Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

Diese Änderungsmeldung enthält Anpassungen an der Spezifikation des Konnektors zum Remote Management.

Änderungsbedarf in gemSpec_Kon

4.3 Konnektormanagement

⌦ **TIP1-A_5005 Protokollierung in der Managementschnittstelle**

Jede Änderung, die ein Benutzer (Administrator) vornimmt, MUSS protokolliert werden durch TUC_KON_271 „Schreibe Protokolleintrag“ {„MGM/ADMINCHANGES“; Op; Info; „User=$AdminUsername; RefID=$ReferenzID; NewVal=$NeuEingestellterWert“}. Der hier geforderte Logging-Level gilt, wenn nicht an anderer Stelle eine abweichende Regelung spezifiziert ist.

Wenn die Änderung über ein Remote-Management-System durchgeführt wird, ohne dass ein Remote-Administrator im Konnektor konfiguriert ist, so MUSS als User eine Referenz auf das Remote-Management-System verwendet werden.

Passwörter DÜRFEN NICHT in den Protokolleinträgen geschrieben werden.⌫

4.3.1 Zugang und Benutzerverwaltung des Konnektormanagements

Der Konnektor verfügt über keine Verwaltung der fachlichen Nutzer, wohl aber über eine Verwaltung der Nutzer, die in der Rolle eines Administrators den Konnektor konfigurieren und die Protokolle einsehen dürfen. Dabei werden drei Administrator-Rollen unterschieden:

1. Lokaler-Administrator: zur Konfiguration des Konnektors über die lokale Managementschnittstelle
2. Remote-Administrator: zur Konfiguration des Konnektors über die remote Managementschnittstelle.
3. Super-Administrator: zur Verwaltung von Benutzerkonten und zur Konfiguration des Konnektors über die lokale Managementschnittstelle

⌦ **TIP1-A_4808 Zugangsschutz der Managementschnittstelle**

Der Konnektor MUSS sicherstellen, dass die Managementschnittstelle vor unberechtigtem Zugang geschützt ist. Die Managementschnittstelle MUSS durch eine Kombination aus Benutzername und Passwort oder einen mindestens gleich starken Mechanismus vor unberechtigtem Zugang geschützt sein.

© gematik – öffentlich_Entwurf

Für die Erstellung und Verarbeitung von Passwörtern der Managementschnittstelle MÜSSEN die Empfehlungen der Grundschutz-Kataloge des BSI beachtet werden (siehe Maßnahme „M 2.11 Regelung des Passwortgebrauchs“ in [BSI_GK]).

Für die Passworterstellung MUSS der Konnektor mindestens folgende Aspekte berücksichtigen:

- dem Benutzer muss es möglich sein, die Zeichen eines Passworts aus den Zeichenklassen Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Ziffern zu wählen. Ein Passwort muss Zeichen aus mindestens drei dieser Zeichenklassen enthalten.
- ein Passwort muss mindestens 8 Zeichen lang sein
- ein Passwort darf nicht die zugehörige Benutzerkennung enthalten (weder vorwärts noch rückwärts, bei Vergleich unter Ignorierung der Groß- und Kleinschreibung)
- die Wiederholung alter Passwörter beim Passwortwechsel durch den Benutzer selbst muss vom Konnektor verhindert werden (Passworthistorie). Dazu muss der Konnektor mindestens die letzten drei Passwörter eines Benutzers bei der Passwortneuvergabe erkennen und als neues Passwort ablehnen.

Für die Passwortverarbeitung MUSS der Konnektor mindestens folgende Aspekte berücksichtigen

- für die Erstanmeldung neuer Benutzer müssen Einmalpasswörter vergeben werden, also Passwörter, die nach einmaligem Gebrauch gewechselt werden müssen. Gleiches gilt, wenn ein Passwort eines Benutzers vom Super-Admin zurückgesetzt wird.
- jeder Benutzer muss sein eigenes Passwort jederzeit ändern können
- bei der Eingabe darf das Passwort nicht im Klartext auf dem Bildschirm angezeigt werden
- die Passwörter müssen im Konnektor zugriffssicher gespeichert werden
- der Konnektor muss nach einem durch den Super-Admin konfigurierbaren Zeitraum (Voreinstellung: 120 Tage) einen Passwortwechsel beim nächsten Login initiieren
- erfolglose Anmeldeversuche müssen mit einer kurzen Fehlermeldung ohne Angabe von näheren Einzelheiten abgelehnt werden. Insbesondere darf bei erfolglosen Anmeldeversuchen nicht erkennbar sein, ob der eingegebene Benutzername oder das eingegebene Passwort (oder beides) falsch ist.
- Nach einer Fehleingabe des Passworts muss eine Verzögerung bis zur nächsten Eingabemöglichkeit des Passworts für dieselbe Benutzerkennung erfolgen. Die Verzögerung soll 3 Sekunden betragen.⌫

Näheres hierzu regeln die Schutzprofile des Konnektors.

⌦ **TIP1-A_4810 Benutzerverwaltung der Managementschnittstelle**

© gematik – öffentlich_Entwurf

Der Konnektor MUSS eine Benutzerverwaltung für die Managementschnittstelle enthalten, in der anmeldeberechtigte Administratoren-Benutzer definiert werden können.

Die Benutzerverwaltung MUSS die Administrator-Rollen Lokaler-Administrator, Remote-Administrator und Super-Administrator unterstützen.

Den Administrator-Rollen MÜSSEN folgende Rechte zugewiesen sein:

- Lokaler-Administrator:
  - ausschließlicher Zugriff über lokalen Endpunkt der Managementschnittstelle
  - Verwaltung aller Konfigurationsdaten und Durchführung aller Administratoraktionen mit Ausnahme von:
    - i. Benutzerverwaltung gemäß Tabelle TAB_KON_655
- Remote-Administrator:
  - ausschließlicher Zugriff über remote-Endpunkt der Managementschnittstelle
  - Verwaltung aller Konfigurationsdaten und Durchführung aller Administratoraktionen mit Ausnahme von:
    - i. Benutzerverwaltung gemäß Tabelle TAB_KON_655
    - ii. Konfigurationseinstellungen und Administratoraktionen gemäß Tabelle TAB_KON_851

    ~~und Werksreset~~
- Super-Administrator:
  - ausschließlicher Zugriff über lokalen Endpunkt der Managementschnittstelle
  - Benutzerverwaltung gemäß Tabelle TAB_KON_655
  - Verwaltung aller Konfigurationsdaten und Durchführung aller Administratoraktionen

Tabelle 1 TAB_KON_655 Konfigurationen der Benutzerverwaltung (Super-Administrator)

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
MGM_USER_LIST	Liste von Benutzernamen und deren Kontaktdaten	Liste von Benutzern und deren Kontaktdaten. Benutzerkonten MÜSSEN angelegt, geändert und gelöscht werden können. Das Passwort eines Benutzerkonten MUSS neu gesetzt werden können.
MGM_ADMIN_RIGHTS	Liste von Zugriffsrechten eines Benutzers	i. Eindeutige Zuordnung eines Benutzerkontos zu einer Rolle. Die Benutzerverwaltung MUSS sicherstellen, dass zu jeder Zeit mindestens ein Benutzerkonto mit

© gematik – öffentlich_Entwurf

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
		der Rolle Super-Administrator vorhanden ist. Gewähren / Entziehen von Rechten für Benutzerkonten: ii. Zugriffsrechte bezüglich der Konfigurationsbereiche. iii. Recht zum Aufbau einer Remote-Management Session und / oder zur Konfiguration des Remote-Management gemäß TAB_KON_663 ~~- Session~~ (USER_INIT_REMOTESESSION). v. Recht für einen Werksreset (USER_RESET_PERMISSION)

Die Benutzerverwaltung MUSS es jedem Benutzer ermöglichen Konfigurationsänderungen gemäß Tabelle TAB_KON_656 vorzunehmen:

Tabelle 2 TAB_KON_656 Konfigurationen der Benutzerverwaltung

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
`MGM_USER_INFO`	`Kontaktdaten`	Der angemeldete Benutzer MUSS seine Kontaktdaten ändern können. Der Benutzername DARF NICHT änderbar sein.

⌫

…

4.3.8 Remote Management

Im Betreibermodell der TI wird unter Remote Management ein delegierter Betrieb dezentraler Produkte durch einen durch den Anwender beauftragten Servicepartner verstanden. Der Servicepartner stellt als Vertragsbestandteil bevollmächtigte Personen zur Verfügung, die sich ständig um die Betriebs- und Datensicherheit der dezentralen Produkte im Rahmen eines Remote Managements kümmern.

Voraussetzung für die Etablierung dieses Bestandteils des Betreibermodells der TI ist, dass ein dezentrales Produkt ein Remote Management technisch unterstützt. Die nachfolgend aufgeführten Anforderungen bilden die Grundlage für die Nutzung von Remote Management am Konnektor. ~~Der Hersteller des Konnektors kann unter Berücksichtigung dieser Anforderungen weitere herstellerspezifische Funktionen zum Remote Management implementieren.~~

Zum Remote Management gehören die Verwaltung von Konfigurationsdaten und die Durchführung weiterer Administratoraktionen wie z. B. die Aktualisierung der Software des Konnektors. Im Rahmen des Remote Managements kann der Konnektor Remote Monitoring unterstützen. Dazu übermittelt der Konnektor Betriebszustandsdaten an das Remote-Management-System.

⌦ **TIP1-A_7276 Remote Management Konnektor**

Der Konnektor MUSS Remote Management technisch unterstützen.⌫

© gematik – öffentlich_Entwurf

⌦ **TIP1-A_5647 Remote Management Konnektor: Personenbezogene Daten**

Der Konnektor DARF über die Remote-Managementschnittstelle KEINE personenbezogenen Daten übertragen oder darstellen.⌫

⌦ **TIP1-A_5648 Remote Management Konnektor: Offene Schnittstelle**

Der Hersteller des Konnektors MUSS die zur Nutzung der Remote-Managemenschnittstelle notwendigen Informationen offenlegen. Der Hersteller des Konnektors MUSS die Remote-Managementschnittstelle so spezifizieren und implementieren, dass diese auch für Dritte (z.B. einen durch den Anwender beauftragten Servicepartner) nutzbar ist. ⌫

⌦ **TIP1-A_5649 Remote Management Konnektor: Standardbasierte Protokolle**

Der Hersteller des Konnektors SOLL für die Implementierung der Remote-Managementschnittstelle standardbasierte Verfahren und Protokolle einsetzen.⌫

⌦ **TIP1-A_5650 Remote Management Konnektor: Aufbau der Verbindung**

Der Konnektor MUSS sicherstellen, dass die Initiierung einer Remote-Managementverbindung im Sinne des Verbindungsaufbaus immer vom Konnektor ausgeht ~~und nur durch einen angemeldeten Benutzer mit einer der Rollen {Lokaler Administrator; Super-Administrator} und dem Recht USER_INIT_REMOTESESSION ausgelöst werden darf~~.⌫

~~Nach Aufbau der Verbindung muss sich der Remote-Administrator gemäß TIP1-A_4808 zuerst authentisieren.~~

⌦ **TIP1-A_5651 Remote Management Konnektor: Absicherung der Verbindung**

Der Konnektor MUSS die Remote-Management-Verbindung durch Nutzung eines kryptographischen Verfahrens gemäß [gemSpec_Krypt] hinsichtlich Vertraulichkeit, Integrität und Authentizität absichern ~~und eine gegenseitige Authentifizierung durchführen~~.⌫

Das Remote-Management-System authentisiert sich auf Transportebene zertifikatsbasiert gegenüber dem Konnektor .

⌦ **TIP1-A_7277 Authentifizierung des Remote-Management-Systems**

Der Konnektor MUSS eine zertifikatsbasierte Authentifizierung des Remote-Management-Systems auf Transportebene durchführen. ⌫

⌦ **TIP1-A_7278 Authentisierung des Konnektors gegenüber Remote-Management-System**

Der Konnektor MUSS sich gegenüber dem Remote-Management-System zertifikatsbasiert oder mittels Username/Password authentisieren. ⌫

⌦ **TIP1-A_7281 Authentifizierung des Konnektors durch das Remote-Management-System**

Das Remote-Management-System MUSS eine Authentifizierung des Konnektors durchführen. ⌫

© gematik – öffentlich_Entwurf

Die Authentifizierung des Remote-Management-Systems durch den Konnektor auf Transportebene ist verpflichtend gefordert.

Darüber hinaus können optional Remote-Administratoren in der Benutzerverwaltung des Konnektors konfiguriert werden. Wenn Remote-Administratoren in der Benutzerverwaltung konfiguriert sind, muss der Konnektor diese verpflichtend auf Anwendungsebene authentifizieren.

Wenn kein Remote-Administrator konfiguriert ist, vertraut der Konnektor der Benutzerverwaltung des Remote-Management-Systems. Auch wenn die Verwaltung von Remote-Administratoren an das Remote-Management-System delegiert ist, werden alle Zugriffe über das Remote-Management-System auf den Konnektor mit der Rolle Remote-Administrator ausgeführt. Das Remote-Management-System muss die Authentisierung der Remote-Administratoren und die Nachvollziehbarkeit der Zugriffe sicherstellen.

⌦ TIP1-A_7279 Authentifizierung des Remote-Administrators

Wenn in der Benutzerverwaltung des Konnektors Administratoren mit der Administrator-Rolle Remote-Administrator konfiguriert sind, MUSS der Konnektor diese gemäß TIP1-A_4808 authentifizieren. ⌫

⌦ TIP1-A_7280 Einschränkung der Rechte des Remote-Administrators

Der Konnektor DARF Remote-Administratoren Rechte gemäß TAB_KON_851 und TAB_KON_655 NICHT gewähren. ⌫

Tabelle 3 TAB_KON_851 Einschränkung der Rechte des Remote-Administrators (Blacklist)

Referenz	Konfigurationseinstellung / Administratoraktion	Bemerkung
Fachliche Anbindung der Clientsysteme		
TIP1-A_4517	Schlüssel und X.509-Zertifikate für die Authentisierung des Clientsystems erzeugen und exportieren sowie X.509-Zertifikate importieren	
TIP1-A_4518	Konfiguration der Anbindung Clientsysteme	
Kartendienst		
TIP1-A_5110	Übersicht über alle verfügbaren Karten	Karten vom Typ eGK und HBA DÜRFEN dem Remote-Administrator NICHT angezeigt werden
TIP1-A_5111	PIN-Management der SM-Bs für den Administrator	
Zertifikatsdienst		
TIP1-A_4704	Zertifikatsablauf anzeigen	Zertifikate von Karten vom Typ eGK und HBA DÜRFEN dem Remote-Administrator NICHT angezeigt werden

© gematik – öffentlich_Entwurf

Referenz	Konfigurationseinstellung / Administratoraktion	Bemerkung
Protokollierungsdienst		
TIP1-A_4716	Einsichtnahme und Veränderung der Protokolle	Personenbezogenen Daten DARF der Remote-Administrator NICHT einsehen und exportieren. Fachmodulprotokollen müssen daher entweder gesperrt, oder die personenbezogenen Daten aus diesen für den Remote-Administrator gefiltert werden.
TIP1-A_4814	Export- Import von Konfigurationsdaten	
Neustart und Werksreset		
TIP1-A_4820	Werksreset des Konnektors	

TIP1-A_5652 Remote Management Konnektor: Konfiguration Remote Management

Der Konnektor MUSS sicherstellen, dass es ausschließlich einem ~~Super-Administrator~~ Administrator mit einer der Rollen {Lokaler Administrator; Super-Administrator} und dem Recht USER_INIT_REMOTESESSION möglich ist, Konfigurationsänderungen gemäß TAB_KON_663 vorzunehmen.

Tabelle 4 TAB_KON_663 Konfigurationen des Remote Managements

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
`MGM_REMOTE_ALLOWED`	`Enabled / Disabled`	Der Administrator MUSS einstellen können, ob der Konnektor eine Remote-Management-Verbindung aufbauen kann, über die Konfigurationen vorgenommen werden können. Enabled: Der Konnektor kann eine Remote-Management-Verbindung aufbauen und erlaubt Konfiguration über das Remote-Management System. Disabled: Der Konnektor erlaubt keine Konfiguration über das Remote Management-System ~~kann keine Remote-Management-Verbindung aufbauen~~ Default-Wert: Disabled
`MGM_REMOTE_MONITORING_ALLOWED`	`Enabled / Disabled`	Der Konnektor KANN Remote-Monitoring unterstützen. In diesem Fall MUSS der Konnektor dem Administrator die Aktivierung und Deaktivierung des Remote-Monitoring ermöglichen. Enabled: Der Konnektor baut eine Remote-

© gematik – öffentlich_Entwurf

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
		Managementverbindung auf. Der Konnektor übermittelt Betriebszustände gemäß TAB_KON_503 an das Remote-Management-System. Disabled: Remote-Monitoring ist deaktiviert. Der Konnektor übermittelt keine Betriebszustände an das Remote-Management-System. Default-Wert: Disabled
Der Konnektor SOLL die Konfiguration der URL des Remote-Management-Systems, der Zertifikatsinformationen zur Authentisierung des Remote-Management-Systems und der Credentials für die Authentisierung des Konnektors beim Remote-Management-System ermöglichen.		

⌫

⌦ **TIP1-A_5653 Remote Management Konnektor: Protokollierung Remote Management**

Der Konnektor MUSS im Rahmen des Remote-Managements folgende Aktionen protokollieren:

- Beginn einer Remote-Session durch TUC_KON_271 „Schreibe Protokolleintrag“ {„MGM/REMOTE_SESSION“; Op; Info; „InitUser=$AdminUsername; RemoteID=<Kennung der Gegenstelle>; Mode=[InitSuccess / InitFail]“}
- Verbindungsabbau Remote-Session durch TUC_KON_271 „Schreibe Protokolleintrag“ {„MGM/REMOTE_SESSION“; Op; Info; „InitUser=$AdminUsername; RemoteID=<Kennung der Gegenstelle>; Mode=Exit“}

Die Protokollierungspflicht gilt nicht für das Remote Monitoring

Wenn ein remote-Zugriff erfolgt, ohne dass ein Remote-Administrator im Konnektor konfiguriert ist, so MUSS als InitUser eine Referenz auf das Remote-Management-System verwendet werden.⌫

…

Ein Softwareupdate gemäß TIP1-A_5657 kann auch über das Remote Management initiiert, ~~und~~ aktiviert und freigeschaltet werden. ~~Auch in diesem Fall muss jedes Softwareupdate vor Aktivierung einzeln vom Nutzer bzw. einem von ihm beauftragten lokalen Administrator freigeschaltet werden.~~

4.3.9 Software- und Konfigurationsaktualisierung (KSR-Client)

⌦ **TIP1-A_5657 Freischaltung von Softwareupdates**

Der Konnektor MUSS sicherstellen, dass Softwareupdates durch den Nutzer bzw. einen von ihm beauftragten ~~lokalen~~ Administrator ~~aus der lokalen Einsatzumgebung~~

© gematik – öffentlich_Entwurf

~~des Konnektors heraus~~ einzeln freigeschaltet werden. Der Konnektor DARF ein Softwareupdate NICHT ohne vorher erfolgte Freischaltung aktivieren.⌫

⌦ **TIP1-A_5659 Bewusste Entscheidung bei Freischaltung von Softwareupdates**

Der Hersteller des Konnektors MUSS in seinem Handbuch den Nutzer (bzw. den von ihm beauftragten ~~lokalen~~ Administrator) darauf hinweisen, dass der Anwender ein Softwareupdate nur dann aktivieren soll, wenn er ausreichend Informationen über den Inhalt des Softwareupdates erhalten hat, die ihm eine bewusste Entscheidung bei der Freischaltung ermöglichen.⌫

Änderungsbedarf in gemProd_Kon_PTV3

Tabelle 3: Anforderungen zur funktionalen Eignung "Produkttest / Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_7276	Remote Management Konnektor	gemSpec_Kon
TIP1-A_7277	Authentifizierung des Remote-Management-Systems	gemSpec_Kon
TIP1-A_7278	Authentisierung des Konnektors gegenüber Remote-Management-System	gemSpec_Kon
TIP1-A_7279	Authentifizierung des Remote-Administrators	gemSpec_Kon
TIP1-A_7280	Einschränkung der Rechte des Remote-Administrators	gemSpec_Kon

Tabelle 5: Anforderungen zur funktionalen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_7276	Remote Management Konnektor	gemSpec_Kon

Tabelle 7: Anforderungen zur sicherheitstechnischen Eignung "CC-Evaluierung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_7277	Authentifizierung des Remote-Management-Systems	gemSpec_Kon
TIP1-A_7278	Authentisierung des Konnektors gegenüber Remote-Management-System	gemSpec_Kon
TIP1-A_7279	Authentifizierung des Remote-Administrators	gemSpec_Kon
TIP1-A_7280	Einschränkung der Rechte des Remote-Administrators	gemSpec_Kon

Tabelle 10: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_7281	Authentifizierung des Konnektors durch das Remote-Management-System	gemSpec_Kon

© gematik – öffentlich_Entwurf