1. Servicebeskrivelse for Context Handler 2

Versions-nummer	Ikrafttrædelses dato	Emne
0.8	27.12.2023	Første udgave
0.9	15.01.2024	Rettet efter første review.
1.0	27.01.2024	Godkendt efter review.
2.0	12.06.2024	Godkendt efter review. Ingen ændringer
3.0	15.01.2025	Godkendt efter review. Ingen ændringer
4.0	18.06.2025	Godkendt efter review. Ingen ændringer
5.0	02.02.2026	Godkendt efter review. Ingen ændringer

1.1.1 Vilkår for registrering af it-system

Nærværende vilkår indeholder bestemmelser om en Tjenesteudbyders forpligtelser i forbindelse med registrering af et it-system i den fælleskommunale infrastruktur for brug af Context Handler 2 på vegne af en offentlig myndighed.

1.1.2 Registreringsproces

For at en Tjenesteudbyder kan benytte Context Handler 2 i den fælleskommunale infrastruktur, skal Tjenesteudbyder i Fælleskommunalt Administrationsmodul registrere sin organisation og it-system, samt whiteliste de myndigheder, der må anvende it-systemet. Herefter vil myndighederne kunne tage systemet i anvendelse I Fælleskommunalt Administrationsmodul kan alle aspekter af en integration til Context Handler 2 i den fælleskommunale infrastruktur administreres, og Tjenesteudbyder skal benytte Fælleskommunalt Administrationsmodul i videst muligt omfang.

1.1.3 Test

Forud for anvendelse af Context Handler 2 i Produktionsmiljøet, skal Tjenesteudbyder via prøvetilslutning anmode om at gennemføre nødvendige test i Eksternt testmiljø.

1.1.4 Tekniske standarder

Tjenesteudbyderen står inde for at overholde tekniske standarder i forbindelse med kald til den enkelte serviceudbyder.

Læs vilkår for anvendelse af sikkerhedsmodellen og beskrivelse af sikkerhedsmodellen på Digitaliseringskataloget.dk.

1.1.5 Sikkerhedskrav

Det er Tjenesteudbyderens ansvar, at it-sikkerheden i egen organisation og egne it-systemer er tilstrækkelig, og at de sikkerhedskrav, der er gældende for Tjenesteudbyderen som it-systemudbyder for den enkelte myndighed, efterleves.

1.1.6 Databeskyttelseslovgivning

Tjenesteudbyderen skal til enhver tid efterleve relevante bestemmelser i gældende databeskyttelseslovgivning, samt gængse standarder på området.

Forestår Tjenesteudbyderen driften af det it-system, som anvender den fælleskommunale infrastruktur, og indgår der personoplysninger i it-systemet og de filer, der udveksles, vil Tjenesteudbyderen være databehandler for myndigheden. Er det tilfældet, skal der indgås en databehandleraftale mellem myndighed og Tjenesteudbyder. Databehandleraftalen skal indgås mellem Tjenesteudbyder og den pågældende myndighed og kan ikke oprettes via Fælleskommunalt Administrationsmodul.

1.1.7 **Afholdelse af udgifter**

Det er myndigheden, via KOMBIT, der afholder alle udgifter til udvikling, drift og forvaltning af den fælleskommunale infrastruktur, herunder ligeledes forbrug af den fælleskommunale infrastrukturs services. Tjenesteudbyderen skal derfor ikke betale for forbrug af den fælleskommunale infrastruktur.

Udgifter vedr. udvikling, etablering, integration, test, drift, udbedring af fejl m.v. af eget it-system med henblik på integration til samt efterfølgende anvendelse af Context Handler 2, herunder også opdatering til nye versioner, afholdes i henhold til aftale mellem Tjenesteudbyder og den enkelte myndighed.

Registrering af it-systemer og brug af Context Handler 2 er derfor vederlagsfrit for Tjenesteudbyder i det omfang, at denne betjener sig selv via Fælleskommunalt Administrationsmodul.

1.1.8 **Overtrædelse af vilkår og retningslinjer**

Tjenesteudbyder erklærer sig ved sin tiltrædelse af nærværende vilkår indforstået med, at Tjenesteudbyderens overtrædelse af disse vilkår eller andre retningslinjer og vilkår for brug af den fælleskommunale infrastruktur, herunder de Generelle vilkår, der fremgår på Digitaliseringskataloget.dk, kan have til følge, at Tjenesteudbyderens it-system afkobles fra den fælleskommunale infrastruktur.

KOMBIT kan træffe beslutning om og kan effektuere teknisk afkobling af et it-system, hvis Tjenesteudbyderen overtræder vilkårene for tilslutning, eller anvender den fælleskommunale infrastruktur uhensigtsmæssigt, herunder ikke retter uhensigtsmæssigt brug uden ubegrundet ophold. KOMBIT afgør, hvad der i den forbindelse skal anses som ubegrundet ophold under hensyntagen til overtrædelsens karakter. Således kan alvorlige sikkerhedsbrud medføre omgående afkobling.

En afkobling vil selvfølgelig ikke finde sted uden saglig grund, og Tjenesteudbyder vil inden effektuering blive kontaktet af KOMBIT via de kontaktoplysninger, Tjenesteudbyder har angivet i Fælleskommunalt Administrationsmodul.

1.1.9 **Ansvar og forudsætninger for relying parties**

Context Handler 2 udsteder tokens på NSIS-sikringsniveau Lav, Betydelig eller Høj, alt efter Tjenesteudbyderens behov.

En Tjenesteudbyder må kun forlade sig på autentifikation af brugere fra myndigheders IdP'er, der er videreformidlet via Context Handler 2 på det krævede NSIS-sikringsniveau, når følgende er opfyldt:

- Tjenesteudbyder har gennemført en teknisk registrering i Fælleskommunalt Administrationsmodul.
- Tjenesteudbyder har forsikret sig om, at det tilbudte sikringsniveau fra Context Handler 2 opfylder Tjenesteudbyderens sikringsbehov.

- Tjenesteudbyder har med pågældende myndighed/myndigheder aftalt eventuel anvendelse af eventuelle autorisations-data indeholdt i Context Handler 2-tokens med henblik på autorisation af rettigheder i Tjenesteudbyderens tjeneste.
- Tjenesteudbyder validerer Context Handler 2-token ved hver enkelt autentifikation inkl. verifikation af digital signatur, herunder gyldighed af ID-tjenestens certifikat, som angivet fra certifikatudsteder.
- Tjenesteudbyder validerer, at det modtagne token i "Audience Restriction" omfatter Tjenesteudbyderen.
- Tjenesteudbyder uddrager det eksplicitte NSIS-sikringsniveau, der er indskrevet i det enkelte token. Bemærk, at dette NSIS-sikringsniveau kan være Lav, Betydelig eller Høj baseret på tjenesteudbyderens krævede sikringsniveau. Hvis niveauet er lavere end det krævede sikringsniveau, er den aktuelle bruger IKKE autentificeret.

Oplysning til relying parties vedrørende Context Handler 2 understøtter lokal sessionsbevarelse i henhold til mulighederne herfor i NSIS-standarden, der kan findes på Digitaliseringsstyrelsens hjemmeside.

Tjenesteudbyder er selv ansvarlig for sikkerhedsforhold omkring eventuelle egne sessionsmekanismer samt vurdering af behovet for at gennemtvinge en ny Autentifikation med aktiv brugerinvolvering (dvs. fravælge SSO), jf. NSIS v. 2 kap. 6 krav 8.

Tokens fra Context Handler 2 kan ikke uden tilladelse fra KOMBIT anvendes til at udstede andre tokens, men kan kun anvendes direkte af en Tjenesteudbyder i forbindelse med Tjenesteudbyderens forretningsfunktionalitet.