DIPS FRONT

Dokumentasjon

CosDoc+, februar 2021

Teknisk Sikkerhetsdokumentasjon

Dokumentkontroll

Dato	Forfatter	Versjon	Endringer
26.01.2021	Stian Grønhaug	0,5	
02.02.2021	Stian Grønhaug	0,8	Oppdatert beskrivelser om nettverkstrafikk etter innspill. Korrigert formuleringer. Lagt til kapitler for å svare bedre opp forventninger.
15.02.2021	Heidi Andresen	0,81	Endret til å bruke mal som brukes for dokumentasjon i Front
15.02.2021	Tormod Førland	0,82	Korrigert beskrivelse for trafikk (dårlig språk)
20.02.2022	Stian Grønhaug	1.0	Endret: Også sensitiv informasjon lagres i sekundærminnet

Distribusjon

Dokumentet er til internt bruk og til våre kunder.

Opphavsrett

Innholdsfortegnelse

1. Innledning

Dette dokumentet må leses som et tillegg til teknisk beskrivelse for DIPS CosDoc. Dokumentet inneholder beskrivelser av sikkerhetsmekanismer og arkitektur for CosDoc+, samt komponenter CosDoc+ er avhengig av for å kunne fungere som klient mot DIPS CosDoc.

2. Arkitektur og komponenter i bruk

2.1. Kommunikasjon mot database

Kommunikasjon mot database settes opp som forbindelsesstreng i konfigurasjonsfiler for tjenestene som skal aksessere den. Integrert sikkerhet skal brukes for å unngå bruk av passord i konfigurasjonsfilene. Som nødløsning kan CosDoc sine tjenester bruke passord som er hashet. Dette anbefales over å bruke passord i klartekst, men må kun benyttes dersom integrert sikkerhet ikke er mulig.

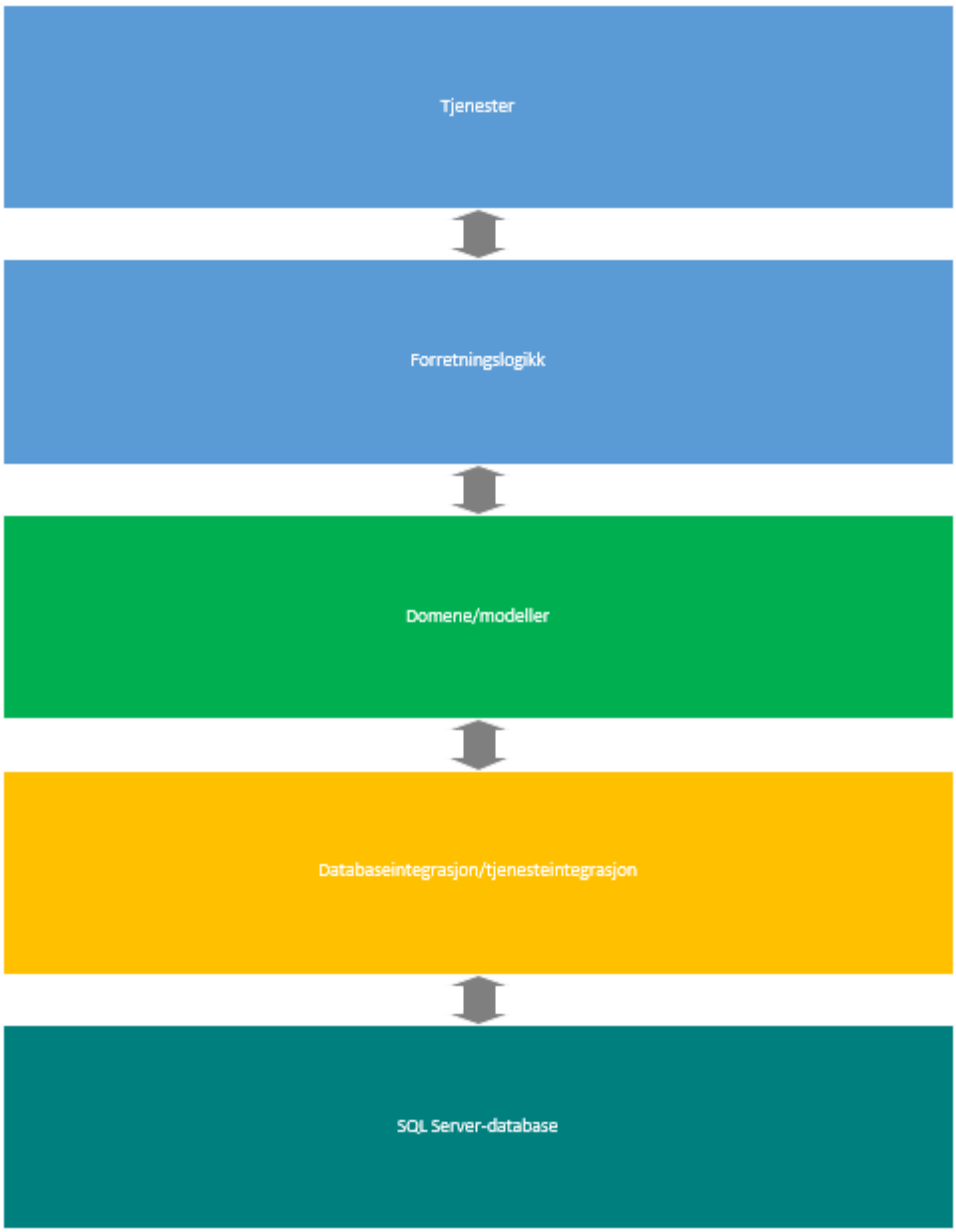
ACOS CosDoc sine tjenester bruker egen applikasjonspool. Som eier av denne opprettes CosDoc-domenebruker laget for dette formål.

Eier av applikasjonspool får tilgang til databasetjener og nødvendige rettigheter i CosDoc sine databaser.

2.2. Tjenester

Alle tjenestekall som er tilgjengelig for CosDoc, er gjort tilgjengelig via et sett av tjenester. Funksjonene er gjort tilgjengelig i et forretningslag, som jobber mot et databaseintegrasjonslag. I sum utgjør dette CosDocAPI. CosDoc API er under kontinuerlig utvikling, og eksisterer i flere versjoner. Opprinnelig API er SOAP-basert laget med Microsoft WCF-teknologi. Nyere grensesnitt er .Net Standard-baserte REST-tjenester. Klienter som CosDoc+ konsumerer fra API. Også samarbeidspartnere (Velferdsteknologileverandører og andre konsumenter) arbeider mot dette.

Logisk er tjenestene lagdelt. Dette er blant annet gjort for å skille mellom programlogikk og det som hentes ut fra database. I tillegg sentraliseres kontaktpunktene som går ut. Denne delingen reduserer fare for å innføre «Sql injection» og andre typer kommandoer som kan hacke eller på annen måte ødelegge.



All forretningslogikk er gjort i forretningslaget. Domenelaget er limet mellom de forskjellige delene.

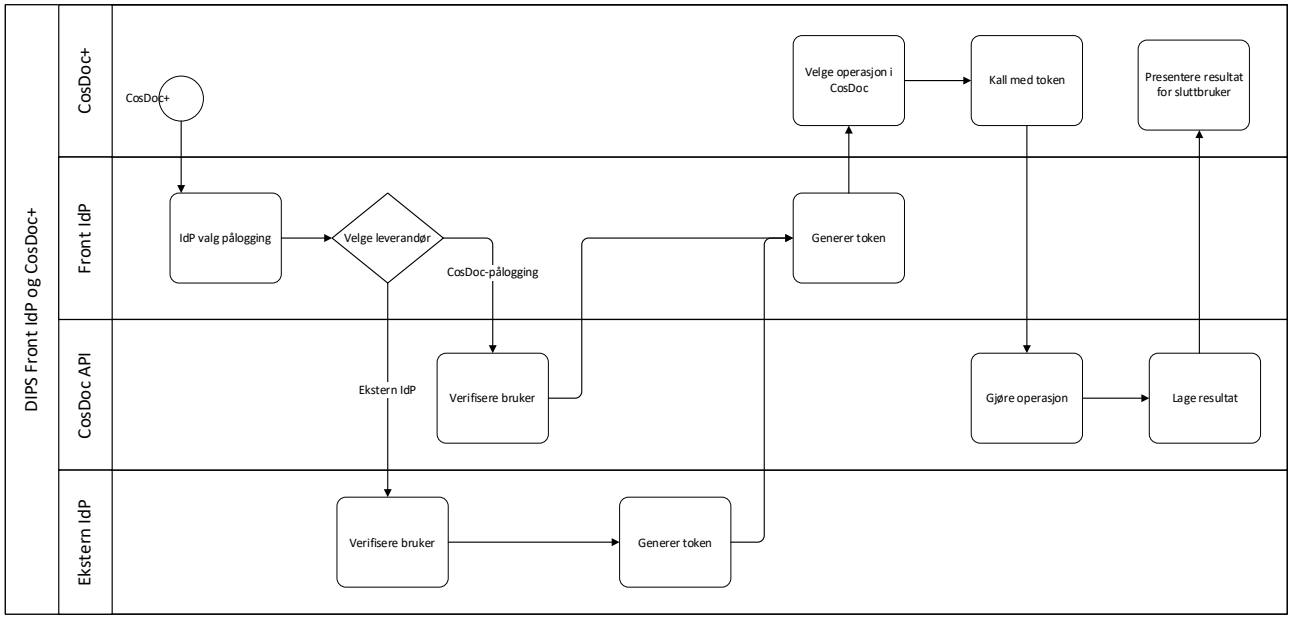
Databaseintegrasjonslaget er det eneste som har tilgang til databasen. Klienter kan kun konsumere funksjoner fra tjenestelaget.

For CosDoc+ anbefales det å benytte proxy-tjenester. Normalt blir dette gjort via metode «Reverse Proxy». Da opprettes et eget aksesspunkt for alle tjenester, som de tjenestene som er i produksjon. Dette gjør det enklere å kontrollere trafikk mot eksterne kilder, som CosDoc+.

2.3. Klienter

CosDoc+ leveres som Windows Universal App eller som Android-applikasjon. Applikasjonene er designet for å fungere utenfor sensitiv sone, som fra Internett. DIPS Front leverer ikke, men anbefaler, bruk av MDA-løsninger.

2.3.1. DIPS Front IdP



Dips Front sin IdP-tjeneste er en Identity Server -implementasjon. Denne har som oppgave å enten logge inn brukere eller tjenester mot CosDoc, eller til å videreformidle til andre autentifiseringsløsninger som HelseId. Tjenesten legger til «claims» som er nødvendig for at token skal fungere med CosDoc.

2.3.2. Kommunikasjon mot REST-baserte tjenester

I kommunikasjon mot REST-tjenestene brukes en kombinasjon av Token (bruker-/personinformasjon) og sikkerhetsbibliotek (ansettelsesinformasjon). Token generert ved innlogging er del av kallet til tjenestene. Tjenestene bruker informasjonen til tilgangskontroll og kontroll av data. Token-basert sikkerhet sikrer også at kun innloggede brukere får tilgang til tjenestefunksjoner.

2.3.3. Kommunikasjon mot SOAP/WCF-baserte tjenester

Tjenestene er sesjonsløse. Alle tjenestekall forutsetter at det medfølger programbrukerinformasjon. Her forventes at det skal medfølge identifikasjon for kallende applikasjon, programbruker og referanse til programbrukers ansettelse. Kallende applikasjon må ha en applikasjonsbruker som er autorisert for å bruke CosDoc.

2.3.4. Enhetsid

Ved alle API-kall er det krav til enhetsid. Alle enheter som bruker CosDoc+, må identifisere seg med en unik enhetsid. Dette er en sikkerhet som er i tillegg til applikasjonsbruker og programbruker. Ved misbruk eller ved tap av enhet, er det mulig å utestenge enhet fra å gjøre API-kall.

2.3.5. Mellomlagring av data

Kodeverk

Nøytrale og ikke-personidentifiserende kodeverk, som eksempelvis landkoder, diagnosekoder, journaltyper og registreringstyper, lagres persistent på enhetene. Dette er vurdert til ufarlig, da disse er felles for alle pasienter og brukere av systemet. Når alt lagres, er ikke dette i seg selv identifiserende for sluttbruker.

Personidentifiserende data

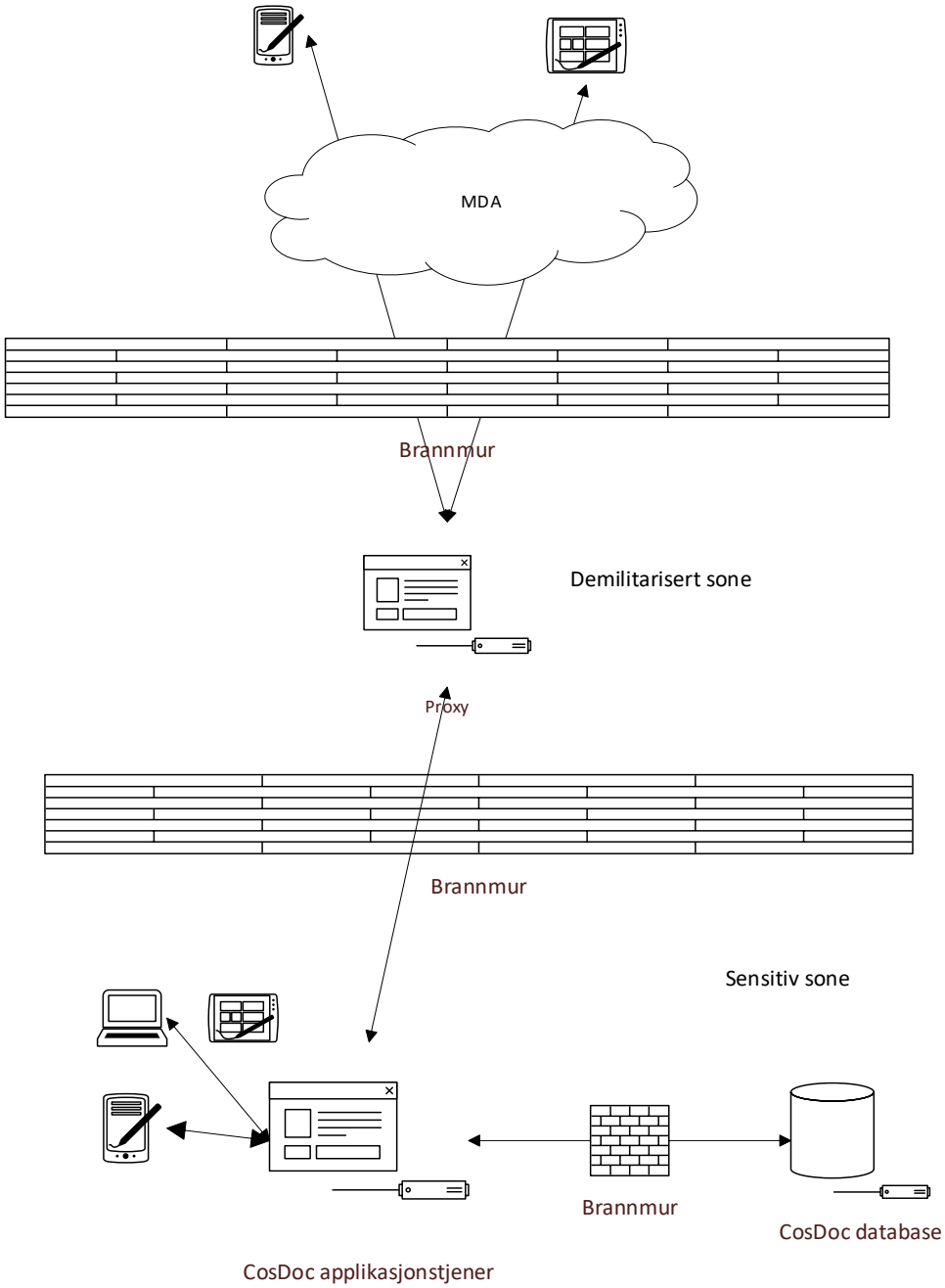
CosDoc+ er designet for å kunne fungere offline. Applikasjon kan bli avsluttet av forskjellig type hendelser:

- Bruker velger å avslutte app, med eller uten at avslutning var intensjonen
- Applikasjon avsluttes av Android etter å ha vært lenge inaktiv

For å sikre at informasjon ikke skal gå tapt, lagrer CosDoc+(fra versjon 21.0.0) også personsensitiv informasjon. Informasjonen blir lagret kryptert på enhetene. Informasjonen er dermed beskyttet av både Android sitt beskyttete område for CosDoc+, og at data er kryptert.

Det hentes kun informasjon utfører har tjenstlig behov for. Altså begrenses dette til informasjon relatert til personer som er på ansatt sin arbeidsliste, eller som er direkte søkt frem.

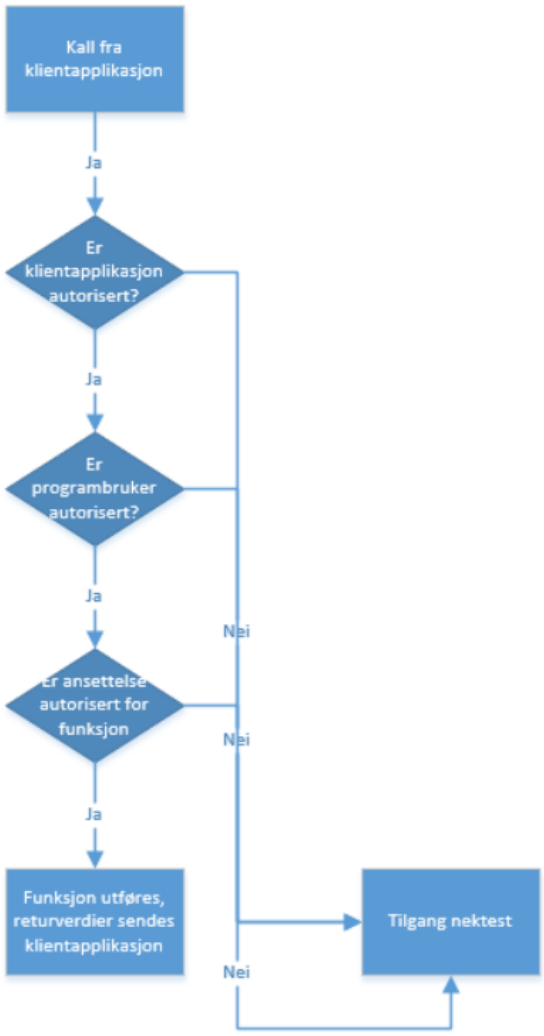
2.4. Dataflyt mellom komponenter i løsningen



Trafikk blir initiert fra CosDoc+. Informasjon fra sensitiv sone til klient er svar på forespørsler fra klient. Kallet går til tjener i demilitarisert sone, som videreformidler kallet til CosDoc applikasjonstjener. Tjenester på

CosDoc applikasjonstjener henter og bearbeider informasjon, og henter eller oppdaterer i databasen. Retur går via etablert kanal for å sende dette tilbake til tjener i demilitarisert sone, som igjen sender tilbake til klient. Portåpning på port 443 i brannmurene må være slik at CosDoc+ kan kontakte tjener i DMZ, og tjener i DMZ må kontakte tjener i sensitiv sone.

3. Tilgangsstyring



Programbrukeridentifikasjon og passord brukes for å verifisere at programbruker har tilgang til CosDoc. Ansettelse brukes for å sjekke hvilke tilganger programbruker er autorisert for. I tillegg er det kontroll på hvilke funksjoner bruker er autorisert for å utføre i programmet, som i journal eller på arbeidsplan. Eksempelvis kan programbruker ha tilgang til å lese legemiddeloversikt, men ikke ha mulighet til å administrere dem.

All tilgangskontroll blir gjort på tjenestene. Et viktig prinsipp for design av tjenestene, er at tjenestene ikke skal returnere data sluttbruker ikke har tilgang til å se. I tillegg blir det gjort kontroller på klient. Kontroll på klient er for å bedre brukeropplevelse. Det er sikkerhetsfunksjonene i tjenestene som kontrollerer hva sluttbruker er autorisert for. Forsøker sluttbruker i CosDoc+ å utføre en operasjon sluttbruker ikke er autorisert for, vil tjenesten returnere en feilmelding. Dette sikrer at det er mulig å korrigere eventuelle

sikkerhetshull raskt på tjenestene, uten at det skaper et øyeblikkelig behov for å oppdatere programvare på enhetene som er i produksjon.

Tjenestene er delt inn i forskjellige tilgangspunkter. Disse har kun data som er relevant for det tjenesten er ment å omfatte. Eksempelvis vil kontaktpunkter for journal aldri returnere navn på pasient, kun referanse til dem. På samme måte vil ikke legemiddeloversikter returnere verken tilhørende journalregistreringer eller navn på pasienter, kun referanser til dem. Eventuell sammenstilling blir gjort i klient som bearbeider og viser data for sluttbruker. Dette oppfyller kravene GDPR har til innebygd sikkerhet (ikke eksponere personinformasjon der det ikke er nødvendig).

4. Logging

Tjenestene sikrer forskriftsmessig logging. Alle pasienter og journaler som blir sendt enhetene, logges og kan kontrolleres via rapporter og uttrekk i etterkant. Det som logges refereres til programbrukere og pasienter via referanser, ikke på navn direkte. Eksempler på logging (ikke utfyllende):

- Pålogging
    - Ansettelsesid på bruker
    - Applikasjonsbruker
    - Tidspunkt
    - Applikasjon (fra vår 2021)
    - Enhetsid (fra vår 2021)
- Henting av pasient
- Henting av journal
- Visning av fødselsnummer

API og CosDoc+ tilbyr funksjon for nødsøk. Alle nødsøk blir logget på forskriftsmessig måte. Oversikt over utførte nødsøk er tilgjengelig i lister og i rapporter.

5. Endringssyklus

DIPS Front jobber etter smidig utviklingsmetodikk. Utvikling går i sykluser på 14 dager. Prioritering til sprint inkluderer utviklingspunkter basert på et veikart. Her prioriteres feilretting og nye funksjoner ut fra det som gir mest verdi for sluttbruker. Testing skjer fortløpende. Utviklerne bruker både enhetstester og integrasjonstester i utviklingsarbeidet. I tillegg testavdelingen ressurser som lager mer omfattende integrasjonstester som kan kjøres automatisk ved hver versjon. Manuell testing av hele programvaren blir gjort kontinuerlig.

6. Sletteprosedyre for sletting av data

I selve løsningen for CosDoc+ er det ingen lagring av personsensitive data.