Norsk helsenett

SSA-R Bilag 1 Vedlegg 1 – Kundens Kravspesifikasjon

Avtale om Antivirustjeneste for Helsenorge

Saksnr 24/01596

Innhold

Innhold

1 Innledning

Dette bilaget oppstiller Kundens krav til ytelsen. Kravene gjøres gjeldende for alle leveranser under rammeavtalen. Leverandørens besvarelse av kravene i dette dokumentet skal gjøres i ***Bilag 1 Vedlegg 2 Leverandørens løsningsbeskrivelse.***

NHN skal etter anskaffelse ha tilgang til et produkt/løsning som dekker Helsenorge og andre tjenester i NHN sine behov for antivirus med funksjonalitet for skanning av dokumenter og vedlegg.

Løsningen skal ikke dekke behovet for endepunkt-sikkerhet som typisk skanner minne, lokale disker eller annen generell infrastruktur da dette er dekket i andre løsninger allerede.

2 Krav og kravtyper

2.1 Kravtyper

Nr.: Kravpunktets unike løpenummer
Beskrivelse: Tekst som beskriver kravet
Type krav: Se tabell nedenfor

Absolutte krav (A)	Kravet MÅ tilfredsstilles. Kravet er å anse som et minimumskrav.
Absolutte krav (A)*	Kravet MÅ tilfredsstilles. Kravet er å anse som et minimumskrav, hvor «mer er bedre». Stjerne tilsier at kravet er gjenstand for relativ vurdering.
Ønskede krav (B)	Kravet BØR tilfredsstilles, men det er ikke et absolutt krav. Svar vil likevel ha betydning for evaluering av tilbudet.
Info (I)	Ikke et direkte krav til leveransen, men leverandøren skal i sin løsningsbeskrivelse gi utfyllende informasjon. Svar vil ha betydning for evaluering av tilbudet.

2.2 Leverandørens besvarelse

Tilbys: I hvilken grad leverandøren kan tilfredsstille kravet (Ja, Nei, Delvis). For krav som besvares med Delvis, må det i løsningsbeskrivelsen særskilt utdypes hva som ikke kan tilfredsstilles.

Løsningsbeskrivelse: Utfyllende informasjon om hvordan kravet tilfredsstilles.

Der Leverandøren f.eks. av plasshensyn ikke finner det hensiktsmessig å legge løsningsbeskrivelsen inn i selve kravtabellen, kan beskrivelsen legges i eget vedlegg. I så fall skal det i kravtabellen gis referanse til hvor løsningsbeskrivelsen ligger, og det skal i løsningsbeskrivelsen klart fremkomme hvilket krav som utdypes.

Leverandøren er selv ansvarlig for å beskrive alle nødvendige løsningselementer for å få en komplett løsning, selv om ikke alle disse er kravsatt.

3 Overordnet om ytelsen

3.1 Formål med anskaffelsen

Helsenorge plattformen må fornye en antivirus/anti-skadevare tjeneste (Løsningen) og ønsker å hente inn tilbud fra aktuelle leverandører. En ny løsning skal i utgangspunktet benyttes av Helsenorge-plattformen, men må kunne utvides senere til også å støtte andre tjenester som driftes av Helsenett. Det er derfor viktig at løsningen er skalerbar og har tilpasningsmuligheter for å være en sentral antivirus-tjeneste for Norsk Helsenett.

Løsningen er ikke tiltenkt benyttet for standard endpoint-scanning, men skal i utgangspunktet støtte skanning av dokumenter og vedlegg basert på at helsenorge.no ber antivirus-tjenesten om dette via et API eller annet kall som kan utføres programmatisk.

3.2 Bakgrunn for dagens løsning

Helsenorge og andre tjenester i NHN har et behov for å skanne dokumenter og innhold som sendes mellom innbyggere og helsesektoren for å ivareta sikkerheten ved håndtering av slikt innholdet.
Tidligere har vi benyttet nettverkstjenester (Proxy) for å gjennomføre slik skanning, men som kravene i anskaffelsen viser, så ønsker vi nå å legge til rette for at vi kan kalle antivirus-løsningen på flere måter og mer fleksibelt enn i dag

3.3 Hva slags informasjon skal skannes?

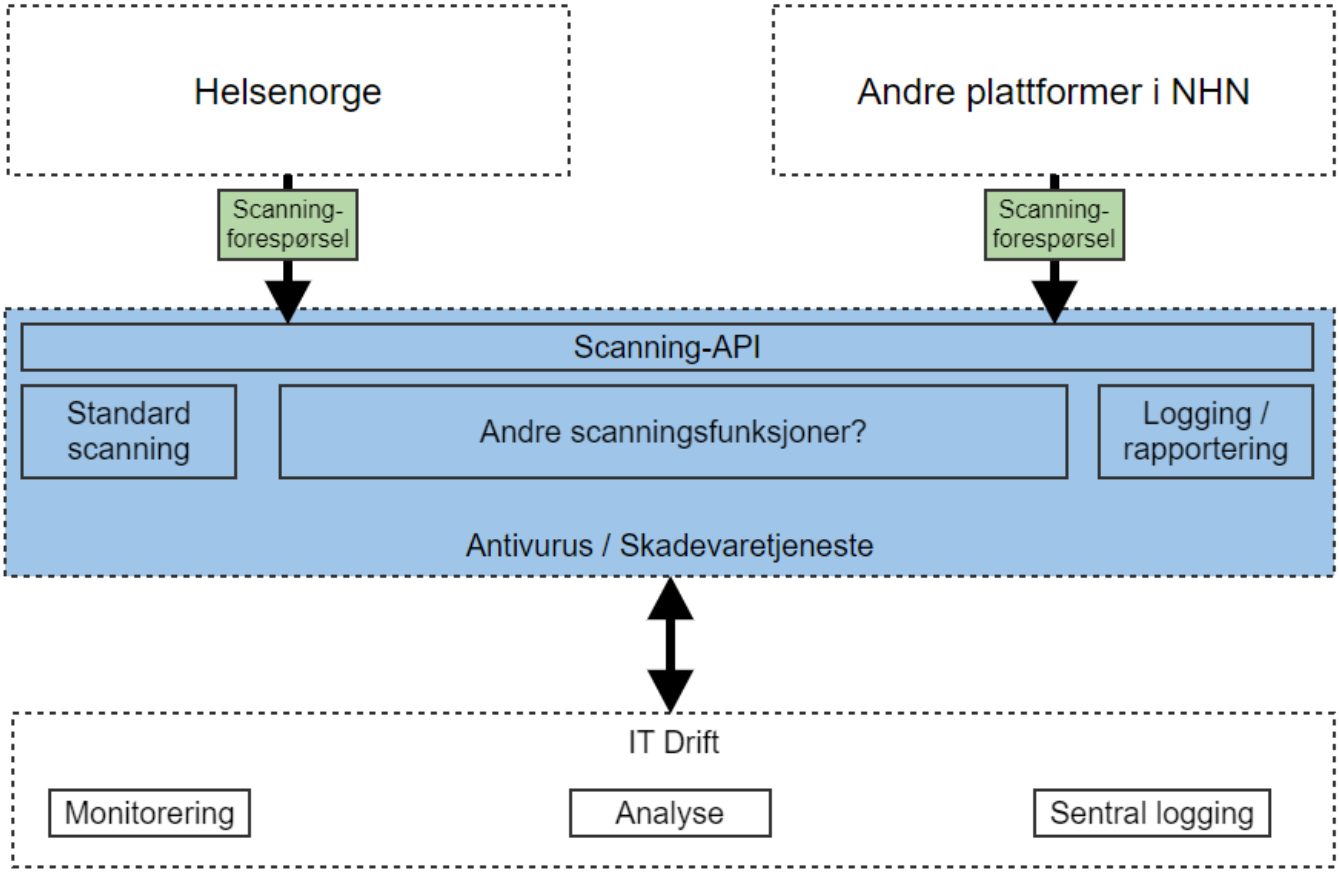
Informasjonstype som vanligvis skal skannes inkluderer *dokumenter som håndteres i Helsenorge; typisk PDF, Word, bildefiler eller andre standardformater. Dokumenter eller informasjon kan også være del av en sammensatt fil som inneholder flere enn 1 type innhold; typisk en base64 enkodet fil i en struktur som sendes til et API (se krav under)*

Vi utfordrer leverandøren til å gi mer informasjon om deres løsning også kan skanne annen type informasjon som del av løsningen eller som opsjon; for eksempel URL'er, skanninger av fritekstfelt for HTML kode eller lignende. Vi kan score løsninger som kan utvides med mer funksjonalitet høyere enn løsninger med bare en ren dokumentskanning

3.4 Overordnet design og krav

Tegningen under viser konseptet slik det er tenkt, der de blå tjenestene er det som skal leveres av ny AV tjeneste

Vi er i ferd med å flytte flere av tjenestene våre over til NHN sin private skyplattform som kjører i et containermiljø.


Helsenorge
Andre plattformer i NHN
Scanning-forespørsel
Scanning-forespørsel
Scanning-API
Standard scanning
Andre scanningsfunksjoner?
Logging / rapportering
Antivurus / Skadevaretjeneste
IT Drift
Monitorering
Analyse
Sentral logging

4 Brukerscenarier – Hva skal ny skadevaretjeneste løse?

Under er hovedscenario for løsningen:

4.1 Scenario: Bruk av skadevaretjenesten

Scenario 1:
Dokumenter / vedlegg / informasjon som sendes fra en bruker til Helsenorge

1. En bruker laster opp et dokument via nettleser eller annen klient til Helsenorge.
2. Helsenorge sender et kall til skadevare-løsningens API og ber om at informasjonen skannes
3. Helsenorge får tilbakemelding fra skadevareløsningen om dokumentet/informasjonen anses som trygt, evt. inneholder skadevare
4. Helsenorge kan da, basert på skanningen, vurdere hvordan dokumentet skal håndteres mens brukeren venter på svar på opplastingen

Scenario 2:
Dokumenter / vedlegg / informasjon som behandles i plattformen som del av system til system

1. Et dokument eller annen informasjon sendes/mottas via en meldingstjeneste på Helsenorge (f.eks., AMQP) eller via et API (maskin til maskin)
2. Helsenorge sender dokumentet til skadevareløsningen for skanning
3. Helsenorge får tilbakemelding fra skadevaretjenesten om dokumentet/informasjonen anses som trygt, evt. inneholder skadevare

Kundens krav				**Leverandørens besvarelse**	
Nr.	**Beskrivelse**	**Dokumentasjonskrav**	**Type krav**	**Tilbys (Ja/Nei/ Delvis)**	**Løsningsbeskrivelse**
4.1.1	Skadevareløsningen skal håndtere stegene i scenarioene der den skal ta imot et kall fra Helsenorge, skanne innholdet og gi en tilbakemelding om resultatet	Beskriv/dokumenter hvordan løsningen håndterer stegene i scenario 1/2, med fokus på steg 2 og 3.	**A***		

5 Krav til løsningen

5.1 Funksjonelle og tekniske krav

Kundens krav				Leverandørens besvarelse	
Nr.	**Beskrivelse**	**Dokumentasjonskrav**	**Type krav**	**Tilbys (Ja/Nei/ Delvis)**	**Løsningsbeskrivelse**
5.1.1	**Løsningen må kjøre on-prem hos NHN**	Skanning av dokumenter eller annet innhold må foregå on-prem og ikke være avhengig av sky-tjenester eller overføring ut av NHN sitt datasenter. Oppdateringer, lisenssjekk og annen tilsvarende nødvendig trafikk kan være avhengig av eksterne koblinger, men leverandøren må beskrive evt. krav og/eller anbefalinger til bruk av skytjenester utover selve skanningen/ oppdateringer.	**A***		
5.1.2	**Løsningen bør kunne kjøre som en container i et containermiljø**	Det er preferert at AV løsningen kjører i containere i et containermiljø, men leverandøren kan også velge å levere tilbud på egen HW / appliance dersom de mener det gir en bedre løsning. AV løsningen bør kunne kjøre uten "root"-tilganger til containermiljøet	**B**		
5.1.3	**Bred støtte for AV motorer** Løsningen bør støtte skanning med flere antivirus/skanning -motorer / signaturfiler fra forskjellige leverandører.	Vi ønsker et tilbud på ca. 5 motorer, men leverandøren kan foreslå andre løsninger som ivaretar like god eller bedre sikkerhet.	**B**		

Kundens krav				Leverandørens besvarelse	
Nr.	**Beskrivelse**	**Dokumentasjonskrav**	**Type krav**	**Tilbys (Ja/Nei/ Delvis)**	**Løsningsbeskrivelse**
5.1.4	**Støtte for å finne ukjent / ny skadevare basert på oppførsel eller annet**	For å finne ukjent skadevare bes leverandøren beskrive muligheter for å finne slik skadevare basert på innhold eller oppførsel. Hvordan kan løsningen finne ukjent skadevare som ikke finnes ved skanning basert på signaturfiler? Kan slik skanning skje innenfor kravet til ytelse/hastighet som er gitt i eget krav til ytelse? Vi kan vurdere dette som opsjon eller mulighet senere og dette må skilles ut som egen prislinje i lisenstabellen, jfr. Bilag 5, vedlegg 1	**B**		
5.1.5	**Redundans** Løsningen må være mulig å kjøre fullt redundant; også på tvers av datasenter.	Leverandøren bes beskrive hvordan redundans oppnås ved bruk av deres løsning.	**A***		
5.1.6	**Krav til responstid** Mye av skanningen skal fullføres mens bruker/innbygger venter på svar fra portalen. For å ivareta bruker-vennligheten, så må skanningen skje innenfor 0.5 sek for et normalt dokument på opptil 2MB	Leverandøren bes beskrive målt ytelse i løsningen	**B**		

Kundens krav				Leverandørens besvarelse	
Nr.	**Beskrivelse**	**Dokumentasjonskrav**	**Type krav**	**Tilbys (Ja/Nei/ Delvis)**	**Løsningsbeskrivelse**
5.1.7	**Bruk av flertråds-behandling**	Leverandøren bes beskrive muligheten for flertrådsbehandling slik at behandling av et stort dokument ikke nødvendigvis stopper eller lager kø for andre skanningsforespørsler	**B**		
5.1.8	**Skalering** Antall skanninger kan endres over tid og løsningen må støtte skalering opp eller ned ved behov. Statistikk fra nåværende løsning viser at vi skanner opptil 50.000 dokumenter per døgn, og dette kan forventes å øke.	Leverandøren bes beskrive hvordan dette kan ivaretas. Beskrivelsen må inkludere evt. endringer i lisensiering for å skalere løsningen.	**A***		
5.1.9	**API for skanning** Løsningen skal tilby et API der Helsenorge eller andre plattformer kan be om skanning av et dokument / innhold og få tilbake informasjon om status for dokumentet via et API kall. Dagens løsning benytter REST basert API, men leverandøren kan bruke/anbefale andre standarder	Leverandøren bes beskrive funksjonaliteten i API'et for slik skanning/bruk	**A***		

Kundens krav				Leverandørens besvarelse	
Nr.	**Beskrivelse**	**Dokumentasjonskrav**	**Type krav**	**Tilbys (Ja/Nei/ Delvis)**	**Løsningsbeskrivelse**
5.1.10	**Tilpasse forespørsel til API**	Leverandøren bes beskrive hvor fleksibelt løsningens API'et er ved bruk; Er det f.eks. mulig å tilpasse hvordan skanningen utføres som del av API kallet / av klienten som kaller API'et. En slik tilpasning kan være type skanning / antall AV motorer som skal benyttes eller andre tilpasninger av skanningen klienten som kaller AV API'et ønsker	**B**		
5.1.11	**Skanning i batch og prioritering av type skanning**	Leverandøren bes beskrive om det er mulig å sende inn en "batch"-basert/asynkron skanning; f.eks. der vi har mange dokumenter i et fillager som skal skannes samtidig som vi behandler dokumenter som sendes via Helsenorge generelt. I et slikt scenario kan det være ønskelig at det generell skanning har høyere prioritet enn den batch-baserte skanningen som ikke har samme krav til ytelse/responstid	**B**		

Kundens krav				Leverandørens besvarelse	
Nr.	**Beskrivelse**	**Dokumentasjonskrav**	**Type krav**	**Tilbys (Ja/Nei/ Delvis)**	**Løsningsbeskrivelse**
5.1.12	**Skanning av dokumenter eller innhold i en struktur**	Leverandøren bes beskrive om AV løsningen støtter deteksjon av at det er virus i en sammensatt fil som inneholder flere enn 1 type innhold. Typisk struktur som vil sendes inn til skanning er metadata med base64-enkodet filinnhold, der innholdstypen på disse ikke er begrenset til de typiske scenarioene med bilde og/eller PDF. Filinnholdet kan også være komprimerte arkiver (e.g. zip) som inneholder en eller flere filer. Leverandøren bør også beskrive hvordan de forholde seg til enkodet, komprimert, passordbeskyttet og kryptert innhold	**B**		
5.1.13	**Autentisering mot tjenesten** AV tjenesten må støtte autentisering mot skanning-API'et / kunne skille mellom hvilke klienter som kallet tjenesten	Beskrive hvordan autentisering mot skanning-API'et vil fungere slik at vi kan skille mellom flere klienter / løsninger som benytter løsningen (se neste krav som er relatert) Beskrivelsen bør inneholde evt. ytelsesmessig påvirkning ved bruk av tokens eller annen autentisering (f.eks. krav til fornyelse av tokens)	**A***		

Kundens krav				Leverandørens besvarelse	
Nr.	**Beskrivelse**	**Dokumentasjonskrav**	**Type krav**	**Tilbys (Ja/Nei/ Delvis)**	**Løsningsbeskrivelse**
5.1.14	**Støtte å være en fellestjeneste** AV løsningen må støtte at flere plattformer / løsninger (klienter) benytter den for skanning og kunne skille mellom de enkelte klientene for bl.a. logging og statistikk.	Leverandøren bes beskrive hvordan dette håndteres i løsningen	**A***		
5.1.15	**Kryptering av kommunikasjon** AV løsningen skal støtte at all overføring av informasjon til eller fra AV løsningen sikres og krypteres med f.eks. med TLS eller andre mekanismer	Leverandøren bes beskrive hvordan dette håndteres i løsningen	**A***		
5.1.16	**Sentral drift og monitorering** Løsningen må støtte integrasjon og/eller rapportering til sentrale drifts og monitorerings-løsninger, f.eks.; - Logging til SPLUNK - Ytelsesdata / statistikk - Varslinger ved funn	Leverandøren bes beskrive hvordan dette kravet oppfylles og evt. om de har egne løsninger for dette i tillegg til mulighet for integrasjon mot våre løsninger	**A***		

Kundens krav				Leverandørens besvarelse	
Nr.	**Beskrivelse**	**Dokumentasjonskrav**	**Type krav**	**Tilbys (Ja/Nei/ Delvis)**	**Løsningsbeskrivelse**
5.1.17	**Lisensiering for test og utviklingsmiljøer** I tillegg til produksjon, trenger vi Test/QA miljø + utviklingsmiljøer der vi kan teste integrasjon mot tjenesten Disse løsningene har ikke samme behov for ytelse eller redundans	Leverandøren bes beskrive lisensmodell for test og utviklingsmiljøer	**B**		
5.1.18	**Support innenfor EU** Det er ønskelig at support håndteres innenfor EU.	Leverandøren bes oppgi hvordan support organiseres for å støtte vår driftsavdeling med å ivareta/drifte løsningen	**B**		
5.1.19	**Support** Leverandøren må tilby 24/7 støtte for løsningen til vårt driftsteam	Leverandøren bes beskrive hvordan dette kan leveres, inkludert bl.a. responstid, omfang, nivåer o.l. Det er mulig å legge ved standardisert dokumentasjon på supporttjenesten, inkludert på engelsk.	**A***		

Kundens krav				Leverandørens besvarelse	
Nr.	**Beskrivelse**	**Dokumentasjonskrav**	**Type krav**	**Tilbys (Ja/Nei/ Delvis)**	**Løsningsbeskrivelse**
5.1.20	**Dokumentasjon av løsningen** Det skal foreligge tilgjengelig dokumentasjon av løsningen inkludert informasjon som er nødvendig for å installere, konfigurere og vedlikeholde denne	Leverandøren bes beskrive hvordan dette kan leveres	**A***		

6 Sikkerhet

Informasjonssikkerhet og personvern skal ivaretas i alle NHNs anskaffelser og i avtaleforvaltningen. Kravene nedenfor er generelle sikkerhetskrav som NHN anser som relevante for denne anskaffelsen.

6.1 Informasjonssikkerhetskrav

Kundens krav				**Leverandørens besvarelse**	
Nr.	**Beskrivelse**	**Dokumentasjonskrav**	**Type krav**	**Tilbys (Ja/Nei/ Delvis)**	**Løsningsbeskrivelse**
6.1.1	**Sikkerhet i programvaren ved bruk av tredjeparts-komponenter** Leverandøren skal ha oversikt over eventuelle komponenter i programvaren laget av tredjepart, og at disse komponentene ikke inneholder kjente sårbarheter.	Leverandøren bes beskrive eventuelle tredjepartskomponenter i programvaren, og hvordan leverandøren forholder seg til trusler knyttet til bruk av tredjeparts programvare.	**I**		
6.1.2	**Brukeradministrasjon og tilgangsstyring** Løsningen bør ha mulighet for brukeradministrasjon, tilgangsstyring og tilgangskontroll og evt. integrasjon med sentrale brukerkataloger	Leverandøren bes beskrive løsningens muligheter for brukeradministrasjon, tilgangsstyring og tilgangskontroll.	**B**		

Kundens krav				Leverandørens besvarelse	
Nr.	**Beskrivelse**	**Dokumentasjonskrav**	**Type krav**	**Tilbys (Ja/Nei/ Delvis)**	**Løsningsbeskrivelse**
6.1.3	**Verdikjede** Leverandøren skal jobbe med kontinuerlig oppfølging av underleverandører på området sikkerhet og personvern, for å sikre transparens i verdikjeden.	Leverandøren bes beskrive sitt arbeid med kontinuerlig oppfølging av underleverandører på området sikkerhet og personvern, for å sikre transparens i verdikjeden.	**A***		
6.1.4	**Sikkerhetsoppdatering** Leverandøren skal sikre at programvaren får løpende sikkerhets-oppdateringer i hele kontraktens levetid	Leverandøren bør beskrive hvilke rutiner som gjelder for varsling og innføring av nye sikkerhetsoppdateringer til kunden dersom det avdekkes/oppstår alvorlige sårbarheter i programvaren. Beskrivelsen bør inneholde informasjon om hvor raskt kunden får beskjed om slike oppdateringer.	**A***		
6.1.5	**Varsling** Leverandøren skal ha prosess for varsling av kunde ved funn av sårbarheter i levert programvare.	Leverandøren bes om å beskrive sine varslingsrutiner ved funn av sårbarheter i levert programvare.	**A***		

Kundens krav				Leverandørens besvarelse	
Nr.	**Beskrivelse**	**Dokumentasjonskrav**	**Type krav**	**Tilbys (Ja/Nei/ Delvis)**	**Løsningsbeskrivelse**
6.1.6	**Vurdering av anskaffet programvare** Leverandøren skal akseptere at Kunden gjennomfører en ROS av tilbudte løsning/programvare før løsningen implementeres. Dersom det avdekkes forhold som strider mot Kundens styringssystem for informasjonssikkerhet og personvern, skal Leverandøren uten opphold bistå Kunden med å avklare slike forhold.	Bekreftes	**A**		
6.1.7	**Behandling av personopplysninger i programvaren eller tilkoblede løsninger hos leverandøren**	Leverandøren bes beskrive om tilbudte programvare/løsning samler inn personopplysninger, informasjon/statistikk (brukerstatistikk, diagnostikk e.l.) og hvilket formål dette benyttes til samt hvor denne informasjon/data lagres og behandles.	**I**		

Kundens krav				Leverandørens besvarelse	
Nr.	**Beskrivelse**	**Dokumentasjonskrav**	**Type krav**	**Tilbys (Ja/Nei/ Delvis)**	**Løsningsbeskrivelse**
6.1.8	**Behandling av personopplysninger utenfor EU/EØS skal ha et gyldig overføringsgrunnlag** Dersom personopplysninger behandles utenfor EU/EØS, skal dette gjøres i henhold til gyldig overføringsgrunnlag, f.eks. SCC 2021 (Standard Contractual Clauses 2021) eller privacy policy med tilsvarende beskyttelsesnivå som SCC.	Leverandøren bes beskrive hvordan kravet er oppfylt. Vilkårene for kjøp og bruk av tjenesten vedlegges som en del av besvarelsen på kravet.	**A***		
6.1.9	**Revisjon** Kunden skal ha rett til å gjennomføre revisjon og verifikasjon av Leverandøren og programvarens etterlevelse av krav til informasjonssikkerhet og personvern. En slik revisjon, kan gjennomføres basert på følgende prinsipper: - revisjon gjennomføres av Kunden - revisjon gjennomføres av uavhengig tredjepart	Bekreftes. Leverandøren skal samtykke i dette og skal på forespørsel yte bistand til Kunden ved gjennomføring av en slik revisjon	**A**		