VERSIONSHINWEISE

CGM KIM-CLIENTMODUL

Stand: Dezember 2025

Synchronizing Healthcare

CompuGroup Medical

INHALTSVERZEICHNIS

EINFÜHRUNG

In diesem Dokument finden Sie Hinweise zu neuen Funktionen oder Änderungen in der jeweiligen CGM KIM-Clientmodul-Version.

CGM KIM 1.5 – 1.10.0

Clientmodul intern

- Behebung von möglichen Schwachstellen im CGM KIM-Clientmodul.
  CGMTPMR-1365, CGMTPMR-1338
- Verlagerung des temporären Ordners für das CGM KIM-Clientmodul in den Hauptinstallationsordner des Clientmoduls, sowie Behebung eines Fehlers, der dazu führte das temporäre Dateien des CGM KIM-Clientmoduls nicht zuverlässig gelöscht worden sind.
  CGMTPMR-1357
- Herabstufen der Logausgabe in der Konsole des Clientmoduls auf INFO, da gewisse Konstellationen in der Zeichenfolge der Logausgabe dazu geführt haben, dass Signaltöne getriggert worden sind.
  CGMTPMR-1333
- Das Clientmodul bricht die Verarbeitung, bei einem KIM-Nachrichtenversand, bzw. Empfang, nicht mehr mit einem Fehler ab, solange die auf dem Konnektor befindliche Trust Service Status List (TSL) gültig ist.
  CGMTPMR-1312

Benutzeroberfläche

- Update des Frameworks für die Grafische Benutzeroberfläche auf VIA Version 17
  CGMTPMR-1323
- Behebung eines Rechtschreibfehlers in der Maske zur Bearbeitung eines im CGM KIM Clientmodul angelegten Clientsystem.
  CGMTPMR-1344
- Einfügen des Wertes „KIM1.5+“ auf der Einstellungsseite bei der Auswahlbox zur Aktivierung der Bereitschaft zum Empfang großer KIM-Nachrichten.
  CGMTPMR-1358

CGM KIM 1.5 – 1.11.0

Clientmodul intern

- Weitere Härtung der Verarbeitung des "MAIL FROM"-Commands, damit unterschiedliche Schreibweisen und extra Leerzeichen nicht zu einem Abbruch in dem Mailversand führen.
  CGMTPMR-1431
- Update intern verwendeter DNS-Bibliotheken
  CGMTPMR-1423
- Entfernen der Base64-Transportcodierung aus der Ermittlung der Nutzdaten und Entscheidung ob KAS genutzt werden muss oder nicht (15MiB) der vom Clientsystem an das Clientmodul übertragenen Maildaten.
  CGMTPMR-1405

Installer

- Härtung des Installers für das Clientmodul, sodass bei einer silent-Installation nicht dieselbe CM-Version nochmals installiert werden kann und der Dienst gestoppt wird. Der Installer bricht die silent-Installation ab mit vermerk im Log des Installers (Voraussetzung das Logging ist aktiv).
  CGMTPMR-1369

CGM KIM 1.5 – 1.11.1

Clientmodul intern

- Verbesserung des Verbindungsmanagements (Connection Pooling) zum Konnektor, sodass weniger TLS-Sessions benötigt werden bei Aufruf von Methoden zur bsp. Ver- oder Entschlüsselung von KIM-Nachrichten.
  CGMTPMR-1361
- Verbesserungen im Garbage Collector des Clientmoduls.
  CGMTPMR-1440
- Nicht genutzte Verbindungen zum Konnektor (als LDAP Proxy) werden nach einer einstellbaren Zeit abgebaut und nicht unendlich offen gehalten.
  CGMTPMR-1487
- Optimierungen im Caching des Konnektorzertifikates, wenn dieses erneuert / ausgetauscht wird.
  CGMTPMR-1327 (in Teilen)

CGM KIM 1.5 – 1.11.3

Installer

- Bugfixing des Installers für das Clientmodul, sodass ein Update einer CM Version bei einer „stillen“ Installation nicht abgebrochen wird.
  CGMTPMR-1507

Clientmodul intern

- Optimierung der Prüfintervalls , ob nicht genutzte Verbindungen geschlossen werden können.
  CGMTPMR-1513

CGM KIM 1.5 – 1.12.3

Das KIM-Clientmodul ab der Version 11.0.0-8_1.12.3 arbeitet nach der aktuellsten Spezifikationslage der gematik im Release 1.5.2-8.

Benutzeroberfläche

- Umsetzung der gematik Anforderung, dass bei der Kommunikation hin zu Clientsystemen (POP3 / SMTP) das KIM-Clientmodul über ein Self-Sign-Zertifikat auf Basis von RSA 3072 oder ECC mit NIST-Kurven, oder ein importiertes Zertifikat einer eigenen CA eine Verbindung zum Clientsystem etablieren muss, da Clientsysteme nicht immer mit ECC-Zertifikaten unter Verwendung von Brainpool-Kurven umgehen können. Dies wurde im administrativen Bereich der Benutzeroberfläche unter dem neuen Menüpunkt „Mail-Kommunikations-Zertifikate“ implementiert.

  Hinweis:
  Nach dem Update auf die Version 1.12.3 kommuniziert das KIM-Clientmodul mit einem neuen RSA 3072 Self-Sign-Zertifikat für POP3 und SMTP in Richtung des Clientsystems.
  Dies führt je nach Clientsystem dazu, dass die Vertrauensstellung zwischen Clientsystem und KIM-Clientmodul erneut hergestellt werden muss. Hierzu muss das Clientsystem (Thunderbird, Outlook, Primärsystem) dem neuen Zertifikat vertrauen.
  Bei Verwendung von Outlook muss das Zertifikat im Zertifikatsspeicher unter „Vertrauenswürdige Stammzertifizierungsstellen“ importiert werden.

  Im KIM-Clientmodul kann jederzeit ein neues Zertifikat, auf Basis RSA 3072 oder ECC mit NIST-Kurven, erstellt werden.
  CGMTPMR-1263, CGMTPMR-1540

- Bei einem Kartenwechsel über die GUI des KIM-Clientmoduls ist es nun möglich, auch eine für eine eHBA benötigte User-ID anzugeben. Zudem wurde die Möglichkeit geschaffen, auch Karten über verschiedene

Konnektoren und Kontexte hinweg auszuwählen.
CGMTPMR-845

- Umsetzung der gematik Anforderung A_24322, dass bei der Anlage eines Konnektors die Fingerprints auch in einem Block Format angezeigt werden müssen. Zudem wurde gemäß gematik Spezifikation die Anforderung umgesetzt, dass der Kunde bestätigt, den angezeigten Fingerprint gegen den Fingerprint aus der Konnektor Oberfläche geprüft zu haben.
  CGMTPMR-1327, CGMTPMR-1378
- Bei der Anlage eines Konnektors im KIM-Clientmodul wird in einem Schritt geprüft, ob Komponenten der TI erreichbar sind (Damit wird die Route geprüft). Es wurde ein Button integriert, der er ermöglicht die Route nochmals zu prüfen, falls diese noch nicht existiert hat und jetzt angelegt worden ist.
  CGMTPMR-1335
- Verbesserung der Fehleranzeige in der Benutzeroberfläche, wenn der Benutzername oder das Passwort bei einer Anmeldung nicht korrekt angegeben wurde. Zuvor wurde die Meldung „Unbekannter Fehler“ ausgegeben.
  CGMTPMR-1376
- Verbesserung der Fehlermeldung im KIM-Clientmodul, wenn zur Anmeldung an der Benutzeroberfläche mit einem KIM-Account eine falsche Karte gewählt worden ist.
  CGMTPMR-1358
- Update des Frameworks für die grafische Benutzeroberfläche auf VIA Version 18
  CGMTPMR-1491
- Korrektur einzelner Rechtschreibfehler.
  CGMTPMR-1522, CGMTPMR-1521

Clientmodul intern

- Optimierung bei der Entschlüsselung, sodass auch ECC only verschlüsselte KIM-Nachrichten entschlüsselt werden können.
  CGMTPMR-1052
- Performance Optimierungen innerhalb des KIM-Clientmoduls, sodass TLS-Verbindungen zum Konnektor nach einer Nutzung wieder nachgenutzt werden, sowie das Verbindungen zum LDAP-Proxy (Konnektor) auch nach einstellbarer Zeit abgebaut werden wenn nicht mehr in Nutzung.
  CGMTPMR-1361, CGMTPMT-1487
- Das KIM-Clientmodul verwendet nun gemäß gematik Anforderungen das KIM-Clientmodul-Zertifikat ausschließlich zum Verbindungsaufbau mit den jeweiligen Fachdiensten oder dem Konnektor.
  CGMTPMR-1382
- Um alle erforderlichen Karten für eine Entschlüsselung einer KIM-Nachricht vom Konnektor zu bekommen, wird dieser nun gemäß gematik Anforderung angewiesen vorrangig ECC-Zertifikate zurück zu geben und nur

im Bedarfsfall die RSA-Zertifikate.
CGMTPMR-1383

- Das KIM-Clientmodul weißt den Konnektor, gemäß gematik Anforderung an, die Signatur einer KIM-Nachricht vorrangig mit ECC-Zertifikaten der SMC-B durchzuführen.
  CGMTPMR-1384
- Härtung des Verhaltens des KIM-Clientmoduls, wenn eine KIM-Nachricht der Integritätsprüfung unterzogen wird und das sendende Clientsystem Sonderzeichen enthält in den zu prüfenden Headern und diese nicht gemäß RFC codiert sind.
  Eine solche KIM-Nachricht wird als Integritätsverletzt an das empfangende (abrufende) Clientsystem weiter geleitet gemäß gematik Spezifikation als RFC822 eingebetteter Anhang in einer Fehlernachricht.
  CGMTPMR-1532
- Behebung eines Fehlers der verhinderte, das für die internen POP3 sowie SMTP Ports, Ports größer 32767 vergeben werden konnten.
  CGMTPMR-1518

Clientmodul Logging

- Verbesserung der Ausgabe im error.log, wenn bei einem Mailversand oder Mailempfang das KIM-Clientmodul kein im Benutzernamen übergebenes Clientsystem kennt zu diesem Konnektor.
  CGMTPMR-1375

REST-Schnittstelle

- Umsetzung der gematik Anforderung, dass bei der Kommunikation hin zu Clientsystemen (POP3 / SMTP) das Clientmodul über ein Self-Sign-Zertifikat auf Basis von RSA 3072 oder ECC mit NIST-Kurven, oder ein importiertes Zertifikat einer eigenen CA eine Verbindung zum Clientsystem etablieren muss, da Clientsysteme nicht immer mit ECC-Zertifikaten unter Verwendung von Brainpool-Kurven umgehen können. Dies wurde im administrativen Bereich REST-API unter dem Bereich clientmodule-mail-server-tls-keystore implementiert.

  Hinweis:
  Nach dem Update auf die Version 1.12.3 kommuniziert das KIM-Clientmodul mit einem neuen RSA 3072 Self-Sign-Zertifikat für POP3 und SMTP in Richtung des Clientsystems.
  Dies führt je nach Clientsystem dazu, dass die Vertrauensstellung zwischen Clientsystem und KIM-Clientmodul erneut hergestellt werden muss. Hierzu muss das Clientsystem (Thunderbird, Outlook, Primärsystem) dem neuen Zertifikat vertrauen.
  Bei Verwendung von Outlook muss das Zertifikat im Zertifikatsspeicher unter „Vertrauenswürdige Stammzertifizierungsstellen“ importiert werden.

Im KIM-Clientmodul kann jederzeit ein neues Zertifikat, auf Basis RSA 3072 oder ECC mit NIST-Kurven, erstellt werden.
CGMTPMR-1263, CGMTPMR-1540

CGM KIM 1.5 – 1.18.0

WICHTIG:
Das KIM-Clientmodul ab der Version 11.0.0-15_1.18.0 arbeitet nach der aktuellsten Spezifikationslage der gematik im Release 1.5.2-9 und somit mit ECC-first, sofern ECC-Zertifikate vorliegen.
Das Clientmodul in Release 1.5.2-9 behebt eine Spezifikationsschwäche und ist zwingend einzusetzen um mit einem PTV6-Konnektor (Herstellerunabhängig) erfolgreiche Signaturen durchführen zu können im Kontext KIM Nachrichtenversand.

Benutzeroberfläche

- Update des Frameworks für die grafische Benutzeroberfläche auf VIA Version 19
- Anzeige von Karteninformationen Bei Kartenauswahl
  Es wurde eine neue Funktion bereitgestellt, die es ermöglicht erweiterte Informationen über eine SMC-B oder eHBA anzuzeigen wie Name, Kartenablaufdatum und Telematik-ID
  CGMTPMR-1299
- Anzeige von Verzeichnisdiensteintrag eines angemeldeten Benutzers
  Es wurde eine neue Funktion bereitgestellt auf der Statusseite eines angemeldeten Benutzers, die es ermöglicht den zugrundeliegenden Basisdatensatz im Verzeichnisdienst anzuzeigen.
  CGMTPMR-1300
- Verbesserungen im Wording. Behebung von Typos.
  CGMTPMR-1643

Clientmodul intern

- Behebung eines Fehlers, der verhinderte, dass ein importiertes Clientsystem-Zertifikat gelöscht werden kann.
  CGMTPMR-1564
- Das Clientmodul wurde intern auf eine neue Version des Spring Frameworks gehoben.
  CGMTPMR-753

- Härtung des Clientmoduls, sodass ein ungewollter Absturz des Clientmoduls der in seltenen Fällen auftreten kann, verhindert wird und somit die Systemressourcen des Hosts nicht unnötig belastet werden.
  CGMTPMR-1515
- Behebung diverser CVEs
  CGMTPMR-1563, CGMTPMR-1633. CGMTPMR-1664
- Wiederholter Versuch eines signDocument() mit einer anderen Karte, sofern die aktuell zur Signierung zu nutzende SMC-B durch den Konnektor abgelehnt wird.
  CGMTPMR-1657
- Das Clientmodul prüft gemäß gematik Spezifikation A_21381-01, ob es bereits ein ECC-Zertifikat basierend auf NIST-Kurven besitzt. Ist dies nicht der Fall, beantragt das Clientmodul automatisch ein neues Clientmodul-Zertifikat für die Kommunikation mit den Fachdiensten.
  CGMTPMR-1622
- Das Clientmodul setzt gemäß gematik Spezifikation A_27360 einen zus. neuen Header (X-KIM-KAS-EncSize) in der äußeren KIM-Nachricht wenn es eine Mail über KAS versendet. Dies beinhaltet die abgelegte Datenmenge nach der Verschlüsselung in Byte.
  CGMTPMR-1621
- Zur CMS(CAdES)-Signatur durch den Konnektor übergibt das Clientmodul beim Aufruf der SignDocument-Operation am Konnektor das zu signierende Dokument als MimeType="application/octet-stream" gemäß gematik Spezifikation KOM-LE-A_2299-02.
  CGMTPMR-1620
- Anpassung im Caching der TLS-Serverzertifikate gemäß gematik Spezfikation A_22348-01.
  CGMTPMR-1606
- Anpassung bei der Übermittlung von Fehlernachrichten gemäß gematik Spezifikation A_20650-07, sodass eine Fehlernachricht an den Empfänger einer KAS-Mail gesendet wird, wenn die interne Struktur der Trägermail nicht dem geforderten Struktur entspricht. Es wird er Header X-KIM-Fehlermeldung: 4020 gesetzt.
  CGMTPMR-1555
- Anpassung an der Erzeugung des intern genutzten JWT (Token) zur Nutzung des Accountmanagers gemäß Spezifikation A_19457-04.
  CGMTPMR-1553
- Anpassung an der Erzeugung einer Fehlernachricht gemäß Spezifikation KOM-LE-A_2046-01, wenn eine KIM-Nachricht nicht entschlüsselt werden kann. Der Betreff wurde geändert in „Die Nachricht konnte nicht **entschluesselt** werden“
  CGMTPMR-1120
- Das Clientmodul prüft gemäß gematik Spezifikation A_24020-03, ob die Größe der verschlüsselt auf dem KAS abgelegten KIM-Nachricht der Größenangabe im X-KIM-KAS-EncSize Header der Trägermail entspricht und

lehnt den Download bei Abweichung ab und informiert den Empfänger mit einer Fehlernachricht.
CGMTPMR-1116, CGMTPMR-1670, CGMTPMR-1665

- Anpassung an der internen Struktur einer KAS-Trägermail sowie Anpassung der Größenberechnung für interne Parameter zu einer KAS-Mail gemäß gematik Spezifikation A_19359-10.
  CGMTPMR-1096
- Behebung eines internen Fehlers bei der Auswertung der Größe einer KAS-Mail
  CGMTPMR-1682

REST-Schnittstelle

- Es wurde die Möglichkeit geschaffen, das Hauptkennwort auch über die REST-Schnittstelle zu ändern unter einer administrativen Anmeldung.
  CGMTPMR-1434

CGM KIM 1.5 – 1.20.0

WICHTIG:
Das KIM-Clientmodul ab Version 11.0.0-16_1.20.0 arbeitet gemäß der aktuellsten Spezifikationslage der gematik im Release 1.5.2-10 und adressiert wesentliche sicherheitsrelevante Schwachstellen innerhalb der gematik Spezifikation, die im Rahmen des CVDP (Coordinated Vulnerability Disclosure Program) der gematik gemeldet wurden und mit dieser Version des Clientmoduls gezielt behandelt und behoben werden.

Der Einsatz dieses Clientmoduls wird dringend empfohlen.

Benutzeroberfläche

- Update des Frameworks für die grafische Benutzeroberfläche auf VIA Version 20.0.1.
  CGMTPMR-1812
- Fehler bei der Anzeige/Ausgabe von Karteninformationen bei Kartenauswahl
  Es wurde ein Bug in der neuen Funktion zur Anzeige erweiterter Informationen über eine SMC-B oder eHBA behoben, der die Anzeige verhinderte.
  CGMTPMR-1693, CGMTPMR-1773
- Korrektur einer Fehleranzeige/Fehlertext bei einem Anmeldeversuch mit einer nicht registrierten KIM-Adresse.
  CGMTPMR-1696, CGMTPMR-1697
- Fehlerhafte Fensterverwaltung bei Upload eines Clientzertifikates
  Behebung eines Bugs der dazu führte das das Zertifikatsauswahlfenster, bei Upload eines Zertifikates in das Clientmodul, zweimal geöffnet wurde.
  CGMTPMR-1694

- Verbesserungen im Wording. Behebung von Typos.
  CGMTPMR-1643, CGMTPMR-1680

Clientmodul intern

- Behebung diverser CVEs
  CGMTPMR-1717, CGMTPMR-1852
- Erweiterung der Prüfung von TLS-Server-Zertifikaten
  Erweiterung der Zertifikatsprüfung des CGM KIM-Clientmoduls beim TLS-Verbindungsaufbau zum CGM KIM-Fachdienst. Es wird zusätzlich geprüft, dass das vom KIM-Fachdienst präsentierte Server-Zertifikat die technische Rolle "KIM-Fachdienst" enthält. Des Weiteren wurde die Ermittlung der zugrundeliegenden FQDN-Prüfung gemäß GS-A_5077 gehärtet.
  CGMTPMR-1864, CGMTPMR-1874
- Anpassung des Downloads von KAS-Daten
  Die vorhandene Implementierung für den Download von KAS-Daten (große KIM-Nachrichten) wurde gemäß RFC3986 gehärtet und Abhängigkeiten zu statischen Links, über die Nutzung von DNS-SD entfernt.
  Beim Herunterladen einer KAS-KIM-Nachricht (KIM-Nachricht > 15 MiB) ermittelt das CGM KIM-Clientmodul den KAS-Server nicht mehr direkt aus dem in der KAS-KIM-Nachricht enthaltenen Link, sondern das CGM KIM-Clientmodul ermittelt, mit Hilfe einer DNS-Anfrage und der KIM-Domain der Absender-Adresse, den KAS-Server selbst.
  CGMTPMR-1865
- Nutzung des Schlüsselbundes (MAC)
  Bei der Initialen Einrichtung nach Installation des CGM Clientmodul werden die verwendeten Passwörter, analog zum Anmeldeinformationsdienst unter Windows, im Schlüsselbund des MacOS abgelegt und durch das Clientmodul bei Start aus diesem geladen.
  CGMTPMR-1674
- Behebung eines internen Fehlers bei der Auswertung der Basisdaten einer VZD-Response
  Im Clientmodul wurde ein Fehler behoben bei der Auswertung der Response einer VZD Abfrage.
  Wenn bei der VZD-Response der Basisdaten, unter der die KIM-Adresse registriert ist, der countryCode nicht gesetzt ist, konnte im Clientmodul kein Login an der Oberfläche der GUI als Benutzer durchgeführt werden. Zudem ist ein Mailversand in diesem Falle nicht möglich.
  CGMTPMR-1877, CGMTPMR-1846