Remote Management Interface (RMI) mit SMC-B PIN-Funktion

Was ist eigentlich ein Remote Management Interface?

Healthcare

Eine 2. Datenschnittstelle mit einem gesicherten parallelen Zugang zur Konfiguration & Wartung des Kartenterminals

1. **Interface = Schnittstelle**

   Zusätzliche 2. Management-Schnittstelle, über die sehr viele Informationen, Einstellungen und Befehle des Kartenterminal von einem anderen Daten-Verarbeitungs-System übertragen werden können. (1. Ma-Schnittstelle des KTs: Display und Tastatur)

2. **Management**

   Management bezeichnet im Zusammenhang mit dem Wort Interface eine Schnittstelle, mit der etwas überwacht, konfiguriert und verwaltet werden kann.

3. **Remote (Service)**

   Ist ein Verfahren, über das technische Dienstleistungen mit Hilfe von Telekommunikationsnetzwerken an einem entfernten Ort erbracht werden.

4. **Gesicherter Zugang über LAN**

   Parallel zur SICCT Kommunikation mit dem Konnektor in der TI-Infrastruktur wurde eine mit dem Secure Websocket Protokoll abgesicherter 2. Zugang implementiert.

WORLDLINE

Welche Hauptfunktionen stehen über RMI zur Verfügung?

Healthcare

Alle wesentlichen Funktionen des Terminals können jetzt auch aus der Ferne durchgeführt werden

1. **Einstellungen** vornehmen
   - Vollumfängliche Einstellung des Kartenterminals so, wie man es heute auch über das Display und die Tastatur am Kartenterminal umsetzen kann.
   - LAN / SICCT-Protokoll zwischen KT und Konnektor / VPN / Zeiteinstellung / Display / Töne / Kiosk Modus
2. **Services** ausführen
   - **Direktes Firmware-Update**
   - **Remote SMC-B PIN Feature**
   - **Serien-Nr. gesteuerte Vorkonfiguration über die API**
   - Passwort Änderung für folgende Benutzer: Remote Admin / SICCT Admin / PIN-Provider
3. **Informationen** anzeigen
   - Geräte / Kartenslots / Status der gSMC-KT / Netzwerk / VPN / **Betriebsdaten / Statistik**
     → jetzt übersichtlich in Tabellenform einsehbar

Einstellungen
Datenfelder, die gelesen und verändert werden können.
SICCT Terminal Name: ORGA6100-0141..
Host Name: ORGA6100-Praxis-Müller

Services
ausführbare Funktionen
→ **Zukünftig ausbaubar mit weiteren Anwendungsfällen**

RMI Modul-Funktionen
→ Rechtemanagement
→ Sichere Prozessablauf

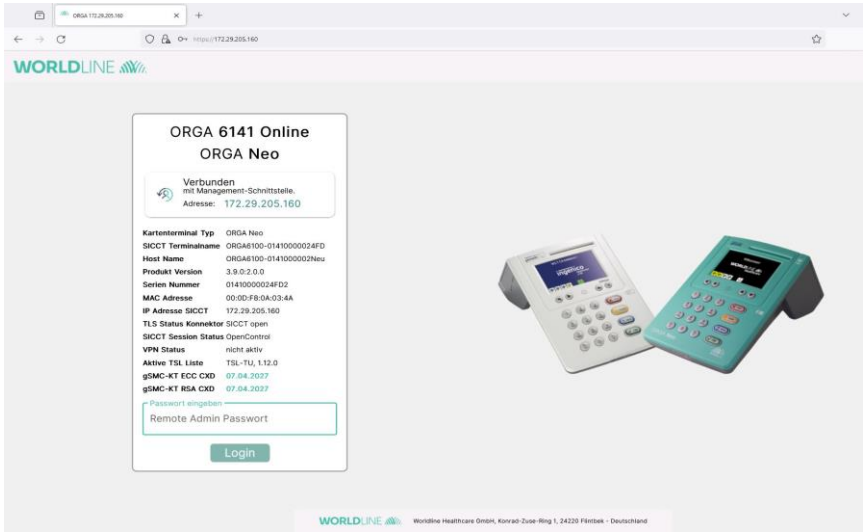
Informationen
Datenfelder, die nur gelesen werden können.
Serien Nummer: 01410000024FD2
Firmware Version: 3.9.0

Was ist die Web-Applikation zum RMI?

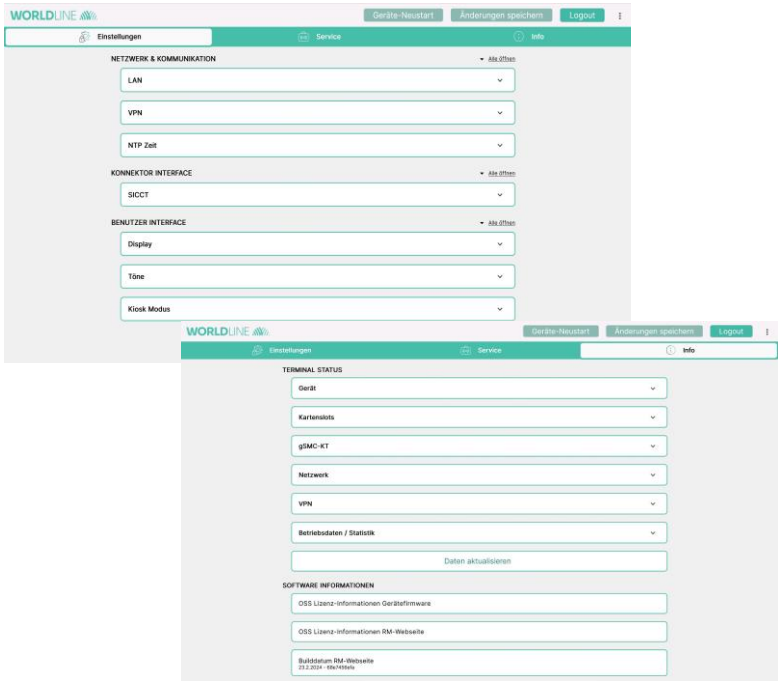
Healthcare

Eine Browser-Anwendung, mit der alle Funktionen an dieser Schnittstelle ausgeführt werden können.

- Wir bieten als Teil ab der FW 3.9.0 eine integrierte Web-Anwendung an, die genau auf den Leistungsumfang der Schnittstelle “zugeschnitten” ist.
- Auf der Startseite werden schon erste wichtige Information angezeigt.



- In den drei Reitern **Einstellungen**, **Services** und **Info** sind alle wesentlichen Informationen und Einstellparameter übersichtlich in Ausklappfenstern angeordnet.



Was ist ein Remote SMC-B PIN Feature?

Healthcare

Freischalten der Praxiskarte (SMC-B) aus der Ferne

1. **Was ist der Use Case?**

   Viele Funktionen (z.B. das Ausstellen eines Rezeptes) benötigen die Freigabe durch eine Praxiskarte (SMC-B) oder auch durch einen elektronischer Heilberufe Ausweis (eHBA)

2. **Was ist das Problem?**

   Wenn es zu Störungen in der Verbindung zwischen Terminal und Konnektor kommt, kann die Verbindung zwischen beiden unterbrochen werden.

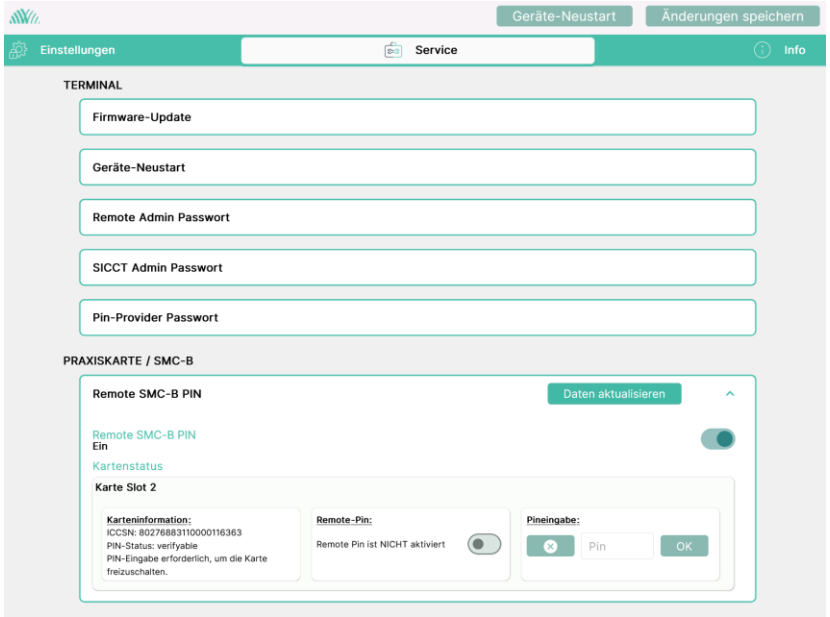
3. **Was ist die Folge?**

   Das Kartenterminal meldet sich beim Konnektor, damit der Konnektor dann eine neue Verbindung aufbauen kann. Das funktioniert automatisch, wenn sich beide Geräte grundsätzlich kennen, also gepairt sind.

   Sind in einem Terminal auch noch Praxiskarten (SMC-B) gesteckt, so müssen die PINs dieser Karten zur Aktivierung bisher lokal am Terminal eingegeben und bestätigt werden.

4. **Die Lösung: Remote SMC-B PIN Service**

   Aus der Ferne wird dieser Freischaltprozess von einer berechtigten Instanz gestartet und im Zusammenspiel mit dem Konnektor werden die PINs remote eingegeben und bestätigt**.**



WORLDLINE

Wie flexible können Kartenterminal & RMI angebunden werden?

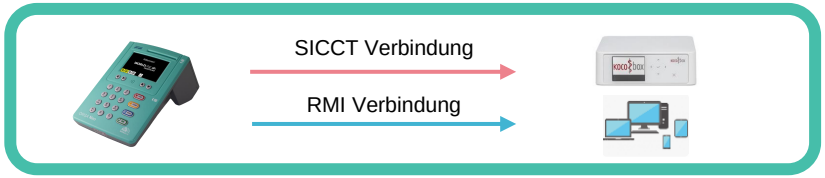
Healthcare

3 Verbindungen pro Benutzerrolle und parallel ansteuerbar über eine VPN-Verbindung sowie eine

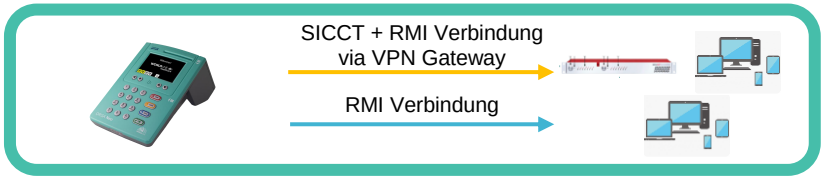
Benutzerrollen und Flexibilitätsgrad:

- Es sind für das RMI 3 neue Benutzerrollen definiert worden: **RMI-Administrator / SMC-B PIN Provider / Anonymous**
- Je Benutzerrolle dürfen sich max. 3 Benutzer gleichzeitig auf das RMI einbuchen.
  → Es werden also insgesamt max. 9 gesicherte Verbindungen zum RMI zugelassen.
- Bei einer bestehenden VPN-Verbindung steht das RMI im Remote Netzwerk sowie weiterhin im lokalen Netzwerk zur Verfügung
- Der lokale Admin Zugriff am Gerät ist darüber hinaus jederzeit möglich. Ein Hinweis zeigt einen bestehenden remote Zugriff an.

1. **Beispiel (Status Quo TI 1.0)**
   - 1x SICCT Verbindung zum Konnektor
   - max. 3x HTTPS/Secure Websocket Verbindungen je Benutzerrolle zum RMI über ein lokales Netzwerk



2. **Beispiel (TI 1.x mit HSK - Konnektoren)**
   - 1x SICCT Verbindung zum HSK-Konnektor via VPN-Gateway
   - z. B. 2x HTTPS/Secure Websocket Verbindungen je Benutzerrolle zum RMI via VPN-Verbindung
   - z.B. 1x HTTPS/Secure Websocket Verbindungen je Benutzerrolle zum RMI über ein lokales Netzwerk



. … und weitere mehr

Was gibt es noch Neues in der FW3.9.0?

Healthcare

Professionalisierung der heutigen TI-Infrastruktur und die „Tür“ zu weiteren neue Anwendungen

1. **Auswahl von 2 Authentisierungsmethoden zur Absicherung der Web-Socket Verbindung**
   - Auswahl der serverseitigen Authentisierung mit Hilfe der TLS-Extension "Server Name Indication" (SNI - RFC 6066 Kapitel 3)
     → Auf dem Terminal generiertes, selbst signiertes Authentisierungszertifikat (Default), basierend auf ECC NIST Kurven.
     → ECC Authentisierungszertifikat einer gSMC-KT G2.1 basierend auf ECC Brainpool Kurven.
     (Umsetzung über den SNI-HostName, der die ICCSN der gSMC-KT beinhalten muss)
       → abgesichert mit offiziellen Zertifikaten aus dem gematik Vertrauensraum der Telematik-Infrastruktur

2. **VPN - Ergänzung von 2 Authentifizierungs-Methoden und der erweiterten Parametrisierung des VPN-Clients**
   a. Ergänzung der IPSec VPN-Client Authentication-Methode **PSK (PreSharedKey)**
   b. Ergänzung der zertifikatsbasierenden Authentifizierungs-Methode **EAP-TLS** im IPSec VPN-Client

3. **Erweiterte Möglichkeiten zur Vorkonfiguration über die RMI-Schnittstelle oder den USB-Stick**
   - **Vorkonfigurationen** können jetzt im Verzeichnis **Seriennummer** oder **Root** angelegt und abgespeichert werde.
     → Damit können individuelle Konfigurationen je Terminal erstellt und ins Terminal übertragen werden
   - Applikation zeigt jeden verarbeiteten Parameter mit Ergebnis auf dem Display und erzeugt eine Log-Datei auf dem USB-Stick
     (Bei direkter Anbindung der Schnittstelle an ein Management-System werden die Ergebnisse zurückgemeldet und können kundenseitig abgespeichert werden.)

Healthcare

Vielen Dank für Ihre Aufmerksamkeit!

WORLDLINE