

### **Name des Projekts:**

Sicherheitsuntersuchung eines Sicherheitsmoduls (Sicherheitsbox) unter Verwendung der Sicherheitsanforderungen der deutschen Kreditwirtschaft (ZKA) im Auftrag eines europäischen electronic cash Netzbetreibers.

### **Aufgabe:**

Die Zulassung einer neuen oder geänderten Sicherheitsbox zum Einsatz in einem deutschen electronic cash-Netz setzt voraus, dass dem Zentralen Kreditausschuss der deutschen Kreditwirtschaft (ZKA) Sicherheitsgutachten der Hardware und Software der Sicherheits-Box vorgelegt werden. Das Sicherheitsgutachten muss unter anderem nachweisen, dass PIN und kryptographische Schlüssel des Zahlungssystems electronic cash darin sicher gehandhabt werden.

### **Lösung:**

SRC hat im Auftrag eines europäischen Netzbetreibers die Software der Sicherheitsbox zum Nachweis der Sicherheitsanforderungen der deutschen Kreditwirtschaft untersucht.

Die Sicherheitsuntersuchung wurde in Form eines ‚White-Box-Tests‘ durchgeführt. Dabei wurde die Sicherheitsfunktionalität anhand des Quellcodes und der zugrundeliegenden Designdokumente geprüft. Die Sicherheitsuntersuchung fand in den Räumen von des Herstellers der Sicherheitsbox statt.

Ziel der Sicherheitsuntersuchung war der Nachweis,

- dass das zugrundeliegende Sicherheitskonzept für das electronic cash Netz, das von Beratern der SRC erstellt wurde, von der Software der Sicherheitsbox korrekt umgesetzt wird,
- dass die Trennung der Applikationen sicher in der Sicherheitsbox realisiert ist und
- dass die Software keine Schwachstellen enthält, die es zulassen würden, PINs oder kryptographische Schlüssel zu kompromittieren.

Die Vorgehensweise bei der Sicherheitsuntersuchung ist vergleichbar mit der Methode zur Durchführung einer Schwachstellenanalyse in ISO/IEC 17025 Common Criteria. Das bedeutet, dass nach gewonnenem Verständnis des Designs und der Implementierung gezielt nach Schwachstellen gesucht wird.

Die Sicherheitsuntersuchung gliederte sich in verschiedene Schritte:

- Prüfung des Designs des Betriebssystems der Sicherheitsbox und Analyse des entsprechenden Quellcodes im Einzelschrittverfahren
- Prüfung des Design der relevanten Applikation der Sicherheitsbox unter Verwendung der Sicherheitskonzepts für electronic cash und Analyse des Quellcodes im Einzelschrittverfahren
- Erstellung und Vorstellung des Berichts beim Arbeitsstab „Sicherheit“ des ZKA.

### **Erfolgsfaktoren:**

Kritisch für den erfolgreichen Abschluss des Projekts waren die Kompetenzen von SRC in den Bereichen:

- Detaillierte Kenntnisse des Zahlungssystems electronic cash, insbesondere auch der technischen Schnittstellenspezifikationen und des Sicherheitskonzepts
- Umfangreiche Erfahrungen in den Bereichen
  - der Analyse von Design und Quellcode von Sicherheitsmodulen,
  - der Durchführung von Sicherheitsanalysen und –evaluationen, insbesondere auch nach den internationalen Standard Common Criteria und
  - der internationalen Zusammenarbeit mit ausländischen Kunden.
- Projektleitung und Koordination aller beteiligten Parteien
  - dem Hersteller der Sicherheitsbox,
  - dem electronic cash-Netzbetreiber und
  - der deutschen Kreditwirtschaft als Zulassungsstelle.

### **Umfang des Projekts:**

Der Umfang des Projekts betrug ca. 20 Personentage.

### **Gesamtdauer:**

Die Dauer des Projekts betrug ca. 2 Monate.