

eHealth 2005

Workshop 2 – Infrastruktur und Dienste

Das Card Application Management System (CAMS)

als zentrale Komponente der elektronischen Gesundheitskarte
mit digitaler Signatur

20. April 2005, Werner Bschorr



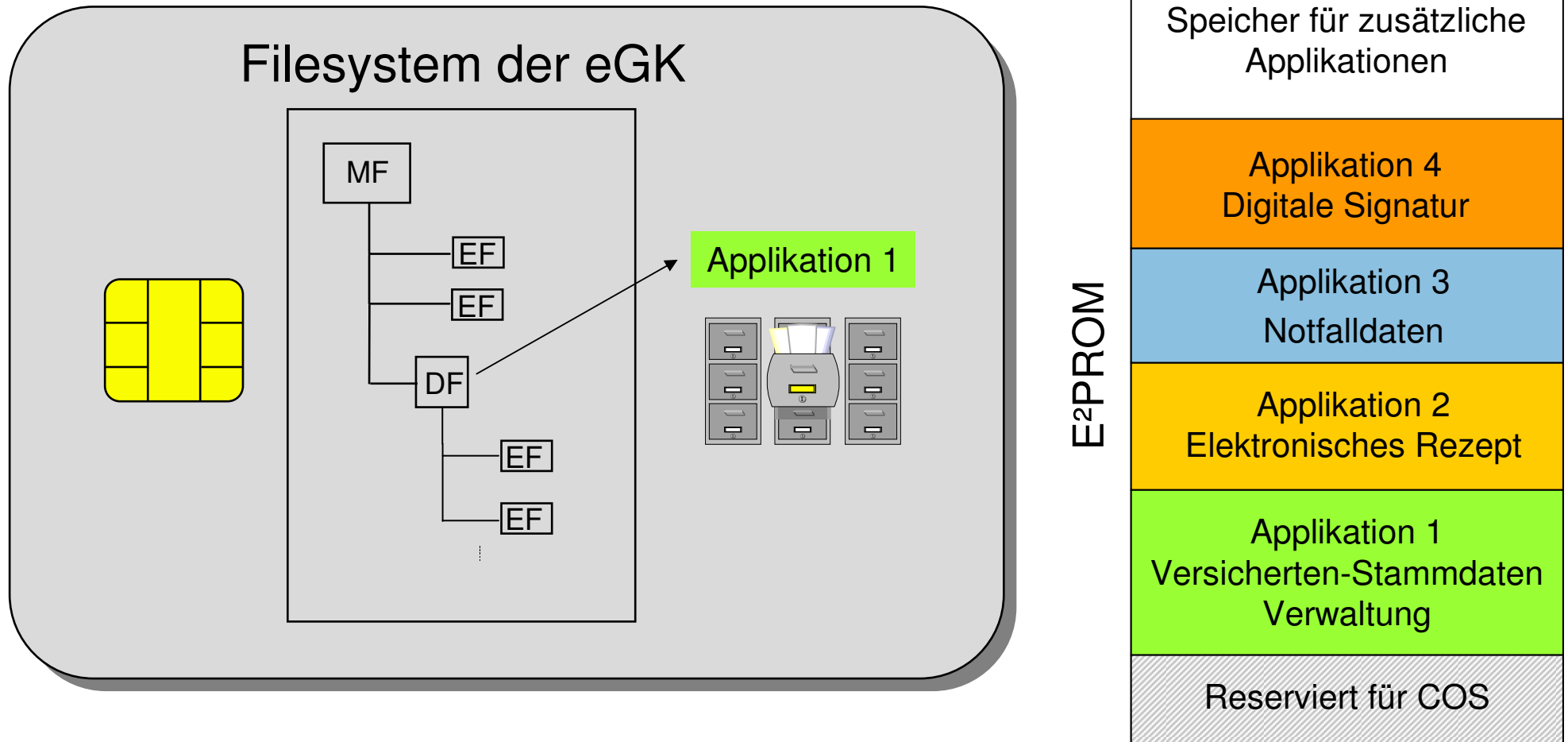
Giesecke & Devrient

Inhalt

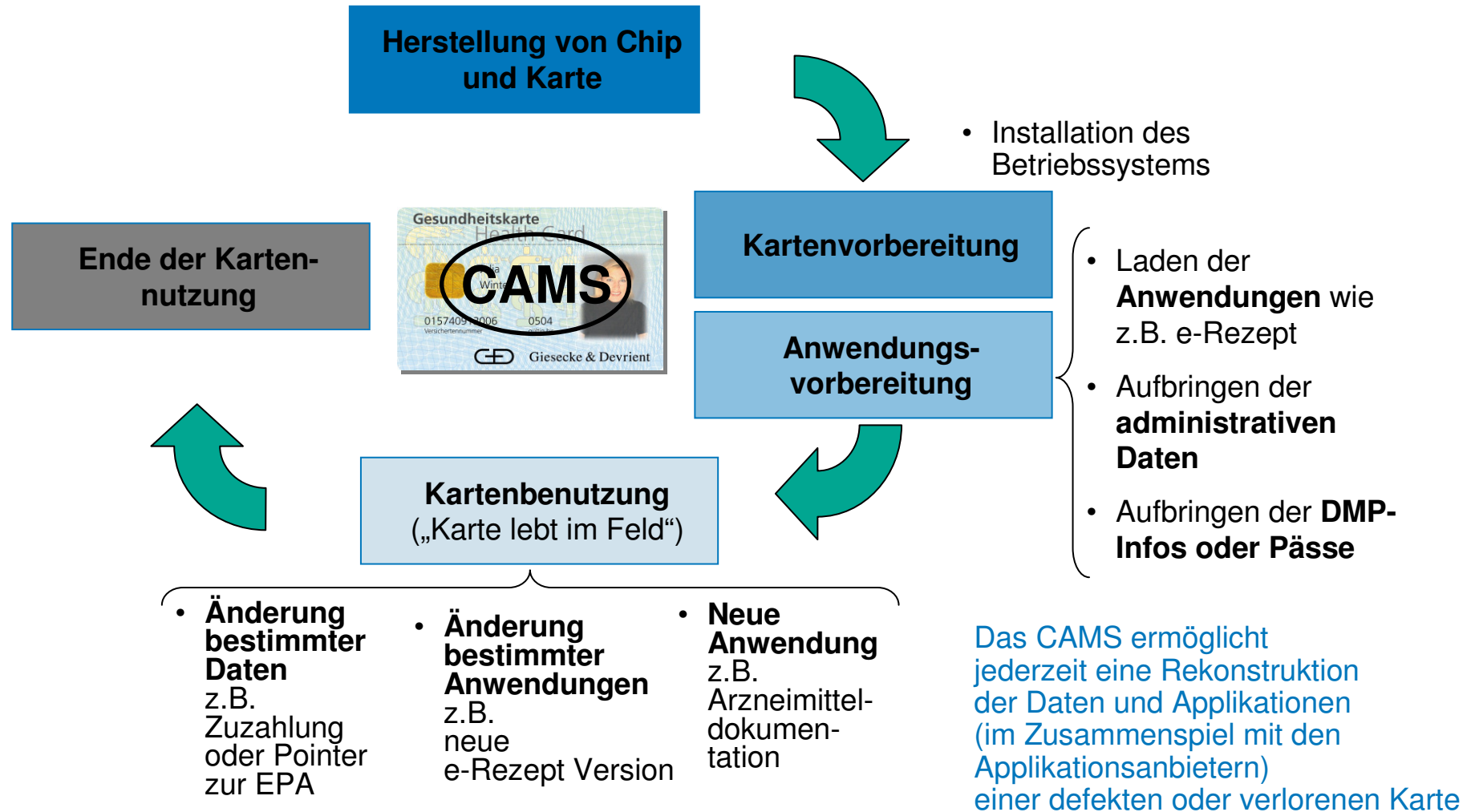
- Aufbau eines multiapplikativen Chipkarten-Betriebssystems
- Karten- und Applikationsverwaltung mit einem Card Application Management System (CAMS)
- Nachladbarkeit von Applikationen im Feld am Beispiel der digitalen Signatur
 - Beantragung eines neuen PKI-Zertifikats
 - Vorbereitung der eGK zum Aufbringen der digitalen Signatur

Aufbau eines multiapplikativen Chipkarten-Betriebssystems

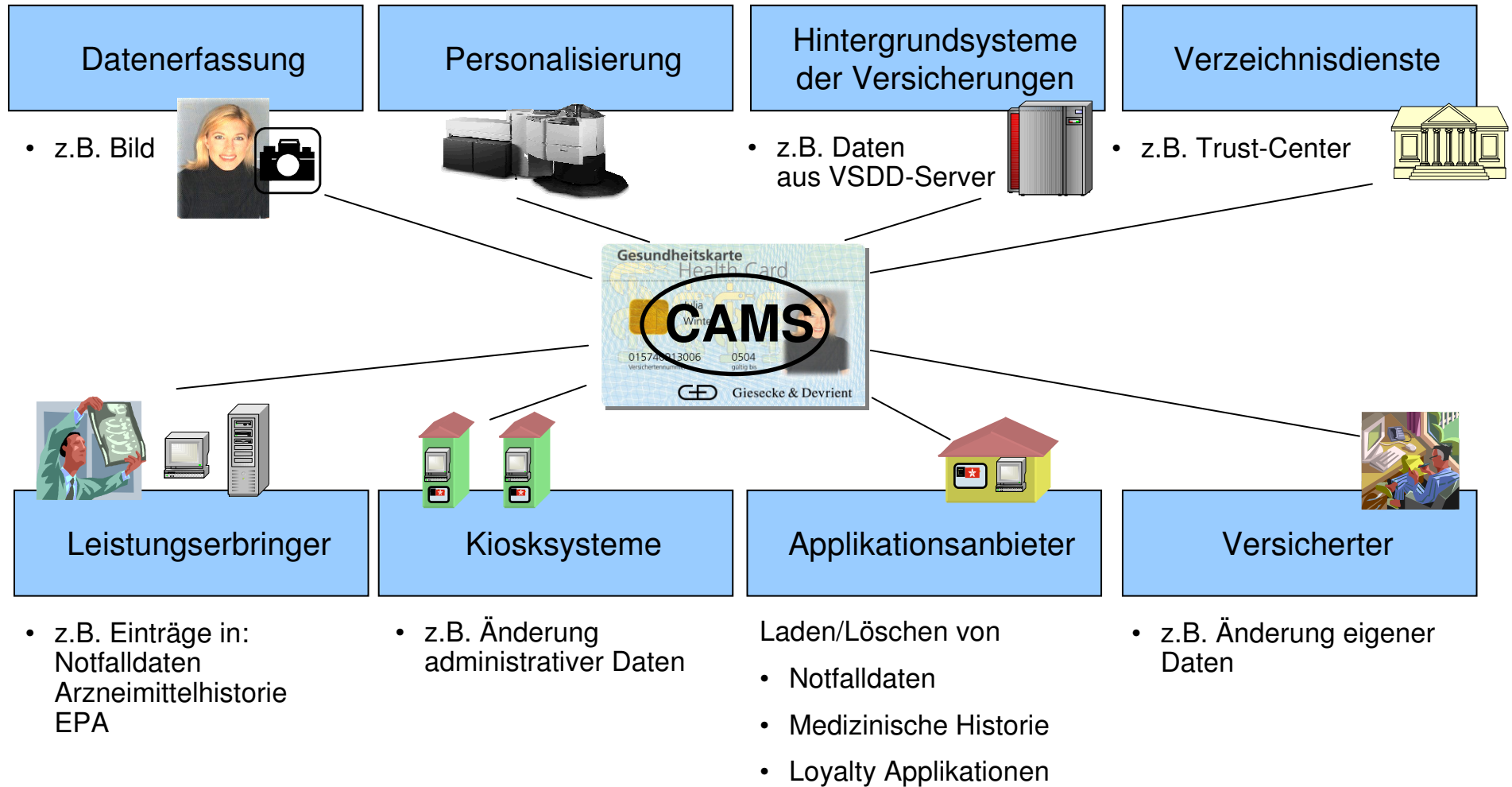
- Das Chipkarten-Betriebssystem steuert mit Hilfe des Filesystems sämtliche Zugriffsberechtigungen auf die verschiedenen Anwendungen der Karte



Karten- und Applikationsverwaltung mit einem CAMS-System



Das CAMS als zentrale Komponente während der Kartennutzung



Nachladbarkeit von Applikationen im Feld

Das CAMS bietet eine Schnittstelle zum Nachladen von Applikationen auf die Chipkarte

Folgende Sicherheitsfeatures werden dabei unterstützt

- Aufbau eines geschützten Kanals zwischen CAMS und eGK für eine sichere Datenübertragung.
- Zusätzliche Berechtigungsschlüssel zum Schutz vor unbefugtem Zugriff oder Manipulationen auf der eGK.

➔ Somit ist es nicht möglich Viren, Trojaner usw. auf die Karte zu übertragen.

Kundencenter

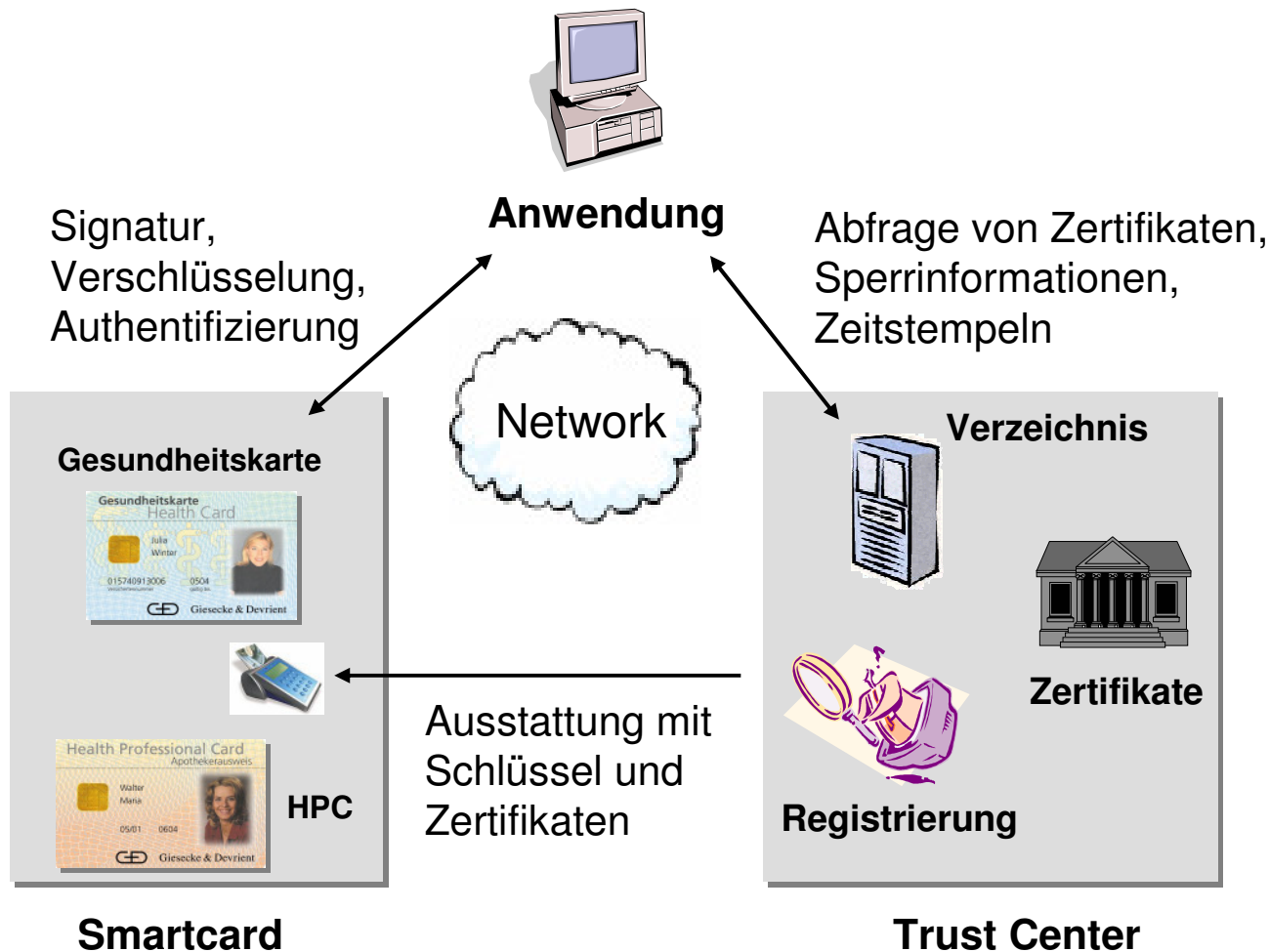
KARTEN- UND APPLIKATIONSVERWALTUNG

	geladen	aktiv	gesperrt	32 kB	64 kB	
Versicherten-Daten	■	■	■	■	■	100 % STARCOS 3.0
eRezept	■	■	■	■	■	
Notfall-Daten	■	■	■	■	■	
Elektronischer Arztbrief	■	■	■	■	■	50 %
Arzneimittel-Dokumentation	■	■	■	■	■	
Elektronische Patientenakte	■	■	■	■	■	
Digitale Signatur	■	■	■	■	■	0 %

Daten übertragen Daten werden übertragen **Daten wurden erfolgreich übertragen**

[Zum Inhalt](#) [Logout](#) Giesecke & Devrient

Komponenten einer PKI-Anwendung



Eine PKI-Anwendung benötigt:

1. eGK als sicheren Träger für den Private Key
2. Trustcenter für die Erstellung und Verteilung der Zertifikate

Vorbereitung der eGK zum Aufbringen einer elektronischen Signatur

Zur Vereinfachung der Nachladbarkeit der elektronischen Signatur im Feld empfiehlt sich bei der Erstausgabe der eGK folgende Vorgehensweise:

- Anlegen eines Verzeichnisses für die Signaturapplikation auf der eGK
 - Definition der Zugriffsregeln für dieses Verzeichnis
 - Anlegen von Administrationsschlüssel innerhalb dieses Verzeichnisses
- Die vorbereitenden Maßnahmen werden mit dem CAMS administriert.
- Danach kann die Signaturapplikation jederzeit mit Hilfe des CAMS in Zusammenarbeit mit einem Trustcenter auf der eGK aktiviert werden.