

TA-01-Q Vedlegg Q – Domeneautorisasjonsmodell

Nytt fagsystem

GARANTIKASSEN FOR FISKERE

Q.1 Formål.....	2
Q.2 Overordnet prinsipp.....	2
Q.3 Domeneobjekter	2
Q.4 Brukerkategorier.....	3
Q.5 Autorisasjonsregler – forklarende modell	3
Q.6 Beslutningsmodell.....	4
Q.7 Typiske misbruksscenarier	4
Q.9 Forvaltning av tilganger	5

Q.1 Formål

Dette vedlegget beskriver hvordan autorisasjon i løsningen skal forstås og anvendes i GFFs fagdomene, herunder både mannskapsrelaterte ordninger og fartøybaserte tilskuddsordninger.

Formålet er å etablere en felles forståelse av hvordan tilgang til data og funksjoner skal vurderes basert på brukerens identitet, rolle og relasjon til objekter i domenet.

Vedlegget er informativt og utdyper kravene i vedlegg TA-01-C, herunder kapittel C.7 og C.7A. Ved eventuell motstrid gjelder kravene i vedlegg TA-01-C.

Manglende eller uklar forståelse av domeneautorisasjon vil kunne føre til løsninger som gir korrekt autentiserte brukere tilgang til data de ikke er autorisert til å se eller behandle.

Q.2 Overordnet prinsipp

Autorisasjon i løsningen skal ikke baseres utelukkende på brukerens identitet, men også på hvilken relasjon brukeren har til det objektet det forespørres tilgang til.

Løsningen skal baseres på følgende hovedprinsipp:

Bruker → Relasjon → Objekt → Tilgang

Dette innebærer at en bruker identifiseres entydig gjennom autentisering, at systemet identifiserer hvilket objekt det forespørres tilgang til, at systemet validerer om det foreligger en gyldig relasjon mellom bruker og objekt, og at tilgang kun gis dersom relasjonen er gyldig og i samsvar med gjeldende regler.

Prinsippet skal anvendes konsistent for alle eksterne og interne brukerflater.

Q.3 Domeneobjekter

Autorisasjon skal vurderes mot konkrete objekter i domenet. Følgende objekter er sentrale.

Q.3.1 Person

Omfatter alle individer som behandles i løsningen, inkludert søker, mannskapsmedlem, fartøyeier, representant for fartøy eller virksomhet, og interne brukere.

Personobjektet er særlig sensitivt og skal underlegges streng tilgangskontroll.

Q.3.2 Fartøy

Omfatter fartøyet's identitet og registrerte tilknytninger, herunder eierskap, disposisjonsrett og relevante relasjoner til personer.

Tilgang til fartøydata forutsetter dokumentert tilknytning.

Q.3.3 Søknad

Omfatter alle typer søknader i løsningen, herunder egenmelding, fellesmelding, melding om fortsatt ledighet og søknader knyttet til fartøybaserte tilskuddsordninger.

Søknader er knyttet til person og, der det er relevant, fartøy og ordning.

Q.3.4 Sak og vedtak

Omfatter journalført sak, dokumenter, vedtak, status, historikk og korrespondanse.

Tilgang til sak og vedtak skal følge autorisasjonsreglene for underliggende objekter.

Q.3.5 Eksterne datakilder

Omfatter data som hentes fra eksterne registre og tjenester.

Disse dataene skal ikke behandles som generelle oppslag, men som kontrollerte datakilder som kun benyttes i kontekst av en autorisert sak eller prosess.

Q.4 Brukerkategorier

Q.4.1 Ekstern privat bruker

Dette er en person som opptrer på egne vegne.

Brukeren har tilgang til egne data, egne søknader og egne vedtak.

Brukeren har ikke tilgang til andre personers opplysninger eller saker.

Q.4.2 Ekstern fartøyeier eller representant

Dette er en bruker som opptrer på vegne av et fartøy.

Brukeren har tilgang til fartøy som vedkommende har dokumentert tilknytning til, søknader og tilskuddsordninger knyttet til disse fartøyene, samt informasjon som er nødvendig for å opprette og følge opp slike saker.

Tilgangen er begrenset til fartøy, ordninger og personer som er knyttet til fartøyet.

Q.4.3 Intern saksbehandler

Dette er ansatte i GFF med tilgang til løsningen via interne brukerflater.

Tilgang er rollebasert og underlagt prinsippet om minste privilegium. Saksbehandling og godkjenning er funksjonelt separert.

Q.5 Autorisasjonsregler – forklarende modell

Q.5.1 Egenidentitet

En bruker har kun tilgang til data som gjelder brukerens egen identitet, med mindre det foreligger en dokumentert relasjon som gir utvidet tilgang.

Q.5.2 Relasjon til fartøy

Tilgang til fartøy og fartøysrelaterte data forutsetter at brukeren har en dokumentert relasjon til fartøyet.

Q.5.3 Relasjon til mannskap

Ved behandling av fellesmeldinger kan brukeren kun forholde seg til mannskap som er knyttet til det aktuelle fartøyet.

Tilsvarende er tilgang til fartøybaserte ordninger begrenset til fartøy brukeren har dokumentert tilknytning til.

Q.5.4 Ingen frie oppslag

Løsningen skal ikke fungere som et oppslagsverktøy for person-, fartøy- eller saksdata, uavhengig av om dataene gjelder mannskap eller fartøybaserte ordninger.

Brukeren skal ikke kunne hente frem informasjon om andre ved å oppgi identifikatorer.

Q.5.5 Behovsstyrt datatilgang

Data som hentes fra interne eller eksterne kilder skal begrenses til det som er nødvendig for den aktuelle funksjonen eller behandlingen, uavhengig av om dette gjelder person- eller fartøyrelaterte forhold.

Q.5.6 Backend som kontrollpunkt

Alle autorisasjonsvurderinger foretas i backend. Klientapplikasjoner skal ikke påvirke tilgangskontroll.

Q.5.7 Feilhåndtering

Dersom systemet ikke kan fastslå at en bruker har rett til tilgang, skal tilgang nektes og saken håndteres videre som avvik eller manuell behandling.

Q.6 Beslutningsmodell

Autorisasjon gjennomføres som en sekvens av vurderinger.

Først identifiseres bruker. Deretter fastslås rolle og kontekst. Systemet identifiserer hvilket objekt det forespørres tilgang til og validerer relasjon mellom bruker og objekt. Relevante regler anvendes før det tas beslutning om tilgang gis eller nektes.

Modellen skal anvendes konsistent i hele løsningen.

Q.7 Typiske misbruksscenarioer

Følgende scenarier illustrerer hva modellen skal forhindre.

En bruker oppgir en annen persons fødselsnummer for å hente data.

En fartøyeier forsøker å registrere personer som ikke er knyttet til fartøyet.

En bruker forsøker å få tilgang til fartøy eller ordninger uten tilknytning til fartøyet.

En bruker får tilgang til rådata fra eksterne registre.

Klientapplikasjonen skjuler data, men backend returnerer dem likevel.

Løsningen skal utformes slik at slike scenarier ikke gir tilgang til data eller funksjoner.

Q.8 Sammenheng med øvrige vedlegg

Dette vedlegget utdyper kravene til autorisasjon i vedlegg TA-01-C og skal sees i sammenheng med funksjonelle krav til søknadsbehandling, krav til håndtering av person- og fartøydata og krav til logging og sporbarhet.

Vedlegg TA-01-Q gir kontekst og forklaring. Bindende krav fremgår av vedlegg TA-01-C.

Q.9 Forvaltning av tilganger

Forvaltning av tilgang i løsningen baseres på at tilgang ikke gis direkte til brukere, men gjennom relasjoner til objekter i domenet, herunder fartøy, person eller sak.

Eksterne brukere autentiseres gjennom ekstern identitetsleverandør. Tilgang til data og funksjoner bestemmes deretter av hvilke relasjoner som er registrert i løsningen.

Relasjoner kan etableres og vedlikeholdes av autoriserte interne brukere. Dette omfatter blant annet registrering av tilknytning mellom bruker og fartøy, og hvilke rettigheter som følger av denne tilknytningen.

Typiske eksempler på slike relasjoner er:

- fartøyeier med tilgang til eget fartøy
- skipper eller representant med tilgang til fartøy og tilhørende søknader
- person med tilgang til egne saker

Når en relasjon etableres, vil dette gi grunnlag for autorisasjon i henhold til reglene beskrevet i dette vedlegget.

Når en relasjon endres eller fjernes, skal dette umiddelbart påvirke hvilke data og funksjoner brukeren har tilgang til.

Forvaltning av relasjoner skal være sporbar. Det skal være mulig å etterprøve hvem som har gitt, endret eller fjernet tilgang, og på hvilket grunnlag dette er gjort.