

SRQ-ID: 0867

**Betrifft (wird vom FLS (optional vom Erfasser) ausgefüllt):**

Themenkreis	Dezentrale Komponenten
Schlagwort	Kartenterminalidentität, Entnahme SK-KT
zu Dokument / Datei	gemSpec_KT
Version	2.6.0
Bezug (Kap., Abschnitt, Tab., Abb.)	3.7

**Stichwort: Kartenterminalidentität, Entnahme SK-KT**

**Frage:**

Welche Vorgaben gibt es Bezüglich einer Entnahme des SM-KT im laufenden Betrieb?

**Betrifft (wird vom PB ausgefüllt):**

Gültig ab Release	0.5.2	Verbindlichkeit	
zusätzlicher Download-Link zu Datei:			
Herstellerbefragung durchgeführt		am	
Wird behoben mit Version	2.6.2	voraussichtl. Zeitpunkt	19.09.08
Anmerkungen:			
Status	<input checked="" type="checkbox"/> erfasst <input type="checkbox"/> intern abgestimmt <input type="checkbox"/> extern abgestimmt <input type="checkbox"/> zurückgezogen <input type="checkbox"/> freigegeben <input type="checkbox"/> eingearbeitet in Folgeversion		

**Antwort:** Die Festlegungen zur Entnahme des SM-KT im laufenden Betrieb sind in Kapitel 3.7 ergänzt.

## 3.7 Festlegungen zur Kartenterminalidentität und Schlüsselmanagement

~~Ein fortgeführter Betrieb der SICCT-spezifischen TLS-Verbindung ohne vorhandenen Sicherheitsanker in Form der SM-KT DARF NICHT möglich sein.~~

Es MUSS nachgewiesen werden, dass bei einer Entnahme des SM-KT, während eine TLS-Verbindung besteht, die unter Verwendung des entnommenen SM-KT aufgebaut wurde, keine zusätzliche Bedrohung zum Fall einer Entnahme des SM-KT ohne eine solche bestehende TLS-Verbindung entsteht.

Beispielsweise KANN dies umgesetzt werden, indem das Kartenterminal bei Entnahme des SM-KT eventuell aktive TLS-Verbindungen, die die korrespondierende SMKT-Identität zum Betreiben des TLS-Kanals nutzen, aktiv beendet. Dies kann bei Entnahme des SM-KT durch folgende Maßnahmen erreicht werden: aktive Maßnahmen, wie direkte Erkennung der Kartenentnahme oder regelmäßigem Pollen der Karte mit anschließend gezieltem Kanalabbau bei fehlender Karte. ~~Bei regelmäßigem Polling DARF das Pollingintervall NICHT mehr als 5 Sekunden betragen.~~

- passive Maßnahmen, bei denen die SM-KT nur in einem Zustand des Geräts gesteckt oder entfernt werden kann, während dem keine TLS-Verbindung **unter Verwendung des SM-KT** möglich ist (z. B. Zugang zum SM-KT Kartenschacht nur nach Entfernen der LAN- und Powerkabel möglich)