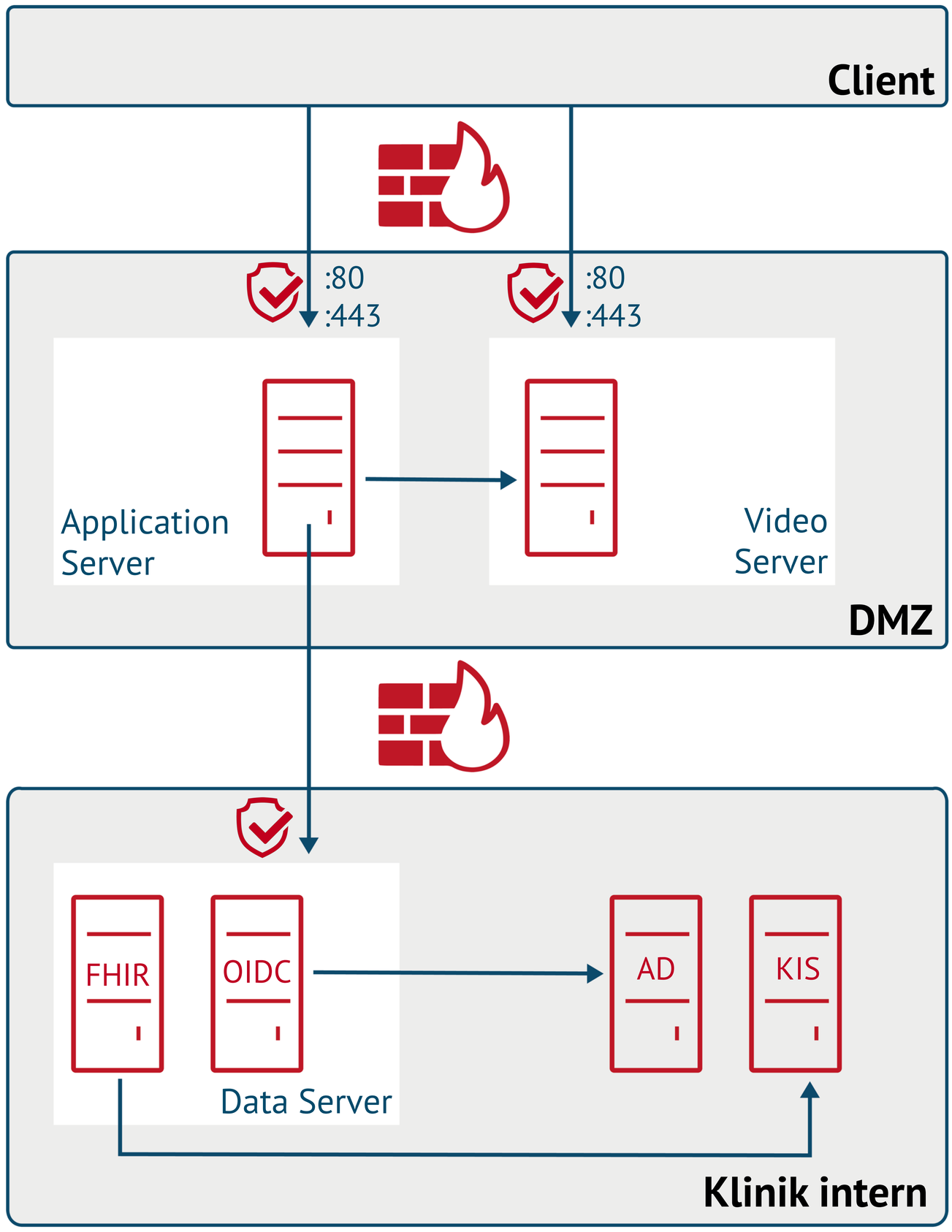
MOLIT
Institut für personalisierte Medizin

Sicherheitskonzept



Authentifizierung und Autorisierung

Zur Authentifizierung wird ein OpenID Connect (OIDC) Provider eingesetzt. OpenID Connect ist eine Authentifizierungsschicht, welche auf dem Autorisierungs-protokoll OAuth 2.0 basiert.
Beim initialen Aufruf einer Applikation wird der Nutzer auf eine vom OpenID Connect Provider zur Verfügung gestellten Login-Seite weitergeleitet. Nach erfolgreicher Authentifizierung durch Eingabe eines Nutzernamens und Passworts erhält der Nutzer ein Authentifizierungs-token in Form eines JSON Web Tokens (JWT), mit dem er sich für weitere Anfragen authentifizieren kann und wird zur Applikation zurückgeleitet.
Über den OpenID Connect Provider ist eine Anbindung an das Benutzerverzeichnis des Klinikums möglich. Dies ermöglicht den Klinikmitarbeitern den Login mit ihren gewohnten Anmeldedaten. Zusätzlich wird unter den verschiedenen Applikationen ein Single-Sign-On (SSO) gewährleistet.

Architektur

Dargestellt ist hier eine mögliche Architektur, um MOLIT-Komponenten in eine bestehende Infrastruktur zu integrieren. Die Architektur besteht aus drei (virtuellen) Servern: Application Server, Data Server und Video Server.
Zur Gewährleistung der Vertraulichkeit und Integrität der auf dem Data Server hinterlegten Patientendaten befindet sich der Data Server im internen Netzwerk des Klinikums. Ein Zugriff von außen ist nur durch den Applikationsserver möglich. Anfragen ohne gültiges Authentifizierungstoken werden zu keiner Zeit an den datenhaltenden FHIR-Server weitergeleitet.

Verschlüsselung

VITU ist komplett browserbasiert und verschlüsselt sowohl die Datenübertragung als auch die Videoübertragung per TLS (HTTPS).

Die Videoübertragung basiert technisch auf Web Real-Time Communication (WebRTC), welches alle Video- und Audiostream ebenso TLS verschlüsselt.

Kontakt: info@molit.eu