wird hier das Zutrittssystem cryptin der Firma Cichon und Stolberg angeboten, das als einziges Gesamtsystem vom BSI geprüft ist. Das System umfasst sichere Server, hochsichere Auswerteeinheiten, geeignete Kartenleser und eben Prozessorchipkarten mit einem Höchstmaß an Fälschungssicherheit.

Authentisierung

Fälschungssicherung der Karte: Authentisierung

Bei Verwendung einer entsprechend leistungsfähigen Chipkarte kann, zusätzlich zur Berechtigungsprüfung, eine Fälschungsprüfung der Karte durchgeführt werden. Dann laufen bei jedem Zutritt folgende Schritte ab:

1. Wenn eine Karte vor den Leser gehalten wird, sendet der Leser die Kartenummer zur Auswerteeinheit (ZKZ, Zutrittskontrollzentrale).
2. Die ZKZ prüft die Berechtigung. Wenn die Karte eine Berechtigung zum Öffnen der Tür hat, wird eine Zufallszahl ausgeknobelt und zur Karte geschickt.
3. Die Karte verschlüsselt nun diese Zufallszahl mit ihrem internen, von außen nicht lesbaren Schlüssel. Dieser Schlüssel wird der Karte bei der Produktion mitgegeben, er kann weder gelesen noch geändert werden. Bei zertifizierten Karten ist die Sicherheit der Daten vom Zertifizierer (z.B. BSI) verbürgt, ansonsten muss man sich auf den Hersteller verlassen.
4. Das dabei entstandene Chifftrat wird zurück zur ACU geschickt.
5. Die ACU hat den Kartenschlüssel auch gespeichert und kann damit nun die verschlüsselte Zufallszahl wieder entschlüsseln.
6. Das Chifftrat wird nun geprüft: Wenn die Entschlüsselung wieder die Zufallszahl ergibt, die ursprünglich zur Karte gesendet wurde, ist die Karte nicht gefälscht. Ansonsten handelt es sich um eine Fälschung, da die Karte den falschen Schlüssel benutzt hat.
7. Wenn die Karte OK ist, kann schließlich die Tür geöffnet werden. Der gesamte Vorgang hat bis hierhin etwa 0,2 sec gedauert.
8. Die Sicherheit der Fälschungsprüfung hängt, neben einer sauberen Implementierung, vor allem vom eingesetzten Verschlüsselungsverfahren ab. Hier hat sich DES/3DES über viele Jahre bewährt, in letzter Zeit kommt auch AES immer häufiger zum Einsatz.

