

TA-01-C

Vedlegg C – Sikkerhet / Identitetsarkitektur

Nytt Fagsystem

GARANTIKASSEN FOR FISKERE

C.1. Formål.....	2
C.2. Overordnet arkitektur.....	2
C.3. Realm-struktur i IAM-løsningen	2
C.4. Nettverkssoneinndeling	3
C.5. Autentiseringsflyt	3
C.6. Token-separasjon og sikkerhet.....	3
C.7. Autorisasjon.....	3
C.7A Domeneautorisasjon	4
C.7B Forvaltning av tilganger	5
C.8. Revisjon og sporbarhet	6
C.9. Fordeler med to-realm og separate gateways.....	6
C.10 Trusselmodell.....	7
C.10.1 Formål.....	7
C.10.2 Angrepsflater	7
C.10.3 Relevante trusselkategorier.....	7
C.11 Spesifikasjon: Identitet og tilgang.....	9
C.12 Komponentbeskrivelse	11
C.13 Soneinndelingsprinsipp	13
C.14 Ikke-funksjonelle krav knyttet til komponentene.....	14

C.1. Formål

Dette kapitlet beskriver formålet med identitets- og tilgangsarkitekturen for løsningen. Arkitekturen skal sikre at både interne og eksterne brukere autentiseres og autoriseres på en kontrollert og etterprøvbart måte, samtidig som systemet opprettholder tydelig separasjon mellom brukergrupper og sikkerhetssoner.

Feil i denne delen vil kunne gi uautorisert tilgang, feil rollebruk og manglende sporbarhet.

C.1.1 Løsningen skal etablere en sikker, skalerbar og revisjonsvennlig identitetsarkitektur.

C.1.2 Løsningen skal støtte både interne og eksterne brukere gjennom separate identitetsdomener.

C.1.3 Løsningen skal basere autentisering på eksterne identitetsleverandører.

C.1.4 Løsningen skal sikre tydelig separasjon mellom autentisering, autorisasjon og forretningslogikk.

C.2. Overordnet arkitektur

Løsningen bygger på prinsippet om tydelig separasjon mellom identitet, API og forretningslogikk. Autentisering håndteres av eksterne identitetsleverandører, mens applikasjonen forholder seg til tokens utstedt av IAM-løsningen (Identity and Access Management).

Komponenter og ansvar er definert i C.12, og deres plassering i sikkerhetssoner er beskrevet i C.13.

Feil forståelse av denne strukturen vil føre til feil implementasjon, svakere sikkerhet og økt kompleksitet.

C.2.1 Løsningen skal benytte eksterne Identity Providers for autentisering.

C.2.2 IAM-løsningen skal fungere som identity broker og token issuer.

C.2.3 Applikasjoner skal validere tokens utstedt av IAM-løsningen.

C.2.4 Trafikk skal separeres mellom intern og ekstern sone via egne gateways.

C.3. Realm-struktur i IAM-løsningen

Dette kapitlet beskriver hvordan identitetsdomener skal struktureres. Separasjon av interne og eksterne brukere er et sentralt sikkerhetstiltak.

Manglende separasjon vil kunne føre til feil tilgang og økt risiko for misbruk.

C.3.1 Løsningen skal benytte et eget identitetsdomene for eksterne brukere.

C.3.2 Eksterne brukere skal autentiseres via nasjonal identitetsinfrastruktur (ID Porten).

C.3.3 Løsningen skal benytte et eget identitetsdomene for interne brukere.

C.3.4 Interne brukere skal autentiseres via virksomhetens identitetsløsning.

C.3.5 Rollemodell skal være kontrollert og basert på minste privilegium.

C.4. Nettverkssoneinndeling

Dette kapittelet beskriver hvordan løsningen deles inn i sikkerhetssoner. Soneinndeling er et grunnleggende tiltak for å redusere angrepsflate og beskytte interne systemer.

Detaljert plassering av komponenter fremgår av C.13.

C.4.1 Løsningen skal ha en ekstern sone for komponenter eksponert mot internett.

C.4.2 Løsningen skal ha en intern sone for API-er, kjernetjenester og databaser.

C.4.3 Intern sone skal ikke være direkte tilgjengelig fra internett.

C.4.4 Trafikk mellom soner skal være eksplisitt kontrollert og dokumentert.

C.5. Autentiseringsflyt

Dette kapittelet beskriver hvordan autentisering gjennomføres. Flyten skal sikre at brukere identifiseres korrekt før tilgang gis.

Feil i autentiseringsflyten vil kunne gi uautorisert tilgang eller feil identitet.

C.5.1 Eksterne brukere skal autentiseres via ekstern identitetsleverandør.

C.5.2 IAM-løsningen skal validere og videreutstede tokens.

C.5.3 Interne brukere skal autentiseres via virksomhetens identitetsløsning.

C.5.4 API skal validere tokenets signatur, gyldighet og opprinnelse før tilgang gis

C.6. Token-separasjon og sikkerhet

Dette kapittelet beskriver prinsipper for håndtering av tokens. Tokens skal ikke kunne misbrukes på tvers av soner eller brukergrupper.

Feil håndtering vil kunne gi uautorisert tilgang til interne systemer.

C.6.1 Ekstern API skal kun akseptere tokens fra eksternt identitetsdomene.

C.6.2 Intern API skal kun akseptere tokens fra internt identitetsdomene.

C.6.3 Tokens skal ikke kunne brukes på tvers av identitetsdomener eller sikkerhetssoner

C.7. Autorisasjon

Dette kapittelet beskriver hvordan tilgang til funksjoner og data styres. Autorisasjon skal være sentralisert og basert på både roller og forretningsregler.

Feil autorisasjon vil føre til uautorisert tilgang eller feil behandling.

C.7.1 Autorisasjon skal håndteres i backend.

C.7.2 Tilgang skal baseres på roller og forretningsregler.

C.7.3 Forretningsrettigheter skal ikke kun styres av IAM-løsningen.

C.7A Domeneautorisasjon

Dette kapittelet beskriver hvordan tilgang til data og funksjoner skal styres basert på brukerens identitet og relasjon til objekter i domenet. Formålet er å sikre at brukere kun får tilgang til opplysninger de er autorisert til å se eller behandle, og å hindre uautorisert innsyn i person-, fartøy- og saksdata.

Kapittelet supplerer de generelle autorisasjonsprinsippene i C.7 ved å konkretisere hvilke regler som gjelder for GFFs fagområde. Uten tydelige domeneautorisasjonsregler vil løsningen kunne gi korrekt autentiserte brukere tilgang til feil data.

Domeneautorisasjon er nærmere beskrevet i Vedlegg Q – Domeneautorisasjonsmodell.

C.7A.1 Løsningen skal sikre at eksterne brukere kun får tilgang til data og funksjoner som er knyttet til brukerens egen identitet eller annen dokumentert relasjon i domenet.

C.7A.2 Løsningen skal validere at alle forespørsler om tilgang til data inneholder entydig identitet for innlogget bruker, og at denne identiteten benyttes som grunnlag for autorisasjonsvurdering.

C.7A.3 Løsningen skal forhindre at eksterne brukere kan søke opp, lese eller behandle opplysninger om andre personer ved å oppgi identifikatorer som fødselsnummer, navn, organisasjonsnummer eller tilsvarende.

C.7A.4 Løsningen skal validere at oppslag mot interne og eksterne datakilder kun utføres for objekter som den autentiserte brukeren har autorisert tilgang til.

C.7A.5 Løsningen skal sikre at tilgang til personopplysninger er begrenset til:

- a) den innloggede personen selv, eller
- b) personer som brukeren har en dokumentert og godkjent relasjon til i domenet.

C.7A.6 Løsningen skal validere at bruker kun kan opprette, lese, endre eller følge opp saker for fartøy som brukeren har dokumentert tilknytning til.

C.7A.7 Løsningen skal validere at bruker kun kan opprette eller følge opp søknader for personer som brukeren har autorisert relasjon til.

C.7A.8 Ved fellesmelding skal løsningen validere at bruker kun kan inkludere eller følge opp mannskap som er knyttet til det aktuelle fartøyet i henhold til godkjent datagrunnlag.

C.7A.9 Løsningen skal ikke tilby funksjonalitet som muliggjør generelle oppslag i person-, fartøy- eller saksdata uten at det foreligger autorisert relasjon til objektet.

C.7A.10 Løsningen skal ikke eksponere rådata fra eksterne registre direkte til eksterne brukere.

C.7A.11 Løsningen skal begrense data hentet fra eksterne registre til det som er nødvendig for den aktuelle funksjonen eller saken.

C.7A.12 Løsningen skal sikre at autorisasjonsregler håndheves i backend, og at frontend ikke benyttes som sikkerhetsbarriere.

C.7A.13 Løsningen skal anvende prinsippet om minste privilegium ved tildeling av tilgang til data og funksjoner.

C.7A.14 Dersom løsningen ikke entydig kan validere at bruker har rett til tilgang, skal tilgang nektes.

C.7A.15 Løsningen skal støtte håndtering av slike tilfeller som avvik, inkludert mulighet for manuell behandling der dette er nødvendig.

C.7A.16 Løsningen skal logge autorisasjonsbeslutninger for sikkerhetsrelevante operasjoner med:

- a) brukeridentitet
- b) rolle
- c) tidspunkt
- d) målobjekt
- e) resultat av autorisasjonsvurdering

C.7A.17 Løsningen skal sikre at loggdata fra autorisasjonsbeslutninger kan benyttes til revisjon, etterkontroll og hendelsesanalyse.

C.7B Forvaltning av tilganger

Dette kapittelet beskriver krav til forvaltning av tilgang for interne og eksterne brukere. Formålet er å sikre at tilgang til data og funksjoner kan etableres, endres og fjernes på en kontrollert og etterprøvbar måte.

C.7B.1 Løsningen skal støtte administrasjon av tilgang for eksterne brukere basert på relasjon til fartøy, person eller sak.

C.7B.2 Løsningen skal gi autoriserte interne brukere mulighet til å registrere, endre og fjerne relasjoner som danner grunnlag for tilgang.

C.7B.3 Løsningen skal sikre at tildeling av tilgang til fartøy og tilhørende data kun kan utføres av autoriserte interne brukere.

C.7B.4 Løsningen skal støtte at eksterne brukere kan få tilgang til fartøy eller saker basert på godkjent relasjon, herunder fartøyeier, skipper eller annen representant.

C.7B.5 Løsningen skal sikre at endringer i relasjoner som påvirker tilgang får umiddelbar effekt for autorisasjon.

C.7B.6 Løsningen skal logge alle endringer i tilgang og relasjoner med:

- a) identitet på den som utfører endringen
- b) tidspunkt
- c) hva som er endret
- d) tidligere og ny verdi

C.7B.7 Løsningen skal støtte at tilgang kan tilbakekalles uten opphold dersom relasjonsgrunnlaget ikke lenger er gyldig.

C.8. Revisjon og sporbarhet

Dette kapittelet beskriver krav til logging og sporbarhet.

Manglende sporbarhet vil gjøre det vanskelig å etterprøve hendelser og avdekke avvik.

C.8.1 Autentiseringshendelser skal logges.

C.8.2 API-operasjoner skal logges med identitet og kontekst.

C.8.3 Loggdata skal kunne brukes til revisjon og analyse.

C.9. Fordeler med to-realm og separate gateways

Dette kapittelet beskriver hvorfor valgt identitetsarkitektur er hensiktsmessig.

Arkitekturen baserer seg på separasjon mellom interne og eksterne brukere, egne identitetsdomener og tydelig soneinndeling.

Denne strukturen bidrar til bedre sikkerhet, enklere drift og større fleksibilitet ved endringer. Uten denne separasjonen vil løsningen bli mer kompleks, vanskeligere å sikre og mer sårbar for feil og misbruk.

C.9.1 Separasjon mellom interne og eksterne brukere reduserer risiko for uautorisert tilgang på tvers av brukergrupper.

C.9.2 Tydelig soneinndeling og separate gateways bidrar til redusert angrepsflate og bedre kontroll på trafikk mellom soner.

C.9.3 Bruk av separate identitetsdomener gir bedre kontroll på autentisering og rollemodell for ulike brukergrupper.

C.9.4 Arkitekturen legger til rette for fleksibel utskiftning eller endring av identitetsleverandører uten å påvirke applikasjonslogikk.

C.9.5 Separasjon mellom identitet, API og forretningslogikk gir bedre vedlikeholdbarhet og enklere videreutvikling av løsningen.

C.10 Trusselmodell

Dette kapittelet beskriver relevante trusler og hvordan arkitekturen håndterer disse. Trusselmodellen gir kontekst for sikkerhetskravene og gjør det mulig å vurdere om løsningen er tilstrekkelig beskyttet.

Uten en tydelig trusselmodell er det vanskelig å vurdere om sikkerhetstiltakene er tilstrekkelige.

C.10.1 Formål

Formålet med trusselmodellen er å identifisere relevante sikkerhetstrusler knyttet til autentisering, autorisasjon og nettverkseksposering i GFFs moderniserte løsning, samt beskrive hvordan arkitekturen reduserer risiko.

C.10.2 Angrepsflater

Følgende hovedangrepsflater identifiseres:

1. Ekstern web-portal (gff-portal)
2. Ekstern API (gff-public-api)
3. IAM-løsningen (eksternt identitetsdomene)
4. Identity Providers (ID-porten, Microsoft Entra ID)
5. Intern admin-portal
6. Intern API
7. Databaser og domene-/kjernetjenester

C.10.3 Relevante trusselkategorier

Dette delkapittelet beskriver sentrale trusselkategorier som er relevante for løsningens identitets-, tilgangs- og sikkerhetsarkitektur. For hver trusselkategori beskrives overordnet risiko og sentrale tiltak som skal redusere sannsynligheten for eller konsekvensen av sikkerhetsbrudd.

C.10.3.1 Uautorisert tilgang (Authentication bypass)

Risiko:

- Forsøk på å omgå autentisering.
- Misbruk av tokens.

- Replay-angrep.

Tiltak:

- Kun IAM-løsningen-utstedte tokens aksepteres.
- Validering av:
 - iss (issuer)
 - aud (audience)
 - exp (expiration)
 - signatur (JWT signature verification via JWKS).
- Separate realms for intern og ekstern bruk.
- Kort levetid på access tokens.

C.10.3.2 Token misbruk mellom soner

Risiko:

- Ekstern bruker forsøker å bruke token mot intern API.
- Intern token misbrukes mot ekstern API.

Tiltak:

- Ekstern API validerer kun issuer = gff-external.
- Intern API validerer kun issuer = gff-internal.
- Separate gateways og nettverkssoner.

Dette etablerer “defense in depth”.

C.10.3.3 Kompromittert ekstern konto

Risiko:

- En fiskers BankID kompromitteres.
- En Microsoft-konto kompromitteres.

Tiltak:

- Autentisering skjer via etablerte og sterke Identity Providers:
 - ID-porten (BankID mv.)
 - Microsoft Entra ID.
- Applikasjonen lagrer ikke passord.
- Autorisasjon baseres også på domene-/forretningsregler (ikke kun identitet).

C.10.3.4 Misbruk av privilegier (Privilege escalation)

Risiko:

- Bruker forsøker å oppnå høyere rettigheter.

- Manipulering av klient-side logikk.

Tiltak:

- Rollevalidering skjer alltid i backend.
- Frontend kan ikke bestemme tilgang.
- Roller og claims valideres server-side.
- Intern rollemodell baseres på Entra-grupper.

C.10.3.5 Angrep mot ekstern gateway

Risiko:

- DDoS
- SQL injection
- Cross-site scripting

Tiltak:

- Web Application Firewall (WAF).
- Rate limiting.
- TLS-terminering i gateway.
- Logging og overvåkning.

C.10.3.6 Datainnbrudd

Risiko:

- Uautorisert tilgang til databaser.

Tiltak:

- Databaser plassert i intern sone.
- Ingen direkte eksponering mot internett.
- Kun API-lag har tilgang.
- Minst mulig privilegier (least privilege).

C.11 Spesifikasjon: Identitet og tilgang

Dette kapittelet samler konkrete og testbare krav til identitet og tilgangsstyring. Kravene er styrende for implementasjon og skal sikre at løsningen oppfyller krav til sikker autentisering, korrekt autorisasjon og tydelig separasjon mellom brukergrupper. Uklare eller manglende krav i denne delen vil føre til inkonsistent implementasjon og økt risiko for sikkerhetsbrudd.

- C.11.1 Løsningen skal etablere to separate identitetsdomener.
- C.11.2 Eksternt identitetsdomene skal benyttes for alle eksterne brukere.
- C.11.3 Internt identitetsdomene skal benyttes for alle interne brukere.
- C.11.4 Løsningen skal integreres med ekstern identitetsleverandør for autentisering av eksterne brukere.
- C.11.5 Løsningen skal integreres med intern identitetsleverandør for autentisering av ansatte.
- C.11.6 Løsningen skal ikke lagre eller håndtere passord lokalt.
- C.11.7 Alle API-endepunkter skal kreve gyldig Bearer token.
- C.11.8 Token skal valideres med hensyn til signatur, utløpstid, issuer og audience.
- C.11.9 Ekstern API skal kun akseptere tokens fra eksternt identitetsdomene.
- C.11.10 Intern API skal kun akseptere tokens fra internt identitetsdomene.
- C.11.11 Rollemodell for interne brukere skal styres via identitetsleverandør.
- C.11.12 Rollemodell for eksterne brukere skal være definert og begrenset.
- C.11.13 Forretningsmessige rettigheter skal håndteres i domenelaget og ikke kun i IAM-løsningen.
- C.11.14 Ekstern gateway skal være plassert i ekstern sone.
- C.11.15 Intern API og databaser skal være plassert i intern sone.
- C.11.16 Trafikk mellom soner skal begrenses til eksplisitt tillatte forbindelser.
- C.11.17 Autentiseringshendelser skal logges.
- C.11.18 Forretningskritiske operasjoner skal logges med brukeridentitet, rolle, tidsstempel og korrelasjons-ID.
- C.11.19 Loggdata skal kunne benyttes til revisjon og hendelsesanalyse.
- C.11.20 Løsningen skal støtte horisontal skalering av identitets- og API-komponenter.
- C.11.21 Løsningen skal kunne utvides med nye identitetsleverandører uten endring i applikasjonslogikk.
- C.11.22 Løsningen skal støtte fremtidige klienttyper som mobilapplikasjoner og eksterne API-integrasjoner.
- C.11.23 Tekniske identiteter og tjenestekontoer skal ha entydig identitet og kun tildeles de rettigheter som er nødvendige for tjenestens funksjon.
- C.11.24 Bruk av tekniske identiteter og tjenestekontoer skal kunne spores til aktuell systemkomponent, integrasjon eller prosess.
- C.11.25 Tekniske identiteter skal ikke benyttes som erstatning for personlig brukeridentitet ved handlinger som utføres av en identifiserbar bruker.

C.12 Komponentbeskrivelse

Dette kapittelet beskriver hovedkomponentene i identitets- og tilgangssarkitekturen og deres ansvar. En tydelig komponentforståelse er avgjørende for korrekt implementasjon og drift.

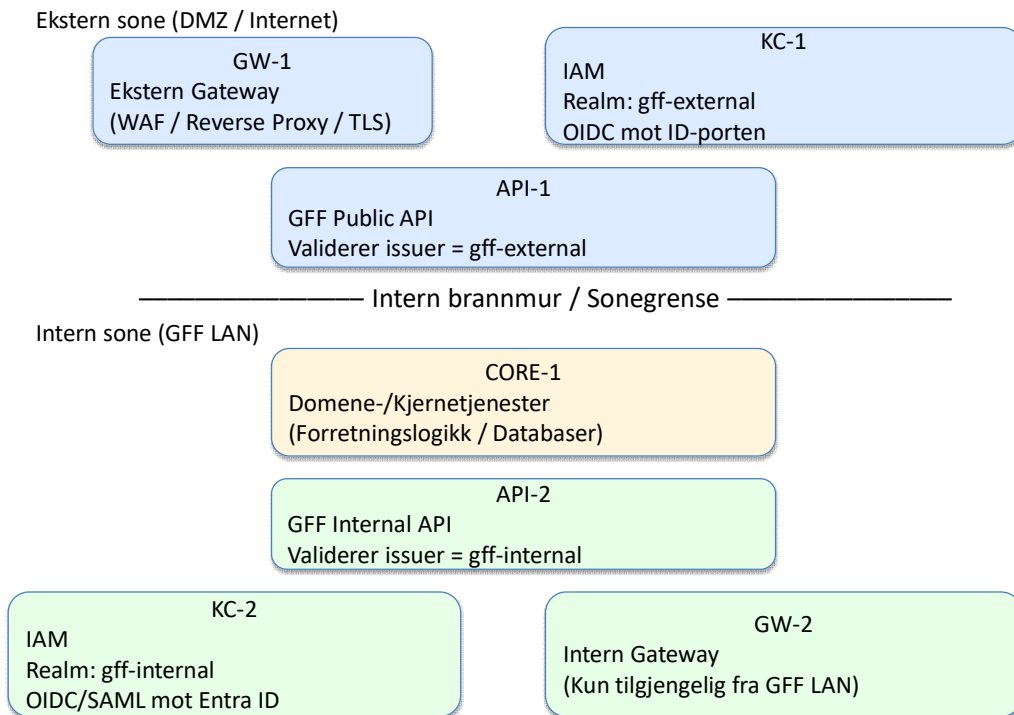
Komponentene som beskrives i dette kapittelet viser løsningens logiske plassering og samhandling med GFFs nettverks- og sikkerhetsinfrastruktur.

Etablering, drift og forvaltning av nettverks- og sikkerhetsinfrastruktur, herunder brannmur, Web Application Firewall (WAF), gateways, reverse proxy, DDoS-beskyttelse og tilsvarende infrastrukturkomponenter, er GFFs ansvar og inngår ikke i leverandørens leveranse.

Leverandøren skal sikre at løsningen kan integreres med og fungere innenfor denne infrastrukturen, samt dokumentere nødvendige kommunikasjonsbehov, porter, protokoller, endepunkter og øvrige tekniske forutsetninger.

Uklare ansvarsforhold mellom komponenter vil føre til feil implementasjon, sikkerhetshull og økt kompleksitet.

GFF – Identitets- og Tilgangssarkitektur (To Realms / Separate Gateways)



ID	Komponent	Funksjon	Ansvar	Sikkerhetskrav
GW-1	Ekstern Gateway (WAF / Reverse Proxy / TLS termination)	Håndterer all innkommende trafikk fra internett. Utfører TLS termination, routing og beskyttelse mot angrep.	- Terminere HTTPS - Rute trafikk til IAM-løsningen (external) og API-1 - Rate limiting - Logging	- Kun port 443 eksponert - Web Application Firewall (WAF) - DDoS-beskyttelse - Streng TLS-konfigurasjon (TLS 1.2+)
KC-1	IAM-løsning – Identitetsdomene: gff-external	Identity broker for eksterne brukere. Integrerer mot ID-porten (OIDC). Utsteder JWT tokens.	- Federere autentisering via ID-porten - Utstedte access tokens - Rolle-/claim-mapping - Event logging	- Kun nødvendige endpoints eksponert - OIDC-validering mot ID-porten - Signering med private nøkler - Logging av alle autentiseringshendelser
API-1	GFF Public API	Ekstern API for søknader, status, dokumentopplasting mv.	- Validering av JWT (issuer, audience, signature) - Autorisasjon basert på roller og domene-regler - Kalle CORE-1	- Aksepterer kun issuer = gff-external - Input-validering - Rate limiting - Ingen direkte databaseeksponering
CORE-1	Domene-/Kjernetjenester	Implementerer forretningslogikk og håndterer data.	- Søknadsbehandling - Fartøy- og eierskapslogikk - Rettighetsvurdering - Datarevisjon logging	- Ikke eksponert mot internett - Tilgang kun fra API-lag - Rollebasert tilgangskontroll - Logging og sporbarhet
API-2	GFF Internal API	API for interne ansatte (saksbehandling, administrasjon).	- Validering av interne tokens - Rollebasert autorisasjon - Tilgang til CORE-1	- Aksepterer kun issuer = gff-internal - Ingen offentlig eksponering - Streng rollevalidering
KC-2	IAM-løsning – Identitetsdomene: gff-internal	Identity broker for ansatte. Integrerer mot Microsoft Entra ID (OIDC/SAML).	- Federere autentisering via Entra ID - Mappe Entra-grupper til roller - Utstedte interne tokens	- Kun tilgjengelig via intern gateway - Streng SSL/TLS - Gruppebasert rolle-mapping

ID	Komponent	Funksjon	Ansvar	Sikkerhetskrav
GW-2	Intern Gateway	Inngangspunkt for interne systemer innenfor GFF LAN.	- Routing av intern trafikk - Begrense tilgang til API-2 og KC-2	- Ikke eksponert mot internett - IP-restriksjoner - Intern TLS

C.12.1 Løsningen skal ha tydelig definerte komponenter og ansvarsgrenser for Identity and Access Management (IAM), API-lag, kjernetjenester og øvrige applikasjonskomponenter, samt dokumenterte grensesnitt mot GFFs nettverks- og sikkerhetsinfrastruktur.

C.12.2 Som del av detaljdesign og etablering av løsningen skal nødvendige forbindelser, protokoller, endepunkter og øvrige tekniske forutsetninger for samhandling med GFFs infrastruktur dokumenteres.

Dokumentasjonen skal være tilstrekkelig detaljert til at GFF kan etablere, konfigurere, sikre, drifte og forvalte nødvendig kommunikasjon mellom løsningens komponenter og GFFs infrastruktur.

C.12.3 Løsningen skal kunne benyttes bak GFFs eksterne nettverks- og sikkerhetskomponenter for kontroll og beskyttelse av innkommende trafikk. Etablering og forvaltning av slike komponenter inngår ikke i leverandørens leveranse.

C.12.4 IAM-løsningen skal håndtere løsningens identitets- og tilgangsfunksjoner, herunder integrasjon mot relevante identitetsleverandører, autentiseringsflyt og tokenutstedelse, i samsvar med kravene i dette vedlegget.

C.12.5 API-laget skal validere tokens, håndheve autorisasjon og sikre kontrollert tilgang til løsningens tjenester og data. API-laget skal utformes slik at kommunikasjon kan styres gjennom GFFs etablerte nettverks- og sikkerhetsinfrastruktur.

C.12.6 Kjernetjenestene skal implementere løsningens forretningslogikk og skal ikke være direkte eksponert mot internett. Tilgang til kjernetjenestene skal skje gjennom definerte og sikrede grensesnitt.

C.13 Soneinndelingsprinsipp

Dette kapittelet beskriver løsningens plassering og kommunikasjonsmønster i GFFs nettverks- og sikkerhetsarkitektur.

GFF er ansvarlig for etablering, drift og forvaltning av underliggende nettverks- og sikkerhetsinfrastruktur, herunder soner, brannmur, gateways, Web Application Firewall (WAF), reverse proxy, DDoS-beskyttelse og tilsvarende infrastrukturkomponenter.

Leverandøren skal utforme løsningen slik at den kan plasseres og operere innenfor denne arkitekturen, og skal dokumentere nødvendige kommunikasjonsbehov mellom løsningens komponenter og GFFs infrastruktur.

Ekstern sone:

- eksternt identitetsdomene / IAM-komponenter som skal være tilgjengelige for eksterne brukere
- eksternt API
- Min Side og øvrige eksternt tilgjengelige applikasjonskomponenter der dette er relevant

Intern sone:

- internt identitetsdomene / IAM-komponenter
- internt API
- kjernetjenester
- databaser
- øvrige interne applikasjonskomponenter

Det skal ikke være direkte nettverkstilgang fra internett til kjernetjenester, interne API-er eller databaser.

C.13.1 Løsningens komponenter som skal være tilgjengelige for eksterne brukere, skal kunne plasseres og operere i GFFs eksterne sikkerhetssone.

C.13.2 Interne API-er, kjernetjenester, databaser og øvrige interne komponenter skal kunne plasseres og operere i GFFs interne sikkerhetssone.

C.13.3 Løsningen skal utformes slik at interne komponenter ikke krever direkte nettverkstilgang fra internett.

C.13.4 Som del av etableringen av løsningen skal nødvendige protokoller, porter, endepunkter og kommunikasjonsretninger dokumenteres.

Dokumentasjonen skal gi GFF tilstrekkelig grunnlag for å konfigurere nødvendig nettverks- og sikkerhetsinfrastruktur og for å kontrollere at kommunikasjon mellom soner og komponenter er i samsvar med løsningens sikkerhetsarkitektur.

C.14 Ikke-funksjonelle krav knyttet til komponentene

Dette kapittelet beskriver ikke-funksjonelle krav til løsningens applikasjons- og identitetskomponenter. Kravene gjelder leverandørens løsning og dens evne til å fungere innenfor GFFs etablerte nettverks- og sikkerhetsinfrastruktur.

Kravene innebærer ikke at leverandøren skal etablere eller forvalte GFFs nettverks-, gateway-, brannmur-, Web Application Firewall (WAF)- eller øvrige sikkerhetsinfrastruktur.

C.14.1 Løsningens applikasjonskomponenter skal kunne skaleres horisontalt der dette er relevant for å ivareta tilgjengelighet, ytelse og kapasitetsbehov.

C.14.2 Identity and Access Management (IAM)-komponenter som inngår i leverandørens løsning skal kunne etableres med nødvendig redundans og skalerbarhet for å understøtte løsningens krav til tilgjengelighet og kapasitet.

C.14.3 Løsningen skal støtte sentral logging og kunne tilgjengeliggjøre relevante logger og hendelser for GFFs etablerte løsninger for overvåkning og sikkerhetsanalyse.

C.14.4 Løsningen skal kunne utvides og skaleres uten vesentlig ombygging av arkitekturen.