DKTK Deutsches Konsortium für Translationale Krebsforschung

dkfz.
Deutsches Konsortium für
Translationale Krebsforschung
Kernzentrum Heidelberg

Federated Information Systems (E260)

IT der Clinical Communication Platform (CCP-IT)

CCP-IT-Modul: Sichere Kommunikation für das DNPM

Stand: 14.10.2024

Version	Datum	Beschreibung	Autoren
0.1	28.09.2023	Erste Fassung	T. Kussel, M. Lablans
0.2	19.01.2024	Einarbeitung Kommentare von O. Kohlbacher, CCP-Office	T. Kussel, O. Kohlbacher, B. Uhl
1.0	23.01.2024	Abgestimmte Fassung	T. Kussel, M. Lablans
1.1	14.10.2024	Korrektur Abb. 1	T. Kussel

Dieses Addendum zum Datenschutzkonzept der CCP-IT beschreibt die Nutzung der Clinical Communication Platform (CCP) zur sicheren Vernetzung der Standorte im Deutschen Netzwerk für Personalisierte Medizin (DNPM).

1. Hintergrund

Im DNPM wird an jedem Standort ein sog. „DNPM-Knoten“ betrieben, der pseudonymisierte onkologische Daten aus den molekularen Tumorboards lokal integriert und für Prozesse im Netzwerk vorhält (ähnlich der im Hauptteil des DSK beschriebenen Brückenköpfe). Bei diesen Prozessen, die der Versorgung oder der Forschung dienen, kommunizieren die Knoten untereinander, um die bereitgestellten Daten über Standorte hinweg anlassbezogen zusammen anzuzeigen. Dabei wird aber an den anfragenden Standorten keine persistente Kopie der Daten erzeugt (föderierte Analyse). Zur Unterstützung dieser verschiedenen Kommunikationsmuster evaluierte eine Arbeitsgruppe des DNPM verschiedene technische Implementierungsoptionen und kam zu dem Ergebnis, dass die Kommunikation des lokalen DNPM-Knotens über eine von zwei Broker-Infrastrukturen erfolgt: entweder direkt über den in Tübingen angebotenen NGINX-Broker oder über die Broker-Funktionalität der CCP.

Jeder Standort wählt also aus zwei Optionen: Option DNPM-Broker sieht vor, dass jeder Standort seine Firewall so konfiguriert, dass der DNPM-Knoten für die nötige Kommunikation von außen erreichbar ist. Auf Wunsch mehrerer DNPM-Standorte wurde alternativ eine Option CCP geschaffen, in der die Kommunikation der DNPM-Knoten über die Brückenkopf-Struktur der DKTK/CCP erfolgt. Dies ermöglicht eine Nachnutzung der bereits etablierten Brückenköpfe und bietet ein erhöhtes Datensicherheitsniveau in dem Sinne, dass die Notwendigkeit von zusätzlichen Firewall-Ausnahmeregeln entfällt und zumindest innerhalb der CCP eine Ende-zu-Ende-Verschlüsselung besteht.

Die beschriebenen in diesem Addendum zusätzlichen Komponenten und Datenflüsse (Beam.Connect, Brücke zum DNPM-Broker) gelten also nur für Standorte, die sich für Option CCP entschieden haben; die anderen CCP-Standorte sind jedoch aufgrund der Joint-Controllership der CCP betroffen. Die initial an Option CCP interessierten Standorte sind in der nachfolgenden Tabelle aufgeführt; eine tagesaktuelle Liste kann jederzeit an jedem teilnehmenden Standort lokal unter der Adresse `https://<BRÜCKENKOPF URL>/dnpm-connect/sites` abgerufen werden.

Tabelle 1: Standorte mit Option CCP

- Uniklinik RWHT Aachen
- Charité - Universitätsmedizin Berlin
- Universitätsklinikum Bonn
- Universitätsklinikum Carl Gustav Carus Dresden
- Universitätsklinikum Düsseldorf
- Universitätsmedizin Essen
- Universitätsmedizin Göttingen
- Medizinische Hochschule Hannover
- Universitätsklinikum Köln
- Klinikum der Universität München
- Klinikum rechts der Isar, München
- Westfälische Wilhelms-Universität Münster
- Universitätsklinikum Würzburg
- Universitätsklinikum Frankfurt

2. IT-Struktur und Datenflüsse

Abbildung 1 zeigt eine schematische Darstellung der für dieses Addendum relevanten Software-Komponenten. Betrieb, Datenmanagement und Datenschutz des DNPM-Knotens selbst sind im DNPM-Datenschutzkonzept geregelt und nicht Bestandteil dieses Dokuments. Dieses Dokument beschreibt die Kommunikation der DNPM-Knoten über die CCP-Brückenköpfe (Option CCP).

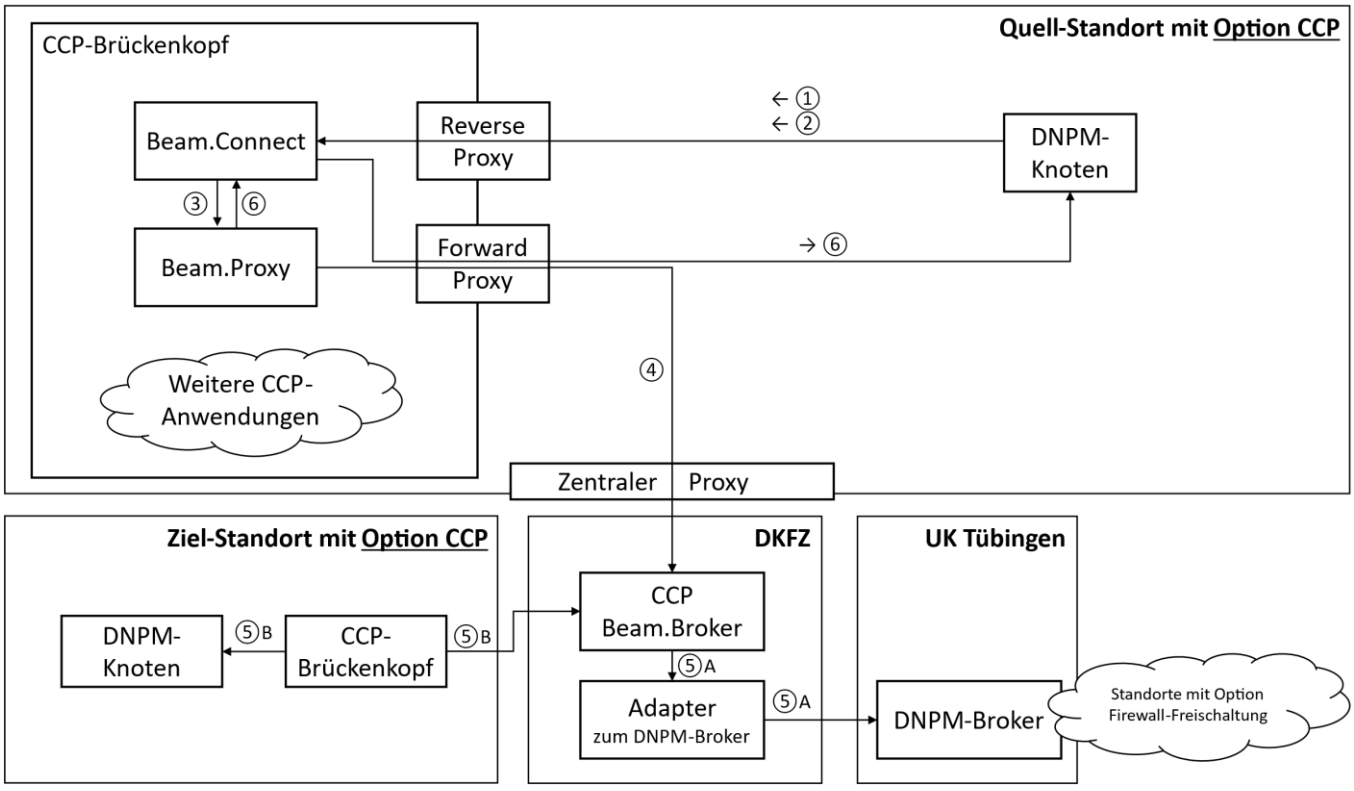

Abbildung 1: Relevante Softwarekomponenten und deren Interaktion.

Kurzbeschreibung: Die Kommunikation eines Option CCP-Standorts im DNPM-Netzwerk funktioniert so, dass der Quell-DNPM-Knoten seine Anfrage an den CCP-Brückenkopf richtet, dieser die Anfrage über die CCP-Kommunikationsschicht (Beam) an den Brückenkopf am Ziel-Standort übermittelt, wo sie an den Ziel-Knoten gerichtet wird. Dessen Antwort wird auf demselben Wege rückübermittelt und dem Quell-DNPM-Knoten zurückgemeldet. Alle Nachrichten innerhalb der Samply.Beam-Infrastruktur sind Ende-zu-Ende verschlüsselt und signiert und können auch am CCP-Beam.Broker nicht eingesehen werden. Nachrichten von und zu Standorten, die sich für die Option DNPM-Broker entschieden haben (auch nicht-CCP-Partner), werden über einen Adapter zwischen der CCP-Infrastruktur und dem DNPM-Broker übertragen.

Detaillierte Beschreibung: Im Folgenden wird diese Kommunikation im Detail beschrieben; die Nummerierung entspricht dabei den Nummern in Abbildung 1:

1. Der lokale DNPM-Knoten ermittelt die Adresse des anzusprechenden entfernten Ziel-DNPM-Knotens. Hierfür lädt er aus der Beam.Connect-Komponente des Brückenkopfes eine Standort-Liste bestehend aus Namen, Kürzeln und anzusprechenden Ziel-URLs der Standorte herunter.
2. Der lokale DNPM-Knoten stellt die HTTP-Anfrage (von hier an „Query“) an die Beam.Connect-Komponente innerhalb des CCP-Brückenkopfes.
3. Beam.Connect verpackt die Query in eine verschlüsselte Beam-Nachricht und übergibt sie dem Beam.Proxy.
4. Der Beam.Proxy übermittelt die Beam-Nachricht an den CCP-Beam.Broker.
5. Die Query wird an den Ziel-DNPM-Knoten übermittelt:
    a. Wird der Ziel-DNPM-Knoten mit Option DNPM-Broker betrieben, wird die Beam-Nachricht durch eine Adapterkomponente entschlüsselt und die enthaltene Query an den DNPM-Broker in Tübingen gestellt (5A).
    b. Wird der Ziel-DNPM-Knoten mit Option CCP betrieben, lädt dessen CCP-Brückenkopf die Anfrage vom CCP-Broker herunter (5B), und führt sie gegen den DNPM-Knoten aus.

    In beiden Fällen wird das Ergebnis der DNPM-Knoten-Anfrage in eine zweite Beam-Nachricht verschlüsselt und dem CCP-Beam.Broker übergeben.
6. Im CCP-Brückenkopf des anfragenden Standorts wird die Beam-Nachricht heruntergeladen, entschlüsselt und an den DNPM-Knoten zurückgegeben. Aus Sicht des DNPM-Knotens handelt es sich dabei um die Antwort auf seine HTTP-Anfrage aus Schritt 2; der gesamte Vorgang passiert im Bruchteil einer Sekunde.

Alle in den Brückenkopf eingehenden Verbindungen werden mittels TLS-verschlüsselten Verbindungen über den Reverse-Proxy an die Komponenten weitergeleitet, alle ausgehenden Verbindungen werden über einen Forward-Proxy gestellt. Es ist empfohlen, dass der Reverse Proxy des Brückenkopfes hierfür mit einem vertrauenswürdigen TLS-Zertifikat konfiguriert und außerdem der DNPM-Knoten ebenfalls TLS-abgesichert wird (vgl. dessen Datenschutzkonzept).

3. Funktionsprüfung

Die Nutzung des CCP-Beam-Netzwerkes für die DNPM-Knoten-Kommunikation stellt Anforderungen bezüglich Verfügbarkeit und Funktionalität an die CCP-Infrastruktur. Um im Fehlerfall schnell und zuverlässig festzustellen, ob die Funktionalität seitens der CCP gegeben ist, werden technische Tests implementiert, die sich manuell oder auch automatisch durchführen lassen.

Die Kommunikation über die CCP gilt als funktionsfähig, genau dann, wenn die folgenden vier Tests erfolgreich ausfallen:

3.1 Zentraler Beam.Broker

Der zentrale Beam.Broker stellt eine Überwachungsschnittstelle zur Verfügung. Überprüft werden hier sowohl seine Erreichbarkeit über das Netzwerk als auch seine Funktionsbereitschaft. Einfluss auf das Funktionieren dieses Tests hat allein das DKFZ.

Test: `curl https://{BROKER_URL}/v1/health` gibt positives Urteil zurück

3.2 Beam.Proxy → Beam.Broker

Im Betrieb stellt jeder CCP-Brückenkopf eine dauerhafte Verbindung zum Beam.Broker her. Dieser Verbindungsstatus dient zur Feststellung, ob ein Proxy zum Broker verbunden ist.

Test: `curl https://{BROKER_URL}/v1/health/proxies/{PROXY_ID}` gibt positives Urteil zurück

3.3 Beam.Connect

Es wird geprüft, ob HTTP-Anfragen, wie sie auch der DNPM-Knoten stellen würde, an über Beam angebundene Brückenköpfe übermittelt werden können (Hin-Richtung), und von diesen beantwortet werden (Rück-Richtung).

Test: `curl -H "Host: {STANDORT-VHOST}" http://{BRÜCKENKOPF_URL}/dnpm-connect/bwhc/peer2peer/api/status`

Fällt dieser Test positiv aus, gilt er als bestanden. Im negativen Fall könnte jedoch auch ein Ausfall des DNPM-Knotens ursächlich sein. Daher wird im negativen Fall zusätzlich die Verbindung zu einem einfachen Echo-Endpunkt in jedem Brückenkopf angesprochen.

Test: `curl -H "Host: {STANDORT-VHOST}" http://{BRÜCKENKOPF_URL}/dnpm-connect/echo`

3.4 Adapter zum DNPM-Broker

Es wird geprüft, ob der DNPM-Broker (Betrieb durch UK Tübingen) über die Adapterkomponente (Betrieb durch DKFZ) angesprochen werden kann.

Test: `curl -H "Host: {NGINX-BROKER VHOST}" http://{BRÜCKENKOPF_URL}/dnpm-connect/sites`

Fällt dieser Test positiv aus, gilt er als bestanden. Im negativen Fall könnte jedoch auch ein Ausfall des Tübinger DNPM-Brokers ursächlich sein. Daher wird im negativen Fall zusätzlich die Verbindung zu einem unabhängigen Dienst im Internet geprüft:

Test: `curl -H "Host: external.virtual" http://{BRÜCKENKOPF_URL}/dnpm-connect/`

Dieser Test gilt also genau dann als bestanden, falls einer der beiden obigen curl-Aufrufe gelingt.