PrehKeyTec

Argumente für PrehKeyTec's Verschlüsselungs – Technologie

- PrehKeyTec bietet eine Verschlüsselung von Kartendaten wie sie von Payment Card Industry Data Security Standard (PCI DSS) gefordert und von Visas (Payment Application Best Practices) PABP empfohlen wird. Zusätzlich zu der Möglichkeit Kartendaten die vom internen Magnetkartenleser der Tastaturen gelesen werden zu verschlüsseln, ist es ebenfalls möglich numerische Tastatureingaben, für die so genannte „card not present transactions", zu verschlüsseln. Diese Lösung sichert und verschlüsselt alle finanziellen Transaktionen direkt bei der Eingabe. Die Daten sind von dem Punkt an dem sie die Tastatur verlassen und durchs Kabel zum Host-Computer übertragen werden verschlüsselt und können so öffentlich übertragen werden, wie es die PCI DSS Punkt 3.4 fordert.

- Damit ist diese Eingabeeinheit für Client Server Systeme, Systeme mit erhöhten Anforderungen oder Systemen an deren Software nichts geändert werden soll prädestiniert. Durch diese fortgeschrittene Technologie und Intelligenz der MCI-Serie kann PrehKeyTec zwei unterschiedliche Verschlüsselungsalgorithmen auf Basis von AES und ARCFOUR anbieten. Beide Algorithmen verwenden eine mehr als für hohe Sicherheit benötigte Schlüssellänge von 256bit. Dies ermöglicht eine einfachere Zertifizierung nach PCI.

- Die Verschlüsselung kann individuell angepasst werden und erlaubt es bei Bedarf, einige Kartendaten unverschlüsselt zu versenden. Die Verschlüsselung kann optional die Daten wie „Issuer Identification Number (IIN)", NAME, etc. in Klartext übertragen, um Belege zu drucken oder zur Abwicklung der Übertragung. Außerdem kann die Verschlüsselung für verschiedene Karten, wie Kreditkarten, Bankkarten oder Bonuskarten individuell angepasst oder abgeschaltet werden.

- Die AES Verschlüsselung basiert auf einem 256bit langen Schlüssel zusammen mit einer optionalen Transaktions-ID, welche so genannten „man-in-the-middle" Attacken vorbeugt. Bei AES werden alle Daten der Spur2 einer Kreditkarte verschlüsselt.

- Die ARCFOUR Lösung besteht aus zwei 256bit Schlüsseln pro Übertragung. Die Firmware der Tastatur beinhaltet eine Ansammlung von 16000 Schlüsseln, jeder mit 256bit Länge, welche wahllos verteilt sind. Für jede Transaktion wird ein 256bit Schlüssel zufällig ausgewählt und mit dem vom Kunden gewählten 256bit Schlüssel kombiniert. Die Tastaturelektronik, kombiniert mit dem schnellen und einfachen ARCFOUR Algorithmus, erlaubt die komplexe Verschlüsselung von Bankkarten-Daten um eine hohe Sicherheit zu gewähren. PrehKeyTecs ARCFOUR Lösung verschlüsselt alle Daten auf Bankkarten (Spur 1, 2, 3). Durch optionale Konfiguration kann sie zusätzliche sensitive Daten, wie z.B. Passwörter und Sozialversicherungsnummern, verschlüsseln und sicher Übertragen.

- Mit dem Softwaretool WinProgrammer (verfügbar auf der PrehKeyTec Internetseite), können System-Integratoren und Administratoren einfach die eigenen 256bit Schlüssel in der Tastatur speichern. Außerdem lässt sich mit der Software auch das Tastenlayout und die Programmierung der Tastatur je nach Kundenwunsch anpassen. Header und Terminator für die MSR-Übertragung lassen sich, genauso wie für die so genannte „card not present transactions“, ebenfalls darüber einbinden.

- Grundsätzlich gibt es kein Limit bei der Schlüsselsequenz. PrehKeyTec empfiehlt einen regelmäßigen Austausch der Schlüssel um die Sicherheit des Systems auf höchster Ebene zu halten. Gegenwärtig bietet PrehKeyTec die Verwaltung von bis zu 5 verschiedenen 256bit Schlüsseln an, die für verschiedene Karten oder Tastatureingaben benutzt werden können.

- Der WinProgrammer bietet darüber hinaus dem Integrator die Möglichkeit die LED für unterschiedliche Situationen zu setzen, wie die Bestätigung für einen Kartendurchzug, z.B. gut gelesen grüne LED blinkt und schlecht gelesen rote LED leuchtet. Ein zusätzlicher Buzzer in der Tastatur liefert Tonfolgen beim Kartendurchzug oder Tastendruck. Beides zusammen gibt der Verschlüsselungslösung die Möglichkeit der akustischen und visuellen Rückmeldung.

- PrehKeyTec bietet eine API für die einfache Entschlüsselung in der Abwicklung an. Bei Bedarf ist PrehKeyTec auch bereit den Sourcecode mit Beispielen zur Entschlüsselung zur Verfügung zu stellen. Für die individuelle Anpassung der Verschlüsselungsausgabe stellt PrehKeyTec einen Simulator zur Verfügung, mit dem die Verschlüsselung unter verschiedenen Gesichtspunkten getestet werden kann.

- Eine zusätzliche API steht bereit, die der Systemintegrator in seine Software einbinden kann, um damit direkt mit der Tastatur zu kommunizieren. Diese API ist immer dann sehr nützlich, wenn der Kunde die Verschlüsselung von seiner Software aus starten will, ohne Erfordernis eines Tastendrucks vom Bediener. Die Flexibilität der Tastatur erlaubt das duale Arbeiten, Eingabe von Verschlüsselten Informationen für sensitive Übertragungen und Standard Eingabe, wenn die eingegebene Nummer nicht verschlüsselt werden muss. Entscheidet sich ein Kunde die Tastatur nur für die Eingabe von verschlüsselten Übermittlungen zu verwenden und für nichts sonst, ist es ebenfalls möglich die Tastatur in dieser Art zu konfigurieren.

- Weil die verschlüsselten Informationen, die direkt aus der Tastatur kommen, über ein Netzwerk zu einem Rechenzentrum zur die Entschlüsselung geschickt werden kann, ist das Produkt in der speziellen Situation, das POS Terminal aus dem Bereich der PCI DSS zu nehmen. Dies reduziert das enorme Risiko und die Kosten die bei der Verarbeitung von Bezahldaten und generellen Handhabung von Kartendaten auftreten.

PrehKeyTec GmbH, Scheinbergweg 10, 97638 Mellrichstadt; Tel: +49 9776 7046 - 0