UPCARE-Abschlussbericht 2024

Deutsch-Französisches Verbundprojekt UPCARE	
Konsortialführer	Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V.
Partner	Bundesdruckerei GmbH
	Krebsregister Rheinland-Pfalz
	EURECOM (franz. Partner)
	Softeam (franz. Partner)
Vorhabenbezeichnung:	User-Centric and Privacy-preserving Cancer Research Platform
Laufzeit des Vorhabens:	1.6.2021- 31.5.2024
Berichtszeitraum:	1.6.2021- 31.5.2024

1. Übersicht und Kurzdarstellung

In Krebsregistern sammeln, speichern und analysieren medizinische Einrichtungen die Krankheitsdaten von Krebspatientinnen und-patienten, damit Forschende die Wirksamkeit von Therapien bewerten und Faktoren untersuchen können, die bestimmte Krebsarten beeinflussen. Die aktuelle Datenverarbeitungsarchitektur von Krebsregistern in Deutschland und Frankreich wurde jedoch zu Zeiten etabliert, als weder der Datenschutz auf dem heutigen Niveau war, noch mobile Apps und Cloud-Dienste existierten. Durch die konstante Weiterentwicklung der Gesetzgebung in Deutschland und Europa wurden seitdem Datenschutzanforderungen konkretisiert und gleichzeitig die Befugnisse der Krebsregister in Bezug auf die Datenanalyse erweitert. Krebsregister stehen somit vor der Herausforderung, detaillierte Datenanalysen in einem sich entwickelnden Markt für mobile Apps und Cloud-Dienste zu unterstützen und gleichzeitig wichtige persönliche und gesundheitsbezogene Daten zu schützen. Aktuell sind Krebsregister immer noch meist als isolierte Datenspeicher organisiert. Krebsforschenden ist es trotz des Rückgriffs auf standardisierte Datenformate dadurch nicht möglich, mehr als ein einzelnes Register gleichzeitig datenschutzkonform abzufragen.

1.1 Zielsetzung des Projekts

Das Projekt „User-Centric and Privacy-Preserving Cancer Research Platform“ (UPCARE) zielt darauf ab, eine moderne, grenzübergreifende deutsch-französische Plattform für die Abfrage von Krebsregistern zu schaffen, die geltende Datenschutzstandards berücksichtigt. Es erforscht, wie zum Beispiel registerübergreifende Anfragen aus Deutschland und Frankreich ermöglicht werden können. Zudem soll ein autorisierter Kreis von Nutzerinnen und Nutzern Daten für weitreichendere Analysen verwenden können. Zum Schutz der Daten werden hierbei verschiedene Verschlüsselungsverfahren und weitere Schutzmechanismen eingesetzt, die einen zweckgebundenen Zugriff auf die Daten sicherstellen. Auf diese Weise werden datenschutzfreundliche Analysemethoden entwickelt und beispielhaft in die Architektur eines ausgewählten Krebsregisters integriert, was einerseits ein hohes Datenschutzniveau verspricht, und andererseits aussagekräftige Erkenntnisse für die Krebsforschung ermöglicht.

Die Entwicklungen des Projekts trug dazu bei, die derzeitige Isolation der einzelnen Krebsregisterdatenbanken zu minimieren. Langfristig kann so eine multinationale Krebsforschungsplattform aufgebaut werden, die es Forschenden erlaubt, europaweite Studien durchzuführen und die dazu beiträgt, die Qualität der Krebsforschung nachhaltig zu verbessern. Gleichzeitig bleiben durch die Datenschutzmaßnahmen die Autonomie der einzelnen Krebsregister sowie der Schutz der Privatsphäre der Patientinnen und Patienten gewahrt. Übergeordnet wurde so exemplarisch gezeigt, dass die weitreichende Nutzung und Analyse von sensiblen Daten mit einem hohen Datenschutzniveau durchaus vereinbar sind.

1.2 Projektpartner

Die Konsortialpartner des UPCARE-Projekts sind das Fraunhofer AISEC (AISEC), die Bundesdruckerei GmbH (BuDru), das Krebsregister Rheinland-Pfalz (KR RLP), EURECOM sowie SOFTEAM S.A. Zusätzlich ist darauf hinzuweisen, dass die Bundesdruckerei GmbH die Firma klargedacht.io im Rahmen eines Unterauftrages in das Projekt eingebunden hatte.

1.3 Projektstruktur und Arbeitsprogramm

Das Projekt war als dreijähriges Projekt geplant und zielte auf die Erstellung und Evaluierung eines Demonstrators im Bereich TRL 4 bis 5 ab, der die Spezifikationen und Bedürfnisse der Krebsregister berücksichtigt. In einer ersten Phase hat das Konsortium gemeinsam an den Anforderungserhebung gearbeitet, um die Details der technologischen Ansätze in einer gemeinsamen Architektur zu vereinen und eine erste gemeinsame Implementierung der Innovationen umzusetzen. In der zweiten Phase werden die einzelnen Technologien vorangetrieben und Beiträge zu den jeweiligen Forschungsfeldern geleistet, während durch regelmäßige Synchronisationspunkte sichergestellt wurde, dass die Architektur wie geplant realisiert werden kann oder entsprechend angepasst werden muss. Das Ergebnis dieser Phase ist eine “Proof-of-Concept"-Implementierung, die alle geplanten kryptografischen Mechanismen und Workflows enthält, jedoch nicht unbedingt vollständig ist. In der dritten und letzten Phase liefen die Arbeitsabläufe wieder zusammen und die Partner haben die Technologien gemeinsam in den Demonstrator integriert und gemeinsam an dessen Bewertung arbeiten. Parallel zu diesen Phasen wurden die Forschungsarbeiten von Verbreitungs- und Projektmanagementaktivitäten begleitet.

Abbildung 1

Im Rahmen der Zusammenarbeit zwischen den Konsortien und Konsortialpartnern wurden entsprechende Konsortien- und Konsortialtreffen geplant und durchgeführt.

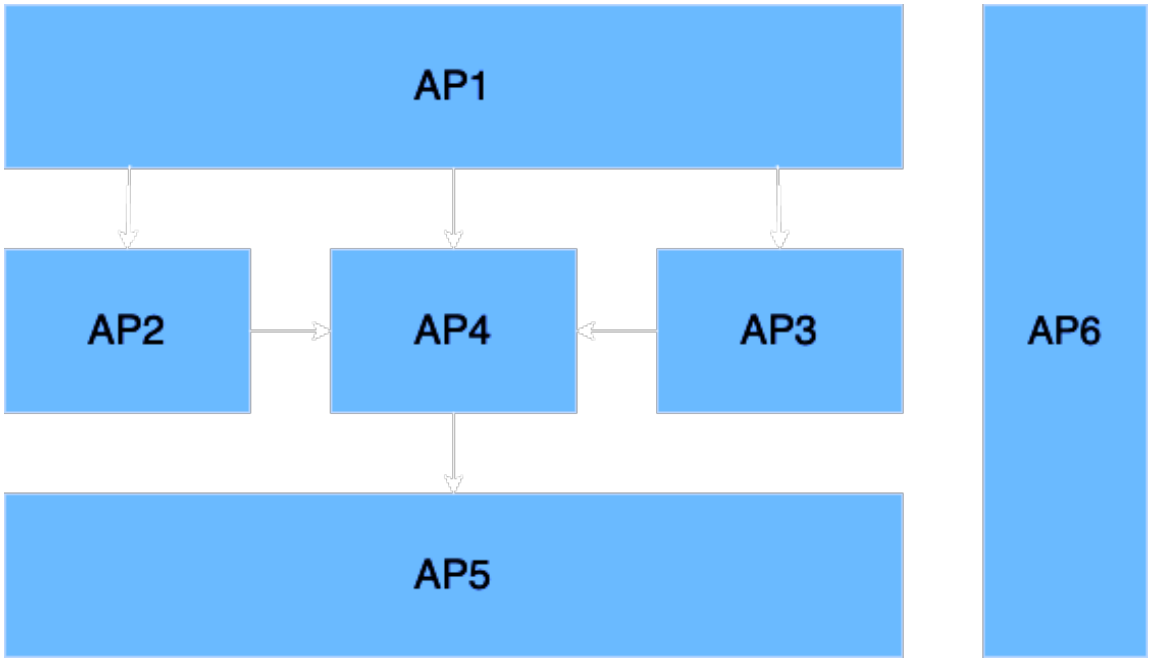


Abbildung 2

Abbildung 2 zeigt das Arbeitsprogramm des UPCARE-Projekts, das sich in insgesamt fünf inhaltliche (AP1-AP5) sowie ein administratives und verwertungsorientiertes Arbeitspaket (AP6) gliedert. Die zentralen Fragestellungen, denen die inhaltlichen Arbeitspakete nachgehen, können wie folgt zusammengefasst werden:

AP1 Anforderungen

- Welche Anforderungen muss eine Krebsforschungs-Plattform erfüllen?
- Was ist der aktuelle IST-Zustand bei der Datenabfrage in Krebsregistern?
- Wo liegen die Grenzen, die durch die praktischen und datenschutzrechtlichen Aspekte gegeben sind?
- Welche Arbeitsabläufe (in den klassischen Krebsregistern) könnten durch eine solche Plattform automatisiert werden?

AP2 Design der Plattform

- Welche Verfahren/Abläufe in den Krebsregistern können mittels kryptographischer Methoden verbessert bzw. automatisiert werden?
- Welche Spezifikationen folgen aus den Anforderungen an eine solche Plattform?
- Wie kann eine solche Plattform am besten umgesetzt werden?

AP3 Design und Entwicklung des „Private Computing“ Moduls

- Welche Verfahren bieten einen Privatsphäre-schonenden Zugriff auf statistische Auswertungen der Daten in den Krebsregistern?
- Wie kann dieser Zugriff auf multiple Krebsregister erweitert werden?
- Wie kann ein solches Verfahren am besten umgesetzt werden?

AP4 Design und Entwicklung der kryptographischen Zugriffskontrolle

- Welche rechtlichen Voraussetzungen liegen vor und wie können diese mit Hilfe eine Zugriffskontrolle umgesetzt werden?
- Welche Akzeptanz bzw. welchen zusätzlichen Nutzen erfährt der Forscher durch eine dynamische Zugriffskontrolle mittels Kryptographie?
- Ist die eingesetzt Kryptographie effizient genug, um die Krebsdaten direkt im Browser des Forschers zu entschlüsseln.

AP5 Demonstration des Anwendungsfalls

- Sind beide Use Cases (AP3 und AP4) mittels eines zentralen Protokolls integrierbar?
- Wie verhält sich der Demonstrator in einer produktiven Umgebung?
- Ist die Effizienz der eingesetzten Verfahren mit Standard-Hardware ausreichend?

AP6 Projektmanagement

- Wie können die Ergebnisse wissenschaftlich verwertet werden?
- Welche Koordination ist zwischen den Projektpartnern notwendig?

1.4 Zusammenfassung der Projektergebnisse

Die Ergebnisse des UPCARE-Projekts lassen sich aus wirtschaftlicher, technischer sowie rechtlicher Sicht wie folgt zusammenfassen:

Wirtschaftliche Perspektive

- Es wurden technologische Anknüpfungspunkte im Rahmen von u.a. europäischen (Medical) Data Spaces Initiativen identifiziert, in welchen die Technologien bzw. das Know-How aus UPCARE auch wirtschaftlich verwertet werden können.

Technische Perspektive

- Umsetzung einer Plattform als Demonstrator zum Zugriff auf Krebsregisterdaten mittels zweier Use Cases
    - Kryptographisch gesicherter statistischer Zugriff auf Durchschnittswerte
    - Kryptographisch gesicherter Zugriff auf personenbezogene Daten nach Erlaubnis der Beteiligten

Rechtliche Perspektive

- Rechtssichere Umsetzung eines datenschutzfreundlichen Zugriffs auf Krebsregisterdaten

1.5 Verwertung

Die Verwertung der erzielten Projektergebnisse in Wissenschaft und Wirtschaft kann wie folgt zusammengefasst werden:

Präsentation und Diskussion der Ansätze in Wissenschaft und Wirtschaft:
- Gesamtzahl der Publikationen: 1
- 1 internationale Konferenzen
- Ca. 10 Präsentationen auf Veranstaltungen

2 Wissenschaftliche und technische Ergebnisse

Im folgenden Kapitel werden die wichtigsten wissenschaftlich-technischen Ergebnisse sowie wichtige Ereignisse gegliedert nach Arbeitspaketen kurz dargestellt.

2.1 AP1 Anforderungen

Das Fraunhofer AISEC, die Bundesdruckerei und das Krebsregister RLP unterstützten SOFTEAM bei der Anforderungserhebung im Rahmen von regelmäßigen Gesprächen und Interviews in Meetings als auch über das von SOFTEAM bereitgestellte JIRA.
Hierbei wurde SOFTEAM bei der bei der Use-Case Modellierung unterstützt. Aus den daraus abgeleiteten Systemanforderungen entstanden die technischen Anforderungen an (1) den kryptografischen, Attributs basierten Zugriffskontrollmechanismus, (2) die Anfrageplattform, (3) den "Keyserver" und (4) den benutzerzentrierten Zustimmungsmechanismus.
Wie bereits erwähnt erfolgte die Dokumentation der Ergebnisse dieses APs über ein JIRA, welches von SOFTEAM bereitgestellt wurde und den aktuellen Stand der Anforderungsdokumentation darstellt.
Das Krebsregister Rheinland-Pfalz arbeitete eng mit den Projektpartnern zusammen, um die Anforderungen an die UPCARE-Plattform zu erheben. Dieser Prozess wurde durch eine Kombination aus verschiedenen Methoden durchgeführt, darunter Brainstorming in gemeinsamen Meetings und internen Interviews. Dabei wurden die spezifischen Bedürfnisse und Erwartungen der verschiedenen Stakeholder sowie der potenziellen Endnutzer von UPCARE erfasst. Ein JIRA-System von SOFTEAM diente als zentrale Plattform, um die gesammelten Anforderungen zu dokumentieren und kontinuierlich weiterzuentwickeln.

2.1.1 AP1.1

Im ersten Arbeitspaket wurden die Anforderungen an das geplante System ermittelt werden. SOFTEAM benutzte hierbei ihre erprobten Werkzeuge, Methoden und Fachkenntnisse, um zusammen mit dem KR RLP eine Basis für die technischen und wissenschaftlichen Arbeiten zu schaffen. Das Krebsregister Rheinland-Pfalz führte eine umfassende Analyse des aktuellen Stands der im Register eingesetzten technischen Infrastrukturen sowie der Datenbereitstellungsprozesse durch. Dabei wurden verschiedene technische Komponenten

und Prozesse des Registers eingehend untersucht, um deren Eignung und Potenzial für die Integration in die Plattform zu bewerten. Zu Beginn der Analyse lag der Fokus auf den verwendeten Datenformaten und Datenmodellen, die im Krebsregister zur Speicherung und Verarbeitung von Meldungen genutzt werden. Es wurde überprüft, ob diese Formate und Modelle standardisiert sind und wie gut sie mit den Anforderungen der UPCARE-Plattform harmonisieren. Ebenso wurde das Datenbanksystem des Registers überprüft, um sicherzustellen, dass es für die geplante Datenabfrage- und Verarbeitungsinfrastruktur der Plattform geeignet ist. Hierbei ging es nicht nur um die Kompatibilität der Systemarchitektur, sondern auch um Aspekte w1e Performance, Skalierbarkeit und Sicherheit der gespeicherten Daten.
Des Weiteren wurde eine eingehende Untersuchung der bestehenden Schnittstellen des Registers vorgenommen. Hierbei wurde geprüft, wie die bestehenden APl‘s oder anderen Kommunikationskanale genutzt werden können, um eine nahtlose Interoperabilität zwischen dem Krebsregister und der Plattform zu gewährleisten. Besondere Aufmerksamkeit galt zudem dem Anfrage-, Prof- und Genehmigungsprozess für die Nutzung von Krebsregisterdaten, insbesondere für aggregierte, pseudonymisierte und personenidentifizierende Daten. Dieser Prozess wurde detailliert analysiert, um zu verstehen, wie Anfragen von externen Forschenden bearbeitet und genehmigt werden. Dabei wurde auch untersucht, wie die bestehenden rechtlichen und organisatorischen Vorgaben in diesem Bereich eingehalten werden. Dies umfasste sowohl die technischen Abläufe der Datenanforderung als auch die Prüfmechanismen, die zur Gewährleistung der datenschutzrechtlichen Compliance erforderlich sind. Die Ergebnisse dieser Analyse waren von zentraler Bedeutung für die Spezifikation der Anforderungen an die Abfrageplattform, um sicherzustellen, dass die Plattform den gleichen hohen Standards in Bezug auf Datenschutz und Datensicherheit entspricht.
Die gewonnenen Erkenntnisse aus dieser umfassenden Analyse flossen direkt in die weiteren Schritte der Anforderungsdefinition ein und bildeten die Grundlage für die Entwicklung einer Abfrageplattform, die sowohl technisch robust als auch rechtlich abgesichert ist. Sie sorgten dafür, dass die Integration des Krebsregisters in die Plattform nicht nur funktional, sondern auch mit den notwendigen datenschutzrechtlichen und sicherheitstechnischen Anforderungen in Einklang stand.

2.1.2 AP1.2

Im Rahmen des AP1 beteiligte sich das AISEC bei der Spezifikation der technischen Anforderungen an den kryptographischen, attributbasierten Zugriffskontrollmechanismus (1), an die Anfrageplattform sowie den "Privacy Proxy" (2) sowie an dem benutzerzentrierten Zustimmungsmechanismus (3).

- Anforderungen an den kryptographischen, attributbasierten Zugriffskontrollmechanismus

  Als Datenformat der Patienten Stammdaten wurde der einheitliche, onkologische Basisdatensatz ADT/GEKID vom neuesten medizinischen Datenformat HL7 FHIR Resources ersetzt. Die Attributstruktur wurde an das neue Datenformat angepasst. Weitere funktionale Anforderungen an den kryptographischen, attributbasierten Zugriffskontrollmechanismus wie die Möglichkeit die Attribute im Chiffrat zu verstecken werden vom AISEC weiter in Betracht gezogen und bei der weiteren

Entwicklung des ABE Schemas erforscht.

- Anforderungen an die Anfrageplattform sowie den "Privacy Proxy":

  Die Anfrageplattform sollte dem Krebsforscher idealerweise einen transparenten, Datenschutz-freundlichen Zugriffspunkt auf Patientendaten bieten. Die Zustimmung der Patienten (Opt-In) wurden der gesetzlichen Realität in Deutschland angepasst, und in ein Opt-Out Verfahren umgewandelt. Um die Integration in die Platform zu ermöglichen, stellt das AISEC Anforderungen an die Entwicklung der Anfrageplattform sowie multipler "Privacy Proxy". Es wurden Anforderungen an die Anbindung der „Privacy Proxies“ an die existierenden Krebsregister Datenbanken (im speziellen KRRLP) gestellt. Die hohe Heterogenität der beteiligten Softwarekomponenten spiegelt sich in die Anforderungen an die zu entwickelnde Programmbibliotheken und Stub-Implementierungen des AISEC wieder. Neben den technischen Anforderungen an die Integrationskomponenten stellte das AISEC Anforderungen an die API's der jeweiligen Komponenten.

- Anforderungen an den benutzerzentrierten Zustimmungsmechanismus ("Web Anwendung"):

  Der benutzerzentrierte Zustimmungsmechanismus soll dem Patienten mit Hilfe der entwickelten kryptographische Zugriffsmethoden einen Datenschutz-freundlichen Mechanismus zum Teilen bzw. Unterbinden der persönlichen Daten zur Verfügung stellen. Hierzu wurden vom AISEC zunächst Anforderungen an den Identifikations bzw. Authentifizierungs-Mechanismus der Benutzer der "Web Anwendung" gestellt. Zunächst wurden die jeweiligen Benutzergruppen identifiziert und definiert. Zur Bereitstellung der Benutzerdaten muss wurden Anforderungen an eine externe Identifikations bzw. Authentifizierungsmöglichkeit von Patienten und Krebsforschern auf Basis OAuth2.0 gestellt.

- Um die Integration der „privacy-preserving Aggregation” der französischen Projektpartner voranzutreiben hat das AISEC Anforderungen an die zu integrierenden Komponenten in Kooperation mit EURECOM entwickelt. Die Anforderungen an ein Protokoll zur privatsphäre-schützenden Abfrage wurden erarbeitet. Die zur Schlüsselgenerierung und zur Berechnung der entsprechenden Werte benötigten Komponenten wurden angepasst und in die Gesamtarchitektur integriert. Eine Übersicht über die Integrationskomponenten mit entsprechenden Funktionsaufrufen ist in untenstehender Abbildung 1 zu sehen.

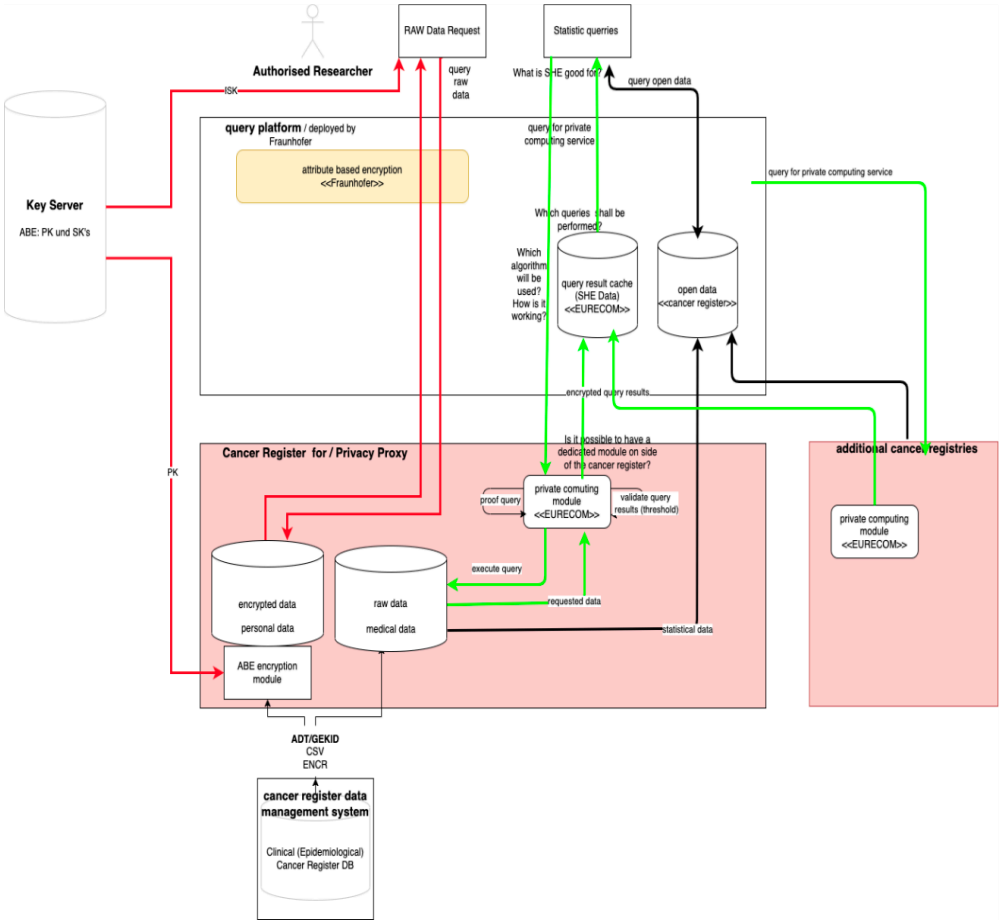


Abbildung 1) Gesamtarchitektur

Das AISEC beteiligte sich ebenfalls bei der Spezifikation weiterer funktionalen und Nicht-funktionale Anforderungen an die Gesamtarchitektur.

Das Krebsregister Rheinland-Pfalz spielte eine entscheidende Rolle bei der Spezifikation der Abfrageplattform. In Zusammenarbeit mit den Projektpartnern wurden die grundlegenden Anforderungen für UPCARE erarbeitet. Dies umfasste nicht nur die funktionalen Anforderungen, sondern auch eine detaillierte Betrachtung der nicht-funktionalen Anforderungen an die Gesamtarchitektur der Plattform.
Zunächst wurde gemeinsam definiert, welche funktionalen Anforderungen die Abfrageplattform erfüllen muss, um eine effiziente und sichere Abfrage sowie Analyse von Krebsregisterdaten zu ermöglichen. Dies beinhaltete unter anderem die Möglichkeit, aggregierte, pseudonymisierte und in bestimmten Fällen auch personenidentifizierende Daten abzufragen, dabei aber gleichzeitig die Privatsphäre der betroffenen Personen zu wahren. Ein wichtiger Bestandteil der Arbeit war auch die detaillierte Ausarbeitung der nicht-funktionalen Anforderungen. Diese umfassen eine Vielzahl von Aspekten, die die Leistungsfähigkeit, Sicherheit und Benutzbarkeit von UPCARE sicherstellen. In Zusammenarbeit mit den Projektpartnern wurden beispielsweise Anforderungen an die Performance der Plattform definiert, um sicherzustellen, dass die Abfrageprozesse schnell und effizient ablaufen, auch bei größeren Datenmengen und komplexen Anfragen. Dies war besonders wichtig, da die Plattform in der Lage sein muss, umfangreiche Datensätze in Echtzeit zu verarbeiten und den Forschenden schnell und zuverlässig Ergebnisse zu liefern.

Ein weiterer wichtiger Punkt war die Zuverlässigkeit und Verfügbarkeit der Plattform. Die Projektbeteiligten definierten, dass die Plattform eine hohe Verfügbarkeit gewährleisten muss, um den Forschungsprozessen jederzeit und ohne Unterbrechungen zur Verfügung zu stehen. In diesem Zusammenhang wurden auch Anforderungen an Redundanz und Fehlerbehandlung festgelegt, um Ausfalle oder Datenverlust zu vermeiden und die kontinuierliche Verfügbarkeit sicherzustellen.
Besondere Aufmerksamkeit galt den Sicherheitsanforderungen, da der Umgang mit hochsensiblen Gesundheitsdaten eine starke Absicherung gegen unbefugten Zugriff und Datenmissbrauch erfordert. Hier wurden spezifische Anforderungen an den Zugriffsschutz, die Daten Verschlüsselung mit ABE und HE und die Integrität der Daten formuliert. Dies sollte sicherstellen, dass die Plattform nicht nur die gesetzlichen Anforderungen zum Datenschutz erfüllt, sondern auch eine vertrauenswürdige und sichere Umgebung für die Durchführung von Forschungsanfragen bietet
Im Rahmen des UPCARE-Projekts wurde ein detailliertes Verständnis der Akteure und Ablaufe der Plattform entwickelt, evaluiert und systematisch dokumentiert. Dies umfasste nicht nur die technischen und funktionalen Aspekte der Plattform, sondern auch eine tiefgehende Analyse der Workflows der verschiedenen Akteure, insbesondere den Forschenden sowie weiterer relevanter Beteiligten wie administrativen Akteuren und Stakeholder. Ein besonderes Augenmerk lag dabei auf den praktischen und organisatorischen Abläufen, die in die tägliche Nutzung der Plattform einfließen.
In Zusammenarbeit mit den anderen Projektpartnern hat das Krebsregister Rheinland-Pfalz 39 High-Level-Anforderungen definiert, die die Basis für die Entwicklung der Abfrageplattform bildeten. Diese Anforderungen wurden gemeinsam mit den Projektpartnern iterativ erarbeitet und kontinuierlich validiert, um sicherzustellen, dass sie sowohl den funktionalen als auch den nicht-funktionalen Anforderungen der verschiedenen Akteure gerecht werden.
Das Krebsregister Rheinland-Pfalz brachte in diesem Prozess besonders seine Expertise in den Bereichen Datenhaltung und Schnittstellen ein. Mit seiner langjährigen Erfahrung in der Verwaltung und Analyse von onkologischen Daten war das Register in der Lage, fundierte Anforderungen an die Datenintegration und die Schnittstellen der Plattform zu formulieren. Dabei ging es darum, sicherzustellen, dass die Daten aus den verschiedenen Krebsregistern problemlos zusammengeführt und in einer sicheren, standardisierten Form abgefragt werden können.
Folgende Aspekte sind in Bezug auf die obigen Anforderungen zu berücksichtigen:

<u>Datenhoheit</u>
Im Rahmen des Projekts bleibt die Datenhoheit jederzeit vollständig bei den Krebsregistern. Das bedeutet, dass die Kontrolle und Verantwortung über die Daten weiterhin bei den jeweiligen Krebsregistern liegt, die diese Daten ursprünglich erfasst haben. Dies ist ein zentraler Aspekt, um sicherzustellen, dass die gesetzlichen Anforderungen an den Datenschutz und die Datenhoheit gewahrt bleiben, insbesondere im Hinblick auf die Sensibilität von onkologischen und personenbezogenen Daten.
UPCARE selbst speichert keine Daten dauerhaft. Sie fungiert vielmehr als ein zentraler Knotenpunkt, der die Anfragen für Daten entgegennimmt und verwaltet, jedoch keine der angefragten Daten direkt speichert. Stattdessen verzeichnet die Plattform lediglich, wo sich die angeforderten Daten befinden, und ermöglicht den sicheren Zugriff auf diese Daten durch die entsprechenden Akteure.

Die eigentliche Datenbereitstellung erfolgt durch die Krebsregister, die die angefragten Daten auf Abruf zur Verfügung stellen. Die Plattform stellt sicher, dass diese Bereitstellung auf eine sichere und datenschutzkonforme Weise erfolgt, aber die Verantwortung für die Pflege und Verfügbarkeit der Daten bleibt vollständig bei den Krebsregistern. Diese sind weiterhin für die Richtigkeit, Vollständigkeit und Aktualität der Daten verantwortlich und müssen sicherstellen, dass die Daten jederzeit in der benötigten Qualität zur Verfügung stehen.
Dieser Ansatz gewährleistet, dass die Krebsregister ihre Kontrolle über die Daten behalten und diese 1n Übereinstimmung mit den relevanten Datenschutzvorgaben verwalten können. Gleichzeitig ermöglicht er eine effiziente Nutzung der Daten für die Forschung, ohne dass die Krebsregister ihre Daten aus der eigenen Infrastruktur herausgeben oder die Verantwortung für die Datenverwaltung auf die Plattform übertragen müssen. Somit bleibt das Prinzip der Datenhoheit unberührt, was sowohl für die Register als auch für die Forschenden ein hohes Mars an Sicherheit und Vertrauen schafft.

Schnittstellen

Die Kommunikation zwischen der Plattform und den Krebsregistern erfolgt über standardisierte Schnittstellen, um einen sicheren, strukturierten und effizienten Austausch von Daten zu gewährleisten. Der FHIR-Standard (Fast Healthcare Interoperability Resources) wird als Grundlage für die Datenübertragung verwendet. Im Rahmen des Projekts wird dieser Standard umfassend evaluiert, um sicherzustellen, dass er den Anforderungen an Datensicherheit, Datenschutz und Interoperabilität entspricht.
FHIR ermöglicht es, verschiedene Gesundheitsdaten- sowohl aggregierte als auch pseudonymisierte Daten- in einem einheitlichen Format zwischen den beteiligten Systemen auszutauschen. Die Verwendung von FHIR tragt dazu bei, dass die Integration in die bestehende Infrastruktur der Krebsregister problemlos erfolgt und gleichzeitig die Datensicherheit sow1e der Schutz personenbezogener Informationen gewährleistet bleiben.

Datenmodell

Ein gemeinsames Datenmodell für alle angebundenen Krebsregister bildet die Grundlage der Plattform. Das OMOP CDM (Observational Medical Outcomes Partnership Common Data Model) wurde als potenzielles Modell mit den Projektpartnern diskutiert und evaluiert. Es sorgt für eine standardisierte und interoperable Struktur der onkologischen Daten, die es ermöglicht, diese effizient zu sammeln, zu speichern und für Forschungszwecke zu nutzen. OMOP CDM unterstutzt die Integration unterschiedlicher Datentypen und bietet eine flexible, skalierbare Losung, die an die spezifischen Anforderungen der Krebsregister angepasst werden kann. Dabei werden auch Datenschutz- und Sicherheitsanforderungen berucksichtigt.
Freigabeprozess
Einige Anfragen auf der Plattform können e1nen Freigabeprozess erfordern, insbesondere wenn sie den Zugriff auf personenbezogene Daten oder sensible Informationen betreffen. In solchen Fällen ist es notwendig, dass die zuständigen Akteure, wie beispielsweise die Patienten oder ihre gesetzlichen Vertreter, ihre Zustimmung zur Datenverwendung erteilen. Dieser Prozess wurde in der Anforderungsanalyse detailliert berücksichtigt, um sicherzustellen, dass alle relevanten rechtlichen und ethischen Anforderungen eingehalten werden.

Zugriffsberechtigungen

Zugriffsrechte und Identitäten auf der Plattform werden durch das Berechtigungssystem FIDES der Bundesdruckerei verwaltet, um den unbefugten Zugriff auf sensible Daten zu verhindern und sicherzustellen, dass nur autorisierte Akteure Zugang erhalten. Es stellt sicher, dass Benutzerrollen und-rechte exakt definiert und strikt eingehalten werden. Dies bedeutet, dass nur berechtigte Personen, auf die jeweiligen Daten zugreifen können- und dies nur im Umfang ihrer Befugnisse. Zu diesem Zweck werden fein granulare Steuerungsebenen implementiert, die es ermöglichen, spezifische Berechtigungen für unterschiedliche Datenzugriffe zu vergeben, sei es für die Anfrage, Bearbeitung oder Analyse von Daten. Es gewährleistet zudem eine vollständige Nachvollziehbarkeit von Zugriffen und Änderungen. Das Projekt fokussiert sich darauf, Forschenden einen sicheren und einfachen Zugang zu dezentralen Daten über eine zentrale Plattform zu ermöglichen.
Dies entspricht den im Projektantrag definierten Anwendungsfallen:

- Zugriff auf nicht-personalisierte Forschungsdaten: Forscher können anonymisierte Daten aus verschiedenen Organisationen abrufen, um statistische Analysen durchzufuhren, ohne die Privatsphäre der Patienten
zu gefährden.

- Zugriff auf personalisierte, pseudonymisierte Forschungsdaten: Forschende erhalten Zugang zu sensiblen Daten unter sicheren Bedingungen, um gezielte Studien oder klinische Forschung zu ermöglichen, wobei die Datenschutzanforderungen beachtet werden.

- Zugriff auf offene Daten über APIs: Offene Daten werden über standardisierte Schnittstellen bereitgestellt, was die Integration in Forschungssysteme und den breiten wissenschaftlichen Austausch
erleichtert.

2.1.3 AP1.3

Die Nutzbarkeit sowie Funktionalität der Gesamtarchitektur wurde vom KR RLP final auf auf Performanz und Effizienz hin getestet. Die Zeitersparnis des UPCARE Ansatzes im Vergleich zu anderen, etablierten Arbeitsabläufen und Methoden konnte hierbei überzeugen. Aus organisatorischen und rechtlichen Gründen ist ein produktiver Einsatz der UPCARE Plattform jedoch noch nicht möglich.

2.2 AP2 Architektur

2.2.1 AP2.1

Die Bundesdruckerei erstellte die Architektur der UPCARE-Plattform in Kooperation mit der Fraunhofer AISEC und dem Krebsregister RLP. Es sollte ein Architekturansatz entstehen, der die bereits existierende Daten-Infrastruktur sowie die Arbeitsabläufe des Krebsregisters RLP berücksichtigt und bestmöglich integriert. Die Architektur wurde insbesondere unter Berücksichtigung der in AP1 definierten Anforderungen entwickelt.
Die Bundesdruckerei hat ein einheitliches Anfrageformat FHIR für die Datensuche, Selektion und Analyse definiert. Sie hat das Authentifizierungs- und Berechtigungskonzept für den sicheren Zugriff auf Anfragefunktionen inklusive API beschrieben. Die API-Spezifikation wurde

für die Zugriffe auf mehrere Krebsregister erweitert. Beispiel-Authentifizierungsanfragen für Identity Management System (IDMS) und Datenzugriffsanfragen für mehrere Knowledge Datenbanken (KDBs) wurden implementiert und als Postman-Collection an das Fraunhofer AISEC geliefert. Das Fraunhofer AISEC hat diese Schnittstelle in die Gesamtarchitektur integriert und somit den Zugriff auf Krebsregisterdaten ermöglicht.
Das Krebsregister Rheinland-Pfalz brachte in dieser Phase seine Expertise im Umgang mit onkologischen Daten ein. Besonders wichtig war es, ein tiefgehendes Verständnis dafür zu entwickeln, wie onkologische Daten sicher erfasst, effizient verteilt und zuverlässig genutzt werden können.

2.2.2 AP2.2

Die Bundesdruckerei hat die Krebsregisterdatenbank, in Form von der FHIR-basierten Cortex Datenbank, vollständig implementiert und als WEB-Service zur Verfügung gestellt. Als Testdaten wurden synthetisierte, medizinische Daten verwendet. Die Testdaten wurden auf 2 unabhängigen Cortex-Datenbank-Instanzen aufgeteilt. Mit Hilfe von mehreren Instanzen können Anfragen an mehrere Krebsregister prototypisch dargestellt werden. Die Schnittstellen für die Integration weiterer Module, die die Datenverarbeitungs-, Verschlüsselungs- und Anonymisierungsfunktionen wurden bereitgestellt. Im Anschluss hat das Fraunhofer AISEC die Teilkomponente “ Krebsregisterdatenbank“ in die Gesamtarchitektur integriert.

2.2.3 AP2.3

Die API für die Integration weiterer Module, die die Datenverarbeitungs-, Verschlüsselung- und Anonymisierungsfunktionen wurden bereitgestellt. Die Anfrageplattform wurde erfolgreich mit ABE- und HE- Modulen integriert. Ein Datenfluss von der Anfrageplattform über die Krypto Module der Privacy Proxy, Query Plattform zum Demonstrator-GUI wurde getestet. Alle Use Cases wurden durch Tests abgedeckt

2.2.4 AP2.4

Die Anfrageplattform und API wurden hinsichtlich in AP1 zwei definierter Szenarien evaluiert. Die Bundesdruckerei und das Fraunhofer AISEC unterstützte das KR RLP bei der Nutzung der Anfrageplattform dabei, den anonymisierten Zugriff bzw. den Zugriff durch den Patienten zu evaluieren.

2.3 AP3 Private Computing Modul

Das Fraunhofer AISEC stimmte sich mit EURECOM über die möglichen Anknüpfungspunkte und gemeinsame Komponenten sowie Schnittstellen ab. Hierbei wurden im Rahmen der angesetzten Meetings zunächst detaillierte Informationen über die zu entwickelnden Komponenten gegenseitig ausgetauscht. Die Ergebnisse flossen insbesondere auch in das AP1 bzw. AP2 bzw. in die Gesamtarchitektur mit ein. Der größte Teil der Entwicklung des HE-Moduls fand bei EURECOM statt.

2.3.1 AP3.1

Die Anfrageplattform API wurden für „Private Computation“-Modul von EURECOM für den Zugriff auf mehrere Cortex-Datenbank-Instanzen angepasst. Das "Private Computing”-Modul beinhaltet homomorphe Verschlüsselungs-Module sowie weitere DP-Module. Zusätzlich wurden alle Schnittstellen des “Private Computation”-Moduls definiert, welches den Informationsfluss in Form von verschlüsselten Daten der Krebsregister DBs erlaubt. Stub Implementierung für sämtliche konzipierten Prozessen, Funktionen und Schnittstellen wurde mit dem Ziel der Integration der Bibliothek in die Plattform abgeschlossen.
Statt einer ursprünglich geplanten Integration des ABE-Moduls mit den "Private Computing"-Komponenten von EURECOM mittels eines FFI-Interfaces wurden REST-APIs definiert und implementiert. Die Integration der Module sowohl im Privacy Proxy als auch der Plattform wurde dadurch stark erleichtert.

2.3.2 AP3.2

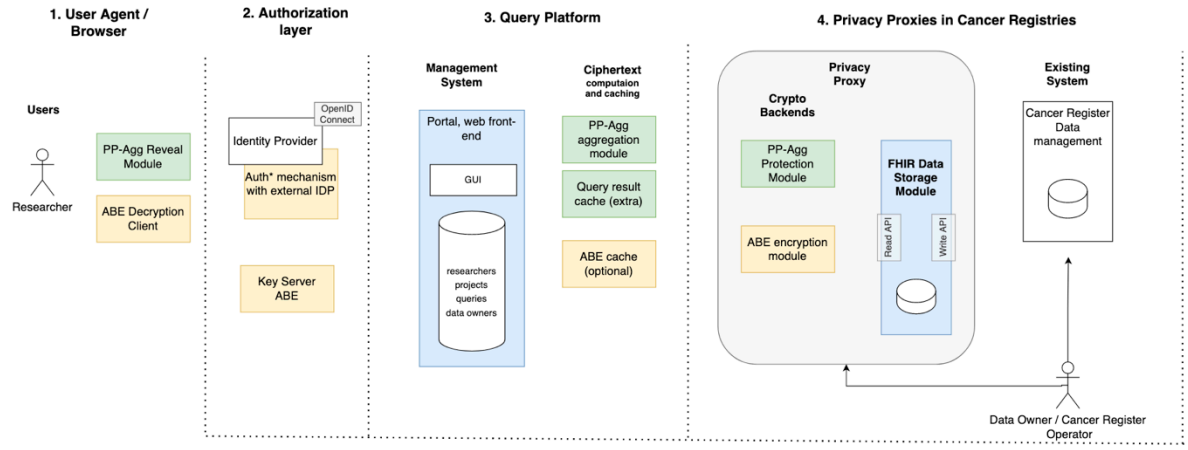
Die Anfrageplattform wurde für Anfragen von „Private Computation“-Modul erfolgreich hinsichtlich des Datenschutzes, der Leistung und des Nutzens evaluiert. Alle notwendigen Daten wurden unter Berücksichtigung des Datenschutzes und der Nutzerrechten geliefert. Da die Verwendung aufwendiger kryptografischer Techniken wie der homomorphen Verschlüsselung von Natur aus zusätzliche Leistungsanforderungen in Bezug auf Berechnung, Speicher und Bandbreite verursacht, wurden die neu entwickelten Module optimiert, um einen solchen Overhead zu kompensieren oder zu minimieren.

2.4 AP4 Zugrifsskontroll Modul

Aufgrund von Verzögerungen bei Projektstart musste die erste Phase, in welcher die rechtlichen, technischen und vor allem die organisatorischen Anforderungen an ein solches Zugriffskontrollkonzept analysiert werden sollten, verkürzt werden.

2.4.1 AP4.1

In der darauffolgenden zweiten Phase wurde vom Fraunhofer AISEC das Konzept zur Zugriffskontrolle mittels ABE erstellt. Die Architektur der kryptografischen Zugriffskontrolle wurde in die Gesamtarchitektur integriert. Dabei hat sich die Bundesdruckerei mit dem Fraunhofer AISEC als auch mit den anderen Partnern regelmäßig abgestimmt.
Es wurde eine API für benutzerbezogene Verwaltung von Zugriffsrechten auf dem Keyserver implementiert, inklusive dazu gehöriger grafischer Interfaces zu Demonstrationszwecken.
Es wurde weiter die Zugriffskontrollarchitektur verfeinert, deren aktuelle und finale Ausprägung im folgenden Schaubild zu finden ist:



2.4.2 AP4.2

Die Zugriffskontrollarchitektur wurde kontinuierlich mit den Anforderungen der Anwendungsfälle abgeglichen und entsprechend angepasst. Dabei hat sich das Fraunhofer AISEC mit dem Krebsregister RLP als auch mit den anderen Partnern regelmäßig abgestimmt.
Es wurde eine API für benutzerbezogene Verwaltung von Zugriffsrechten auf dem Keyserver implementiert, inklusive der dazugehörigen grafischen Interfaces. Dabei entstand eine Web-Anwendung auf Svelte-Basis (https://svelte.dev/), welche die Nutzer gerichtete Anwendungskomponente der UPCARE-Plattform darstellt.
Die APIs sind mittels "Swagger" spezifiziert, was eine automatische Dokumentation dieser impliziert. Weiterhin erlaubt es diese Spezifikation einfach neue (Web)-Anwendungen für diese APIs zu entwickeln.

2.4.3 AP4.3

Um eine Zugriffskontrolle zum Zeitpunkt der Entschlüsselung zu ermöglichen, wurde als Zugriffskontroll-Schema ein KP-ABE Schema festgelegt. Nach der Evaluierung mehrere KP-ABE Schemata, wurde das effizienteste Schema ausgewählt und integriert. Attribute werden im Schema als Strings so kodiert, dass sie eindeutig einen bestimmten Schlüsselwert innerhalb der Patienten-Stammdaten des FHIR-Datenmodells referenzieren (statt ADT/GEKID).
Die Werte der entsprechenden Attribute werden bei der Verschlüsselung des Patienten Datensatzes (innerhalb des "Privacy Proxy") dem jeweiligen Patientenstamm Datensatz entnommen und als Attribut-Werte Paar im zu generierenden Chiffrat hinterlegt.
Zusätzlich zu den abgeleiteten Attributen vom onkologischen Basisdatensatz bestimmte das AISEC Projektspezifische Attribute, wie beispielsweise ein Attribut für den "Vollzugriff“ auf alle Datensätze. Eine Implementierung des Keyservers im Rahmen des Demonstrators wurde erstellt und ist in der finalen Ausprägung des Demonstrators im Einsatz. Auch die Implementierung des ABE-Moduls ist nun final im Privacy-Proxy integriert.

2.4.4 AP4.4

Die entwickelte Zugriffskontrolle wurde auf die Anforderungen aus AP1 evaluiert. Es wurden einige Anpassungen für Zugriff aus mehreren Datenbanken spezifiziert. Die notwendigen Anpassungen bei Implementierung wurden durchgeführt.

2.5 AP5 Use Cases

Die User Stories wurden primär vom Krebsregister RLP und der Bundesdruckerei GmbH im Anschluss an die Anforderungen (AP1) erarbeitet. Von der Bundesdruckerei wurde ein gemeinsames Vokabular ("Dictionary") sowie eine gemeinsame Wissensgrundlage ("Knowledge Base") im Bereich Privacy-Enhancing Technologies (PET) erarbeitet, welches zur besseren Verständlichkeit bei der gemeinsamen Kommunikation unter allen beteiligten Projektpartnern betragen sollte.
Das Krebsregister Rheinland-Pfalz spielte eine zentrale Rolle bei der Entwicklung der Use Cases im Rahmen des Projekts. Zusammen mit den Projektpartnern wurden die Use Cases detailliert ausgearbeitet und auf die spezifischen Anforderungen des Demonstrators abgestimmt, um die geplanten Funktionalitäten und Szenarien realistisch abzubilden. Dabei wurde besonderer Wert daraufgelegt, dass sowohl die Attributbasierte Verschlüsselung (ABE) als auch die Homomorphe Verschlüsselung (HE) in den Demonstrator integriert und durch konkrete Use Cases praktisch umgesetzt wurden. Diese Use Cases dienten nicht nur der Veranschaulichung der technischen Machbarkeit der Verschlüsselungstechniken, sondern auch der praktischen Erprobung ihrer Anwendung im Kontext der Datenverarbeitung und-sicherheit.
Bei der Gestaltung der abzurufenden Daten orientierte sich das Projektteam an den im Krebsregister vorhandenen Daten, die auf dem onkologischen Basisdatensatz7 basieren. Diese Daten bilden die Grundlage für die Use Cases und spiegeln die realen Anforderungen der Forschung wider. In Kombination mit der Expertise des Instituts im Bereich der Anfragen zu Forschungsdaten sowie der Analyse und Auswertung von onkologischen Daten wurden die Use Cases gezielt definiert. Im Anschluss daran wurden diese im Demonstrator getestet, um sicherzustellen, dass die praktischen Anforderungen und Szenarien effizient und sicher umgesetzt werden können.

2.5.1 AP5.1

Auf der Grundlage des ersten definierten Anwendungsfalles, basierend auf Szenario 1, welcher die praktischen Herausforderungen bei der Datenschutzgerechten Abfrage von persönlichen Daten aus den Krebsregistern widerspiegeln, wurden für den Demonstrator verschiedene Beispielabfragen von Krebsforschern, welche auf den Beispielabfragen basieren, erarbeitet:

Use case 1: Attribute-based encryption / cryptographic access control.

- There are two CR attached. Represented by 2 instances of a database/privacy proxy.
- Actors:
    - Alice (Novartizz Research)
    - Bob (Fyzer Research)
    - Access policy:
        - Alice: Access to all relevant attributes: CTYPE, DDATE, HOSPITAL, NAME, ADDRESS, DOB, WEIGHT, HEIGHT, SYMPTOMS, PRESCRIPTION
        - Bob: Access to clinical data: CTYPE, DDATE, HOSPITAL, NAME, ADDRESS, DOB, WEIGHT, HEIGHT, SYMPTOMS, PRESCRIPTION
    - Story Alice:
        - Alice is a researcher at Novartizz and proposes a research project to contact patients (NAME, ADDRESS) with a specific cancer from a specific region close to her (HOSPITAL) to test a new treatment. She

wants to do this using the UPCARE platform and reqests access to data of patients with a specific cancer type (CTYPE=<todo>). The data she wants to investigate are (see Access policy).
        - She now makes a query for the cancer she is interested in (Observation.valueCodeableConcept.code) in that have been discovered between (effectiveDateTime) and (effectiveDateTime) (e.g. 2016 and 2020) in a specific hospital (Encounter.serviceProvider.display) over all CRs (Both KDBs)(she does not know which CR is responsible for patients of HOSPITAL).
        - When the query is processed and results are available, the patient data is displayed to Alice.
        - Alice exports this data (e.g. Plain text containing FHIR or PDF) for use outside of UPCARE in her lab. END.
    - Story Bob:
        - Bob is a researcher at Fyzer and proposes a research project to collect and prepare relevant information on this cancer and its SYMPTOMS/PRESCRIPTIONS for government officials/policy makers. He wants to do this using the UPCARE platform and reqests access to data of patients with a specific cancer type (CTYPE=<todo>).
        - He now makes a query for the cancer she is interested in (CTYPE) in that have been discovered between DATE_0 and DATE_1 (e.g. 2016 and 2020) in a specific hospital (HOSPITAL) over all CRs (she does not know which CR is responsible for patients of HOSPITAL).
        - When the query is processed and results are available, the patient data is displayed to Alice. Data she has no access to is indicated (e.g. “restricted”), data that does not exist is also indicated (e.g. “no data”). Observe how the readable data differs from Alice’s session.
        - Finally, Bob exports this data (e.g. Plain text containing FHIR or PDF) for use outside of UPCARE in his lab. END.
    - Access policy:
        - Alice: Access to all relevant attributes: CTYPE (=”ICD Code”, “SNOMED”), DDATE (=”Tumor Diagnosedatum”), NAME, ADDRESS, DOB, GENDER, SUBSTANCES/MEDICATION (=”Systemische Therapie Substanzen”), OPS
        - Bob: Access to clinical data: CTYPE, DDATE, NAME, ADDRESS, DOB, GENDER, SUBSTANCES/MEDICATION, OPS (Operation-code or equivalent)
        - User consent: We assume (as implemented in German law, for example) that patient consent to data access is already given prior to the data access. ▪ _Reporting of patient data to CRs is mandatory (in Germany) and does not involve patient consent.
        - Using the patient data in the CRs (by researchers) does require (among other things) consent by patients? How does a researcher reach out to patients?
        - Precondition: Research project/context has user consent (e.g. user interacted with plattform to give this consent, not implemented, very complicated, future work). “consent management in cancer research“

2.5.2 AP5.2

Auf der Grundlage des zweiten definierten Anwendungsfalles, basierend auf Szenario 2, welcher die praktischen Herausforderungen bei der Datenschutzgerechten statistischen Abfrage von Daten aus den Krebsregistern widerspiegeln, wurden für den Demonstrator verschiedene Beispielabfragen von Krebsforschern, welche auf den Beispielabfragen basieren, erarbeitet:

Use-case 2: Fully-homomorphic encryption / statistical analysis

- There are two CR attached. Represented by 2 instances of a database/privacy proxy.
- Actors:
    - Charlie (Fyzer Research)
- User consent: We assume (as implemented in German law, for example) that user consent to data access is already given prior to the data access.
- Story Charlie

- Charlie is a researcher at Fizer and proposes a research project to find for specific cancer tumor type (CTYPE="Breast cancer = C-50.1", SNOMED) of a size between X and Y in millimeters over a five year period. He is interested if the average age (of the patient) in recent years has lowered, and the rate of recurrence or relapsing cases has increased. He wants to do this using the UPCARE platform and uses the statistic query feature. (Open Data Research feature).
- In order to propose the research project, he logs into UPCARE (we assume he is already registered and accredited as researcher in the UPCARE platform).
- He now makes one or more queries for the cancer he is interested in with sizes between X and Y and diagnosis year from YEAR to YEAR + 5 and requests the respective statistical queries (AVG TUMOR SIZE and SUM RELAPSED (Recurrence)) over all CRs.
- When the query is processed and results are available, the result data is displayed to Charlie (maybe multiple successive query outputs can be visualized in a diagram).
- Finally, Charlie exports the datapoints (e.g. Plain text containing FHIR or PDF) for use outside of UPCARE in her lab. END.

2.5.3 AP5.3

Die Erstellung eines finalen Demonstrators wurde erfolgreich abgeschlossen. Alle Anforderungen und Kommentare der Endnutzer wurden berücksichtigt. Die Arbeitsszenarien wurden mit Testdaten erprobt und einer Expertengruppe von potenziellen Nutzern vorgestellt. Die beiden Anwendungsfälle wurden aus der Perspektive des KR RLP hinsichtlich der folgenden Aspekte bewertet:

<u>Datenschutz und Datensicherheit</u>

Auch bei aggregierten Daten besteht immer ein gewisses Risiko, Ruckschlusse auf einzelne Personen zu ziehen. Verschiedene Faktoren, wie die Einzigartigkeit bestimmter Merkmalskombinationen sow1e zeitliche und räumliche Informationen, erhöhen das Potenzial einer Re-Identifikation. Dabei spielt auch externes Wissen, das öffentlich oder nicht-öffentlich zuganglich ist, eine Rolle, ebenso wie andere Einflussfaktoren.

Durch den Einsatz homomorpher Verschlüsselung (HE) können Daten sicher aggregiert werden, ohne dass individuelle Patientendaten offengelegt werden. Die verschlüsselten und aggregierten Daten lassen sich weiterhin analysieren, um allgemeine Muster und Statistiken zu identifizieren, wodurch das Risiko einer Re- Identifikation bestimmter Falle reduziert wird. Aus der Perspektive eines Krebsregisters stellt dies e1nen wichtigen Fortschritt 1m Schutz der Patientendaten dar.
Die Attributbasierte Verschlüsselung (ABE) ermöglicht es dem Krebsregister, ein standardisiertes Konzept für Datenschutz und Datensicherheit bei der Bereitstellung personenbezogener Patientendaten für Forschungszwecke zu entwickeln. Krebsregister, die mit UPCARE verbunden sind, müssen nicht mehr auf individuelle Lösungen zur sicheren Bereitstellung von Patientendaten zurückgreifen. Durch die Verwendung von Zugriffsberechtigungen und Delegationsregeln kann der gesamte Prozess- von der Anfrage bis zur Bereitstellung der Daten- auf der Plattform standardisiert werden, dabei immer in Übereinstimmung mit den geltenden Datenschutzvorschriften.
Zugänglichkeit
UPCARE ermöglicht Forschenden einen unkomplizierten und sicheren Zugang zu einer Vielzahl von Krebsdaten. Über eine benutzerfreundliche Weboberflache ist die Plattform jederzeit zuganglich und bietet eine zentrale Schnittstelle, über die Daten sicher aus den angeschlossenen Krebsregistern abgerufen werden können. Während Forschende bisher die Daten bei jedem Krebsregister einzeln anfordern mussten, entfallt dieser administrative Aufwand nun durch die zentrale Plattform.

Machbarkeit
UPCARE ermöglicht eine schnelle Vorab-Prüfung, ob ausreichend Patientendaten für eine Studie verfügbar sind. Antragsstellende geben die relevanten Merkmale der Anfrage an und erhalt ein aggregiertes Ergebnis, das beispielsweise die Anzahl der Patienten und Patientinnen sowie deren Geschlecht und Alter umfasst. Wenn dieses Ergebnis ausreicht, um eine Kohorte zu bilden, können Antragsstellende die Patientendaten direkt über die Plattform bei den ausgewählten Krebsregistern anfordern. So lasst sich zugig beurteilen, ob eine Studie mit den verfügbaren Daten durchfuhrbar ist, ohne jedes Krebsregister einzeln kontaktieren zu müssen. Durch die Vernetzung der Krebsregister besteht zudem eine hohe Wahrscheinlichkeit, auch bei seltenen Tumoren genügend Daten zu sammeln.

Interoperabilität
Für die Kommunikation zwischen UPCARE und den Krebsregistern wurde HL7 FHIR4 als Standard gewählt. Die FHIR-Implementierung basiert derzeit auf FHIR- Ressourcen, die von Synthea8 generiert wurden. Synthea ist ein Generator für synthetische, aber realistische Gesundheitsdaten. Diese Lösung ist für den UPCARE-Demonstrator ausreichend, jedoch werden zukünftig spezifische FHIR- Profile entwickelt werden müssen, um die Anforderungen der UPCARE- Implementierung zu erfüllen und gegebenenfalls notwendige Erweiterungen oder Einschränkungen vorzunehmen.
Prozessstandardisierung
Aktuell stellt die Beantragung personenbezogener medizinischer Daten e1nen komplexen Prozess für Antragsstellende dar. Durch die Einführung der Plattform kann dieser Ablauf für die Anforderung und Bereitstellung von Patientendaten standardisiert und vereinfacht werden.

Datenhoheit

Die Daten verbleiben jederzeit in den Datenbanken der Krebsregister. Die Plattform dient lediglich als zentrale, sichere Instanz zur Anfrage von Daten, während die Krebsregister weiterhin die Datenquelle bleiben und für deren Pflege und Verfügbarkeit verantwortlich sind.

Sichtbarkeit

Krebsregister haben die Möglichkeit, ihre Daten an einem zentralen Ort sichtbar zu machen. Besonders kleinere Krebsregister profitieren von dieser Möglichkeit, da sie ihre Sichtbarkeit und Reichweite erhöhen können. In der Theorie konnte UPCARE zu einem umfassenden Katalog aller Krebsregister innerhalb der EU werden, der nicht nur die Daten, sondern auch Informationen zu den einzelnen Registern bereitstellt.

Eine grafische Abbildung der internen Protokolle beider Use Cases ist in Abbildung 5 und 6 gegeben. Eine grafische Abbildung der entwickelten grafischen Benutzeroberfläche für die Benutzer des Demonstrators ist in Abbildung 7 bis 9 gegeben.

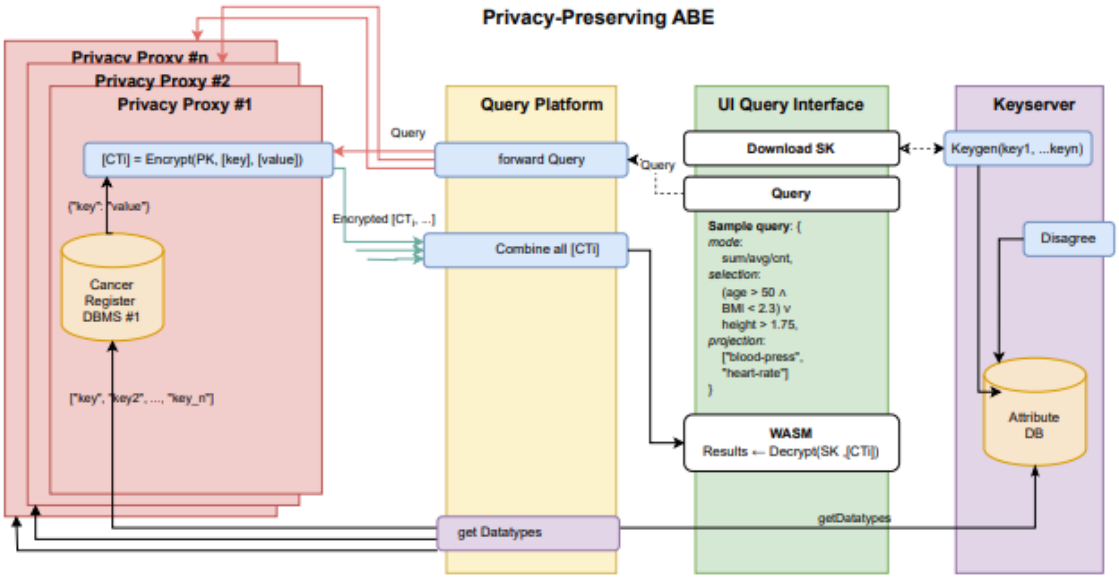


Abbildung 5) Use Case 2

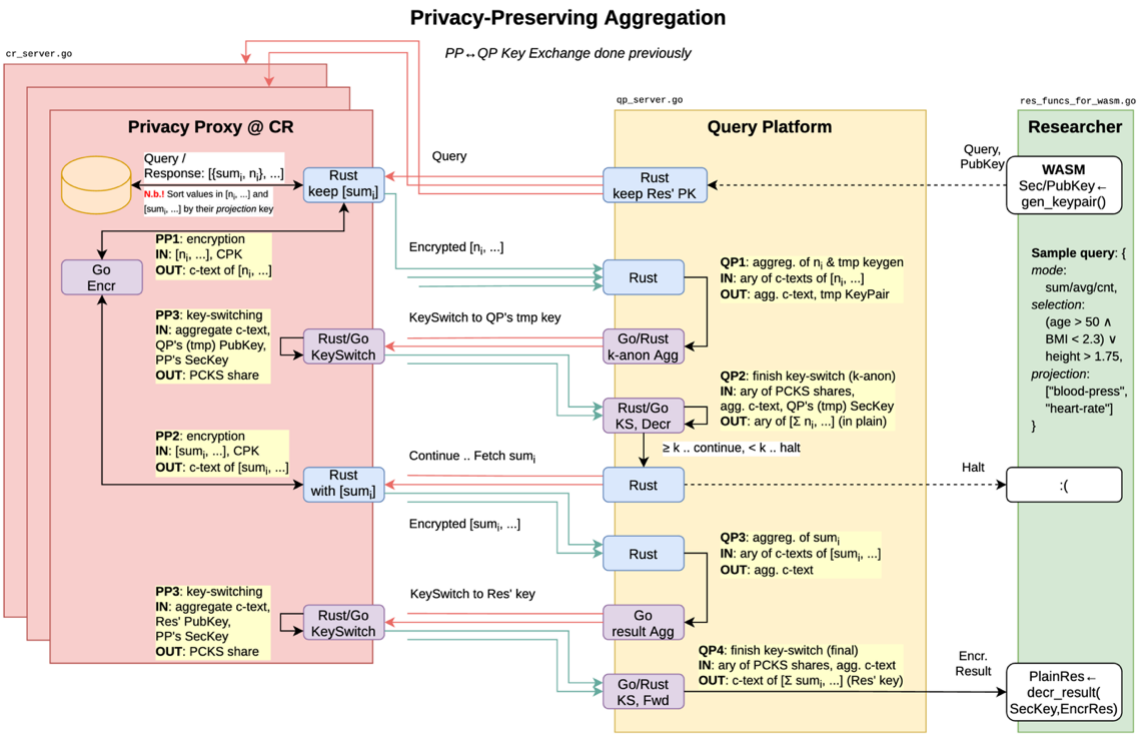


Abbildung 6) Use Case 2

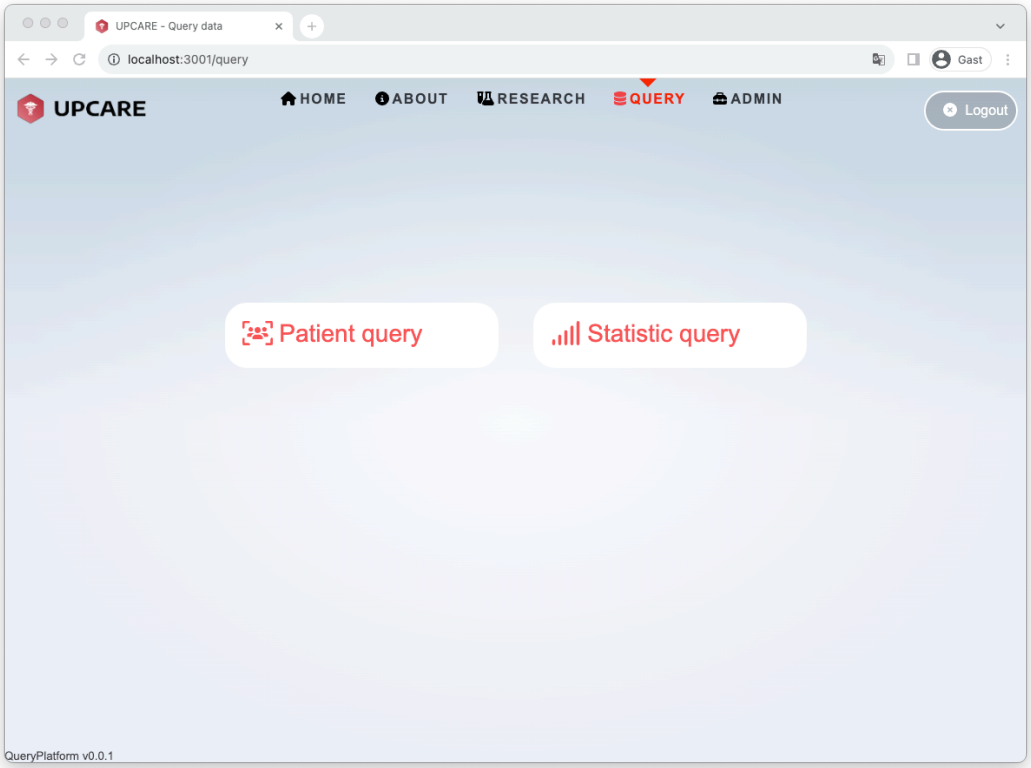


Abbildung 8 (Use Case Übersicht)

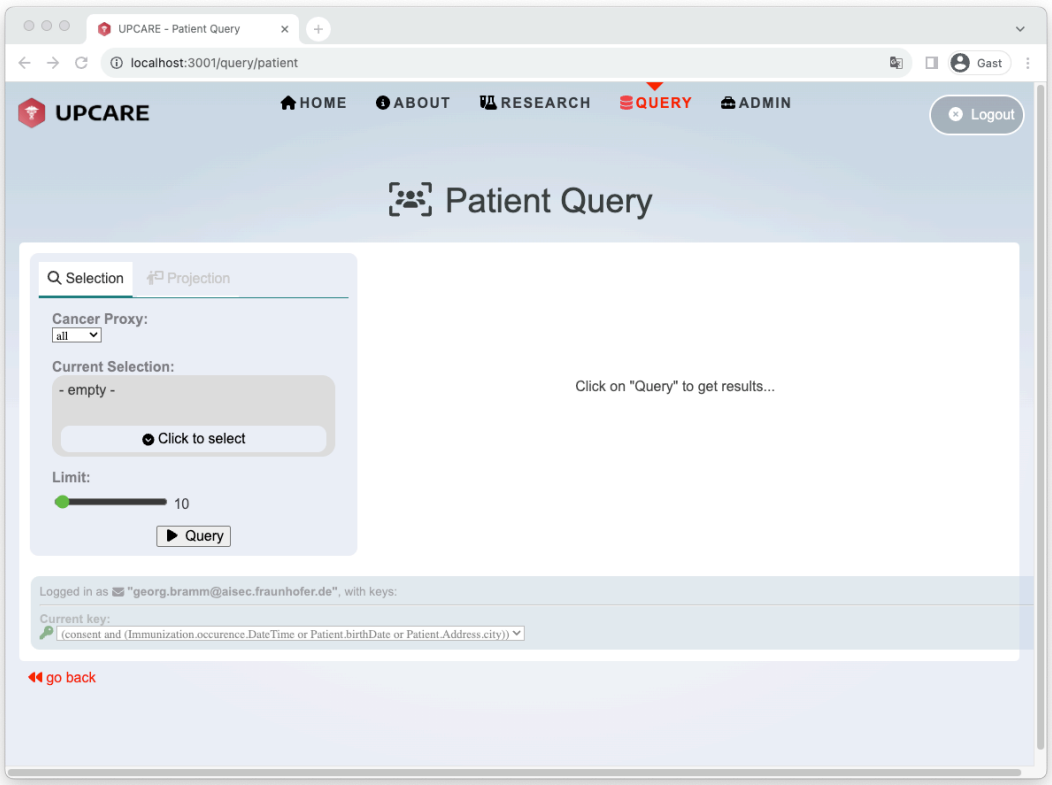


Abbildung 9 (Use Case 1)

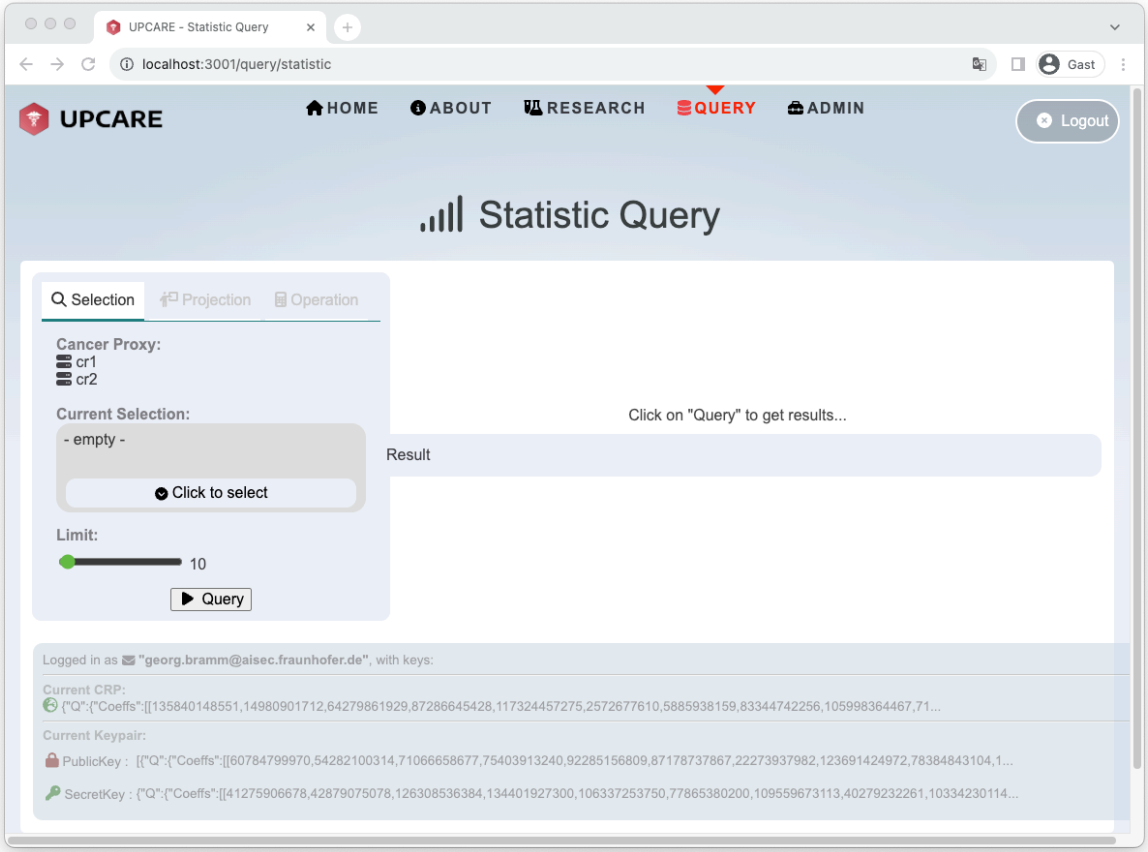


Abbildung 10 (Use Case 2)

UPCARE stellt einen bedeutenden Fortschritt im Bereich der Bereitstellung von Forschungsdaten dar, wobei sie die Datensicherheit gewährleistet und gleichzeitig eine kollaborative Datenanalyse fordert. Durch die Integration fortschrittlicher kryptografischer Techniken w1e der attributbasierten Verschlüsselung (ABE) und der homomorphen Verschlüsselung (HE) stellt UPCARE sicher, dass sensible Gesundheitsdaten während des gesamten Forschungsprozesses vertraulich und sicher bleiben. Die feingranulare Zugriffskontrolle, die durch attributbasierte Verschlüsselung ermöglicht wird, gibt den Patienten und Patientinnen die Kontrolle über ihre Daten, während die homomorphe Verschlüsselung sichere und private Berechnungen auf verschlüsselten Daten ermöglicht und die individuelle Privatsphäre schützt. Darüber hinaus verbessern die Automatisierung der Datenverarbeitung und der Einsatz von Kryptografie nicht nur den Datenschutz, sondern beschleunigen auch den Prozess von Datenanforderungen und-analysen, was zu schnelleren Erkenntnissen und Entdeckungen in der Krebsforschung fuhrt. Auf diese Weise werden datenschutzfreundliche Analysemethoden entwickelt und in die Architektur von Krebsregistern integriert, die einerseits ein hohes Niveau an Datenschutz gewährleisten und andererseits bedeutende Ergebnisse für die Krebsforschung liefern. In Zukunft konnte UPCARE als Vorreiter für die verschlüsselte Bereitstellung von Forschungsdaten über eine zentrale Plattform dienen.
insgesamt stellt UPCARE e1nen bedeutenden Fortschritt in der sicheren und effizienten Bereitstellung von Krebsdaten dar, indem es die Anforderungen der Forschung und des Datenschutzes in Einklang bringt. Für das Krebsregister
bedeutet dies nicht nur eine verbesserte technische Infrastruktur, sondern auch eine Erhöhung der Sichtbarkeit und Zugänglichkeit der eigenen Daten im Forschungsumfeld, ohne die Kontrolle über diese Daten zu verlieren. Auf diese Weise werden datenschutzfreundliche Analysemethoden entwickelt und in die Architektur von Krebsregistern integriert, die einerseits ein hohes Niveau an Datenschutz gewährleisten und andererseits bedeutende Ergebnisse für die Krebsforschung liefern. In Zukunft konnte UPCARE als Vorreiter für die verschlüsselte Bereitstellung von Forschungsdaten über eine zentrale Plattform dienen.

2.6 AP6 Management

Das Fraunhofer AISEC nahm regelmäßig an den angesetzten Telefonkonferenzen der internationalen Partner teil. Diese fanden in der Regel monatlich statt.
Für die Entwicklungstätigkeiten im Rahmen des Projektes setzte das Fraunhofer AISEC ein Quellcodeverwaltungssystem (git) auf. Dieses wurde weiterhin in eine Continuous-Integration-Lösung eingebunden, um reibungsloses Testen und Entwickeln zu gewährleisten.
Das Fraunhofer AISEC nahm weiterhin an den folgenden Konsortialtreffen teil:

- 15.06.2021 Kick-off-Meeting des Deutsch-französischen Projektes (Virtuell)
- 06.09.2021 UPCARE Kick-off-Meeting (Virtuell)
- 07.04.2022 – 08.04.2022 Konsortialtreffen (EURECOM, Nizza)
- 13.10.2022 – 14.10.2022 Konsortialtreffen (Fraunhofer AISEC, München)
- 14.09.2023 – 15.09.2023 Konsortialtreffen (Bundesdruckerei GmbH, Berlin)
- 27.02.2024 – 28.02.2024 Konsortialtreffen (SOFTEAM, Paris)
- 05.05.2024 – 06.05.2024 Konsortialtreffen (KR RPL, Mainz)

Die Konsortialtreffen wurden dazu genutzt, Zwischenergebnisse zu präsentieren und eingehend zu diskutieren. Weiterhin wurden finale Architekturentscheidungen getroffen. Weiterhin gab es wiederkehrende virtuelle Termine in Form von zweiwöchentlichen Treffen mit den deutschen und monatlichen Treffen mit allen Projektpartnern.
Das Fraunhofer AISEC hat das Projekt und die entwickelten Technologien in diversen internen Workshops und Präsentationen vorgestellt und laufend diskutiert.

2.6.1 Präsentation des Projekts auf diversen Veranstaltungen

Das Projekt wurde auf den folgenden Veranstaltungen präsentiert:

- 14.03.2023 - 15.3.2023 Nationale Konferenz IT-Sicherheitsforschung, Berlin
- 23.03.2023 CARE REGIO (https://care-regio.de/amf/programm/), Kempten
- 12.05.2023 - 13.05.2023 New Ideas for Medicine (NIM) 8. Virtual Symposium, School of Medicine
- 08.07.2024- 10.07.2024 SECRYPT24, The International Conference on Security and Cryptography 2024, Dijon, FRANKREICH

2.6.2 Publikationen

Bramm, Georg, et al. "UPCARE: User Privacy-preserving Cancer Research Platform." SECRYPT 2024, 21st International Conference on Security and Cryptography. 2024.

2.6.3 Interne Veranstaltungen

Fraunhofer AISEC und die Bundesdruckerei GmbH haben das UPCARE-Projekt und die entwickelten Technologien in diversen internen Workshops und Präsentationen vorgestellt und laufend diskutiert.

UPCARE-Kurzbericht 2024

1. Übersicht und Kurzdarstellung

In Krebsregistern sammeln, speichern und analysieren medizinische Einrichtungen die Krankheitsdaten von Krebspatientinnen und-patienten, damit Forschende die Wirksamkeit von Therapien bewerten und Faktoren untersuchen können, die bestimmte Krebsarten beeinflussen. Die aktuelle Datenverarbeitungsarchitektur von Krebsregistern in Deutschland und Frankreich wurde jedoch zu Zeiten etabliert, als weder der Datenschutz auf dem heutigen Niveau war, noch mobile Apps und Cloud-Dienste existierten. Durch die konstante Weiterentwicklung der Gesetzgebung in Deutschland und Europa wurden seitdem Datenschutzanforderungen konkretisiert und gleichzeitig die Befugnisse der Krebsregister in Bezug auf die Datenanalyse erweitert. Krebsregister stehen somit vor der Herausforderung, detaillierte Datenanalysen in einem sich entwickelnden Markt für mobile Apps und Cloud-Dienste zu unterstützen und gleichzeitig wichtige persönliche und gesundheitsbezogene Daten zu schützen. Aktuell sind Krebsregister immer noch meist als isolierte Datenspeicher organisiert. Krebsforschenden ist es trotz des Rückgriffs auf standardisierte Datenformate dadurch nicht möglich, mehr als ein einzelnes Register gleichzeitig datenschutzkonform abzufragen.

1.1 Zielsetzung des Projekts

Das Projekt „User-Centric and Privacy-Preserving Cancer Research Platform“ (UPCARE) zielt darauf ab, eine moderne, grenzübergreifende deutsch-französische Plattform für die Abfrage von Krebsregistern zu schaffen, die geltende Datenschutzstandards berücksichtigt. Es erforscht, wie zum Beispiel registerübergreifende Anfragen aus Deutschland und Frankreich ermöglicht werden können. Zudem soll ein autorisierter Kreis von Nutzerinnen und Nutzern Daten für weitreichendere Analysen verwenden können. Zum Schutz der Daten werden hierbei verschiedene Verschlüsselungsverfahren und weitere Schutzmechanismen eingesetzt, die einen zweckgebundenen Zugriff auf die Daten sicherstellen. Auf diese Weise werden datenschutzfreundliche Analysemethoden entwickelt und beispielhaft in die Architektur eines ausgewählten Krebsregisters integriert, was einerseits ein hohes Datenschutzniveau verspricht, und andererseits aussagekräftige Erkenntnisse für die Krebsforschung ermöglicht.

Die Entwicklungen des Projekts trug dazu bei, die derzeitige Isolation der einzelnen Krebsregisterdatenbanken zu minimieren. Langfristig kann so eine multinationale Krebsforschungsplattform aufgebaut werden, die es Forschenden erlaubt, europaweite Studien durchzuführen und die dazu beiträgt, die Qualität der Krebsforschung nachhaltig zu verbessern. Gleichzeitig bleiben durch die Datenschutzmaßnahmen die Autonomie der einzelnen Krebsregister sowie der Schutz der Privatsphäre der Patientinnen und Patienten gewahrt. Übergeordnet wurde so exemplarisch gezeigt, dass die weitreichende Nutzung und Analyse von sensiblen Daten mit einem hohen Datenschutzniveau durchaus vereinbar sind.

Die Konsortialpartner des UPCARE-Projekts sind das Fraunhofer AISEC (AISEC), die Bundesdruckerei GmbH (BuDru), das Krebsregister Rheinland-Pfalz (KR RLP), EURECOM sowie SOFTEAM S.A. Zusätzlich ist darauf hinzuweisen, dass die Bundesdruckerei GmbH die Firma klargedacht.io im Rahmen eines Unterauftrages in das Projekt eingebunden hatte.

Das Projekt war als dreijähriges Projekt geplant und zielte auf die Erstellung und Evaluierung eines Demonstrators im Bereich TRL 4 bis 5 ab, der die Spezifikationen und Bedürfnisse der Krebsregister berücksichtigt. In einer ersten Phase hat das Konsortium gemeinsam an den Anforderungserhebung gearbeitet, um die Details der technologischen Ansätze in einer gemeinsamen Architektur zu vereinen und eine erste gemeinsame Implementierung der Innovationen umzusetzen. In der zweiten Phase werden die einzelnen Technologien vorangetrieben und Beiträge zu den jeweiligen Forschungsfeldern geleistet, während durch regelmäßige Synchronisationspunkte sichergestellt wurde, dass die Architektur wie geplant realisiert werden kann oder entsprechend angepasst werden muss. Das Ergebnis dieser Phase ist eine “Proof-of-Concept"-Implementierung, die alle geplanten kryptografischen Mechanismen und Workflows enthält, jedoch nicht unbedingt vollständig ist. In der dritten und letzten Phase liefen die Arbeitsabläufe wieder zusammen und die Partner haben die Technologien gemeinsam in den Demonstrator integriert und gemeinsam an dessen Bewertung arbeiten. Parallel zu diesen Phasen wurden die Forschungsarbeiten von Verbreitungs- und Projektmanagementaktivitäten begleitet.

1.2 Zusammenfassung der Projektergebnisse

Die Ergebnisse des UPCARE-Projekts lassen sich aus wirtschaftlicher, technischer sowie rechtlicher Sicht wie folgt zusammenfassen:

Es wurden technologische Anknüpfungspunkte im Rahmen von u.a. europäischen (Medical) Data Spaces Initiativen identifiziert, in welchen die Technologien bzw. das Know-How aus UPCARE auch wirtschaftlich verwertet werden können

Weiterhin wurde ein Demonstrator erstellt für die Umsetzung einer Plattform zum Zugriff auf Krebsregisterdaten mittels zweier Use Cases:

1. Kryptographisch gesicherter statistischer Zugriff auf Durchschnittswerte.
2. Kryptographisch gesicherter Zugriff auf personenbezogene Daten nach Erlaubnis der Beteiligten.

Aus rechtlicher Perspektive wurde die rechtssichere Umsetzung eines datenschutzfreundlichen Zugriffs auf Krebsregisterdaten untersucht und die Erkenntnisse kommen im Krebsregister Rheinland-Pfalz zu tragen.

In Bezug auf wissenschaftliche Veröffentlichungen wurde das Papier "UPCARE: User Privacy-preserving Cancer Research Platform." Auf der SECRYPT 2024 (21st International Conference on Security and Cryptography) platziert.