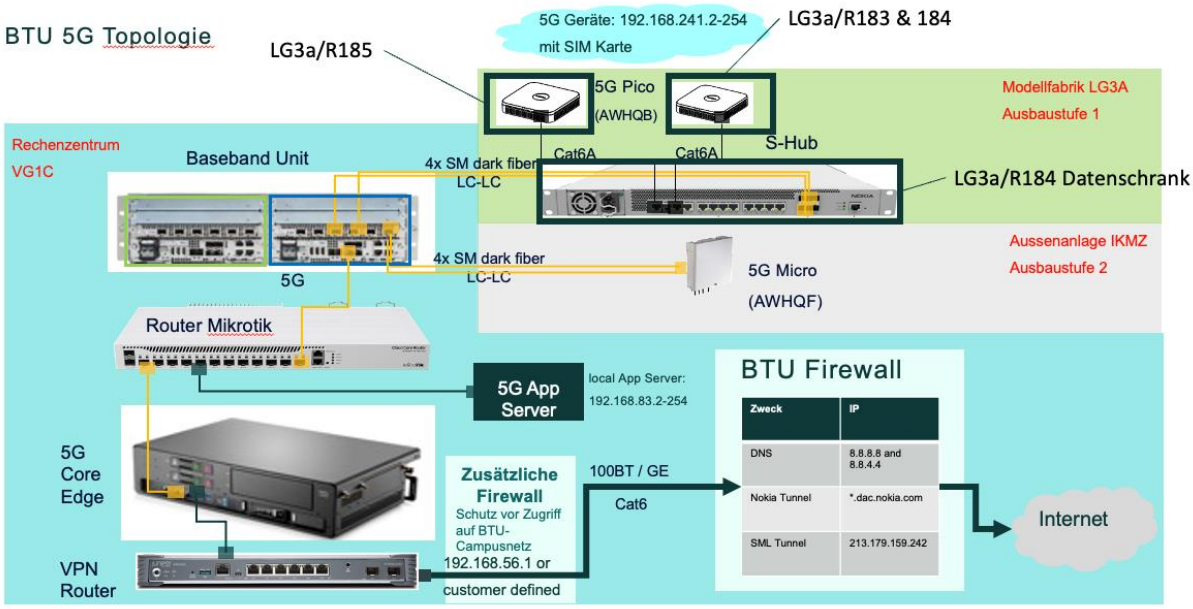
Betreiber- und Sicherheitskonzept für das 5G-Netz der Brandenburgischen Technischen Universität Cottbus-Senftenberg (BTU-CS) am Standort Cottbus.
Erarbeitet von Christine Ruffert, Reinhardt Karnapke und Philipp Staedter auf Basis der Vorarbeiten von Jonas Pantzer

Präambel
Im Rahmen des vom BMBF geförderten Strukturwandelprojektes „Innovationscampus Elektronik und Mikrosensorik Cottbus“ (kurz: iCampus, Fkz. 16ME0420K) soll ein 5G-Campusnetz an der Brandenburgischen Technischen Universität Cottbus-Senftenberg (BTU-CS) am Standort Cottbus betrieben werden. Hierfür wurde eine Machbarkeitsstudie durchgeführt und schließlich die Firma Smart Mobile Labs AG (SML) mit der Durchführung beauftragt.

Die benötigte Hardware der Firma Nokia wurde über SML beschafft und eingebaut. Die folgende Abbildung zeigt die vorgeschlagene und umgesetzt Platzierung der Hardware sowie die initiale Konfigurierung. Zu beachten ist hierbei, dass der gezeigte Zugang zum Internet aktuell auf die zum Betrieb notwendigen Verbindungen zu SML und Nokia beschränkt ist.



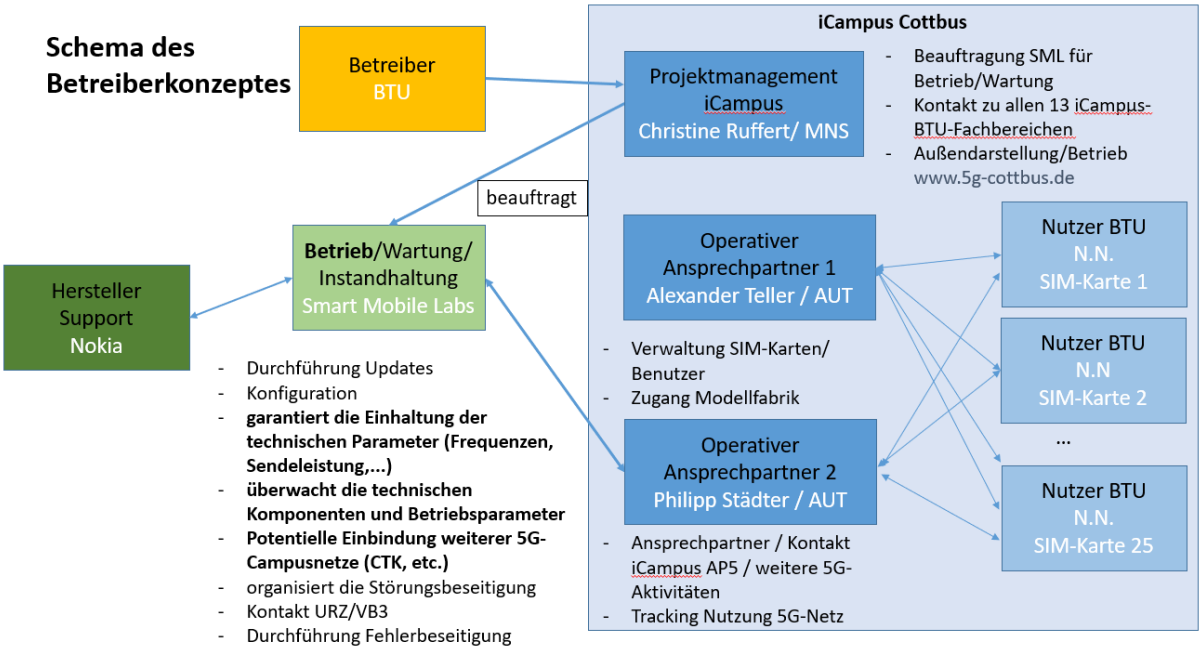
Betreiberkonzept
Für alle **legalen Belange** ist die BTU, vertreten durch den Vizepräsidenten für Forschung und Transfer (Prof. Dr.-Ing habil. Michael Hübner), Betreiber des 5G-Campusnetzes. Da es sich um ein Forschungsnetz handelt, werden keinerlei Garantien zur Verfügbarkeit des Netzes gemacht, insbesondere wird kein weiterführender Betrieb nach Ende des iCampus Projektes zum 31.12.2026 garantiert. Auch während der Laufzeit des Projektes wird nicht garantiert, dass SIM-Karten oder 5G-Netz verfügbar sind so wie von potentiellen Nutzern gewünscht.

Für die **technischen Belange** ist das Projektmanagement des iCampus-Projektes (Priv.-Doz. Dr.-Ing. Christine Ruffert) zuständig.

Das Projektmanagement des iCampus Projektes beauftragt die Firma SML mit Betrieb und Wartung des Campusnetzes. Weiterhin ist das Projektmanagement für die Außendarstellung zuständig und hält Kontakt zu allen beteiligten Fachgebieten.
Die Firma SML wird mit Betrieb und Wartung beauftragt, was insbesondere auch die garantierte Einhaltung der technischen Parameter (Frequenzen, Sendeleistung etc.) und die Überwachung der Komponenten beinhaltet. Die Firma SML steht in Kontakt zum Hersteller der Hardware, Nokia, und kann ggf. Herstellersupport veranlassen.

Für die **operativen Belange** zeichnet sich das Fachgebiet Automatisierungstechnik AUT (Prof. Dr.-Ing. Ulrich Berger) verantwortlich. Dies beinhaltet die Ausgabe und Rücknahme von SIM-Karten und den Zugang zur Modellfabrik (Alexander Teller) sowie die Möglichkeit zur Kontaktaufnahme bei technischen Problemen (Laboringenieur Philipp Städter). Herr Städter hat die Möglichkeit, kleinere Probleme vor Ort zu beheben; bei Bedarf nimmt er Kontakt zu SML auf.

SIM-Karten werden **ausschließlich an Mitarbeiterinnen und Mitarbeiter der BTU** und maximal für ein Jahr ausgegeben. Hierbei werden vorrangig Mitarbeiterinnen und Mitarbeiter der am iCampus-Projekt beteiligten Fachgebiete für ihre Forschung mit SIM-Karten versorgt. Sollten weitere Kapazitäten vorhanden sein, können auch Karten an Mitarbeiterinnen und Mitarbeiter anderer Fachgebiete ausgegeben werden. SIM-Kartenempfängerinnen und -empfängern wird seitens des Betreibers *keine* exklusive Nutzung garantiert, sie können sich untereinander absprechen.



Sicherheitskonzept

Antennen (-Zugang)
Für die Antenne auf dem Dach des IKMZ wurde eine Gefährdungsbeurteilung (GBU) durchgeführt und entsprechende Maßnahmen definiert (siehe Anlage).
Für die Antennen *in* der Modellfabrik im Lehrgebäude (LG) 3A muss nach §§ 5, 6 Arbeitsschutzgesetz keine GBU durchgeführt werden, da ihre Strahlungsleistung weniger als 1 W beträgt.

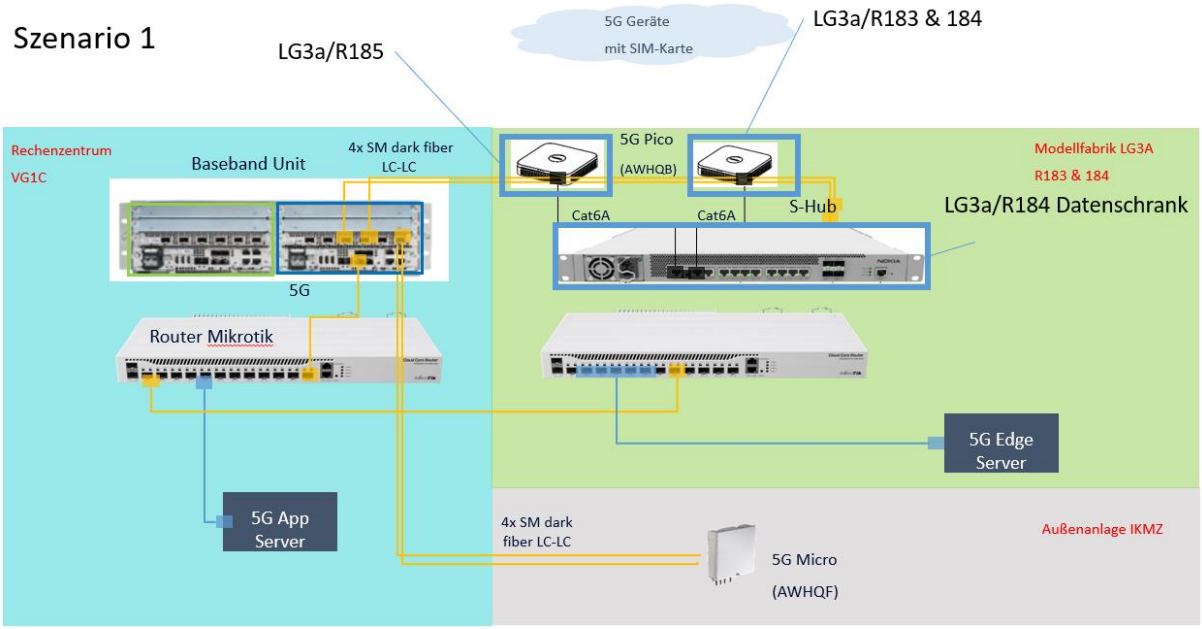
5G Hardware/Software
Die Wartung der 5G-Hardware und Sicherheitsupdates der zum direkten Betrieb dieser notwendigen Software sind Teil des Auftrags zu Betrieb, Wartung und Instandhaltung des 5G-Campusnetzes an die Firma SML.

IT-Sicherheit
Die zum Betrieb des 5G-Campusnetzes notwendige Verbindung zu SML und Nokia wird durch eine entsprechende Firewallkonfiguration vom Universitätsrechenzentrum ermöglicht (Dr. Klaus-Dieter Krannich/Thomas Pawell/Jörg Ladusch).
Wie im Betreiberkonzept dargelegt, werden SIM-Karten nur an Mitarbeiterinnen und Mitarbeiter der BTU ausgegeben. Diese garantieren beim Empfang mit ihrer Unterschrift, dass sie

- den Zeitraum bis zur Rückgabe der SIM-Karte(n) (maximal 1 Jahr) zur Kenntnis genommen haben,
- mindestens für den Zeitraum bis zur Rückgabe der SIM-Karte(n) an der BTU beschäftigt sind,
- die SIM-Karte(n) nicht an Dritte weitergeben,
- bei SIM-Kartenverlust für die Neubeschaffung aufkommen,
- die SIM-Karte(n) bei vorzeitigem Verlassen der BTU umgehend zurückgeben.

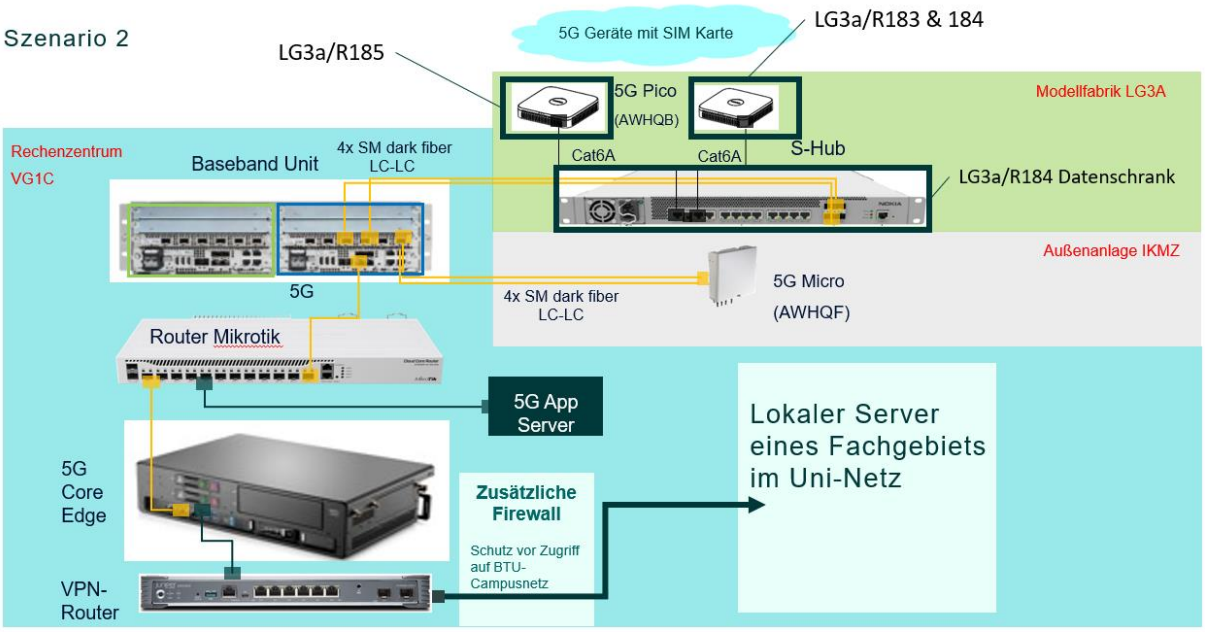
Im Folgenden werden drei Szenarien für die Verwendung des 5G-Campusnetzes betrachtet:

Szenario 1: Geschlossenes System
Es besteht die Möglichkeit, in Absprache mit dem Fachgebiet Automatisierungstechnik einen Server im LG3A zu platzieren. Dieser kann per Kabel mit dem 5G-Netz verbunden werden. Das Netz stellt sich schematisch wie folgt dar:



Geräte, welche sich mit einer der beiden 5G Pico-Antennen im LG3A oder der 5G-Micro-Antenne auf dem Dach des IKMZ verbinden, können somit über die Baseband Unit und den Mikrotik-Router diesen (Edge)-Server erreichen und mit ihm bilateral kommunizieren (Abbildung 2). Zugang für Anwenderinnen und Anwender besteht nur zu ihren Geräten mit SIM-Karte und zum (Edge)-Server und nicht zu anderen, in der Infrastruktur vorhandenen Geräten.
Da es sich um ein geschlossenes System handelt und keine Verbindung zum Universitätsnetz besteht, sind **keine weiteren Maßnahmen** nötig.

<u>Szenario 2: Verbindung zum lokalen Server eines Fachgebiets</u>
Es besteht die Möglichkeit, eine Verbindung zwischen mit 5G SIM-Karten ausgestatteten Geräten und dem Server eines der beteiligten Fachgebiete herzustellen. Hierfür muss eine Verbindung zwischen dem VPN-Router und dem Server des Fachgebiets eingerichtet werden. Dies bedarf einer expliziten Freischaltung durch das Universitäts-rechenzentrum (Dr. Klaus-Dieter Krannich/Thomas Pawell/ Jörg Ladusch) und muss entsprechend unter der Angabe, welche SIM-Karte(n) sich mit welchem Server binden können soll(en) in der Form: Quell-IP, Ziel-IP, Service, beantragt werden. Da SIM-Karten nur an Mitarbeitende der BTU ausgegeben werden, sind **keine weiteren Maßnahmen** notwendig. Das Netz stellt sich wie folgt dar:



Szenario 3: Zugang für Dritte

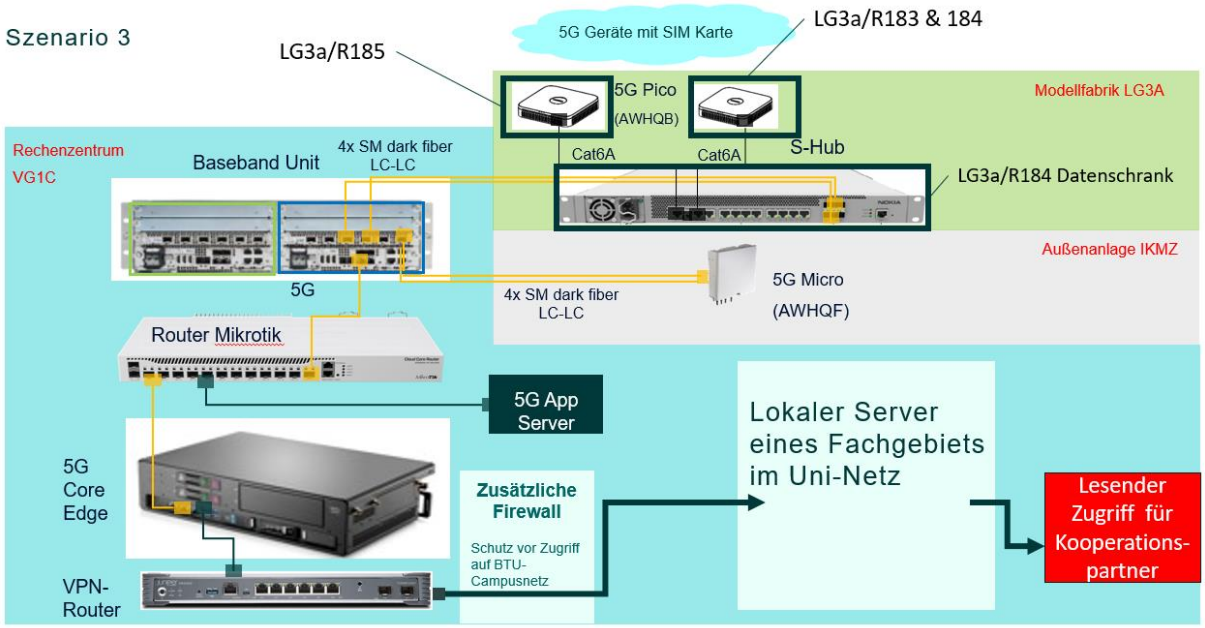
Die Ausgabe von SIM-Karten an Dritte ist *nicht* vorgesehen. Die Fachgebiete der BTU haben jedoch die Möglichkeit, mit Dritten zu kooperieren. Hierfür sind zwei Möglichkeiten denkbar, welche sich an den vorherigen Szenarien orientieren.

Szenario 3a: Geschlossenes System

Die Kooperationspartner können den Fachgebieten Geräte (z.B. Sensoren) zur Verfügung stellen, welche vom Fachgebiet mit einer SIM-Karte ausgerüstet werden und (i) am Fachgebiet oder (ii) im LG3A bzw. (iii) an der BTU in Cottbus verbleiben. Diese Geräte können sich gemäß Szenario 1 mit einem (Edge)-Server verbinden und mit diesem kommunizieren, dort Daten ablegen etc. Den Kooperationspartnern kann, in Absprache mit dem Fachgebiet Automatisierungstechnik, physischer Zugang zu diesem Server gewährt werden. Das Netz stellt sich wie in Szenario 1 gezeigt dar.
Da es sich um ein geschlossenes System handelt und keine Verbindung zum Universitätsnetz besteht, sind keine weiteren Maßnahmen nötig.

Szenario 3b: Verbindung zum lokalen Server eines Fachgebiets

Wie in Szenario 2 beschrieben, können die Daten der mit dem 5G-Netz verbundenen Geräte auch an einen lokalen Server eines Fachgebiets übertragen werden. Zu diesem Server kann ein stark eingeschränkter Zugang für Dritte ermöglicht werden. Hierbei muss garantiert werden, dass der Zugriff „nur lesend“ stattfindet. Gemeint ist hiermit, dass zwar die zum Server gesendeten Daten zugänglich gemacht werden, es aber keine Rückverbindung vom Server zu den Geräten geben kann. Der Grund hierfür liegt in der Tatsache, dass **Dritte keinen Zugang zum Universitätsnetz** bekommen dürfen.
Die Protokolle Remote-Desktop (rdp) und Secure-Shell (ssh) werden explizit ausgeschlossen. Ferner muss jede einzelne Firewall-Freigabe geprüft werden. Sollte eine Änderung an einem oder mehreren der Geräte vorgenommen werden müssen, so kann dies entweder durch eine Mitarbeiterin/einen Mitarbeiter des Fachgebiets vorgenommen werden oder in Absprache mit dem Fachgebiet Automatisierungstechnik durch physischen Zugang stattfinden. Das Netz stellt sich wie folgt dar:



Die folgende Abbildung stellt das Sicherheitskonzept unabhängig von den einzelnen Szenarien schematisch dar: