# Autentisitetsstøtte

## Innledning

Dette er en oppsummering av materialer som StandardLab teamet har skapt i løpet av sitt arbeid med behovet "Autentisitetsstøtte": https://github.com/arkivverket/standardlab/issues/12 (versjon fra 22. september 2022).

Dokumentets struktur har vært definert i denne filen: github.com/arkivverket/standardlab/blob/f004fe89a734cfd20b89d1bc949c015ccb00cbe4/standarder/autentisitetsstotte.md#disposisjontemaer-som-skal-dekkes

Innhold merket med TBD i kursiv var planlagt beskrevet, men ikke påbegynt da arbeidet ble stoppet.

## Innholdsfortegnelse



## Kontekst

### Relaterte egenskaper

- All registrert informasjon er dokumentasjon (eller records på engelsk), dvs. at den kan brukes til å dokumentere noe.
    - Informasjon som har egenskapene autentisitet, pålitelighet, integritet og anvendbarhet blir betegnet som autoritativ dokumentasjon. Dette er egenskaper som samlet sett sørger for å støtte opp under informasjonens bevisverdi, og dermed tilliten til informasjonen som dokumentasjon.
        - Autentisitet går på omstendighetene rundt registreringen av informasjonen, dvs. at den faktisk dokumenterer det som det påstås at den skal

dokumentere, herunder hvem som opprettet eller sendte den, når det skjedde, osv. Ivaretakelsen bygges inn i dokumentasjonsprosessene.
        - Pålitelighet handler om at den registrerte informasjonen skal være fullstendig og nøyaktig, herunder at det ikke er et selektivt utvalg av informasjon som er registrert. Forutsetter at registreringen av informasjon skjer i direkte tilknytning til hendelsen som skal dokumenteres, av noen (person eller system) med direkte kjennskap til hendelsen.
        - Integritet går på at informasjonsinnholdet er komplett og uendret. Informasjonen må beskyttes mot uautoriserte endringer, og det må være tydelig spesifisert hvilke endringer som er tillatt, eller som kan autoriseres, under hvilke forhold. All autorisert endring skal være eksplisitt tillatt og sporbar.
        - Anvendbarhet går på at informasjonen kan gjenfinnes, fremhentes, presenteres og forstås av relevante interessenter innen rimelig tid. Informasjonen må kunne knyttes til forretningsaktiviteten eller transaksjonen som skapte den, og den må kunne knyttes til relatert informasjon. Forutsetter metadata som gjør at informasjonen kan fremhentes og presenteres, som identifikatorer, format og lagringsinformasjon.
    - ISO 15489 fastsetter at dokumentasjon skal støtte utøvelsen av forretningsaktiviteter, bidra til at virksomheten overholder reguleringer, og sikre tilstrekkelig etterrettelighet. For å få til dette må virksomheten sørge for å opprette og vedlikeholde informasjon som er autentisk, pålitelig og anvendbar, og at integriteten beskyttes så lenge det er behov for det.
    - InterPARES-prosjektet konkluderte med at autentisitet er én av tre egenskaper ved dokumentasjon som støtter opp under dokumentasjonens troverdighet. De to andre er pålitelighet og nøyaktighet.
        - Autentisitet er dokumentasjonens troverdighet som dokumentasjon, dvs. kvaliteten ved dokumentasjon som er det som det påstås at den er, og som ikke er tuklet med eller korrumpert. Autentisitet etableres ved å undersøke dokumentasjonens identitet og integritet.
            - Integritet er det kvaliteten ved at dokumentasjonen er komplett og uendret.
            - Identitet er summen av de egenskaper ved dokumentasjon eller et dokument som gjør at det kan identifiseres som unikt og atskilles fra ethvert annen dokumentasjon eller dokument
    - InterPARES: Autentisitet = integritet + identitet
- Ekthet, Ikke-benektelse og Pålitelighet i ISO 27000 (TBD)

## Forhold til lovverk

- Arkivlov – dokumentasjonsverdi (KUD-brev 2009) + opphavet er kjent (forslag til ny lov)
    - Arkivloven stiller krav til at informasjon som faller inn under lovens dokumentbegrep skal sikres som informasjonskilde for samtid og ettertid. Vilkårene for at informasjon skal omfattes av lovens dokumentbegrep, er at den enten er underlagt saksbehandling, eller at den har verdi som dokumentasjon.
    - KUD har skrevet om dokumentasjonsverdi i brev av 18.02.2009:

        - Et dokuments verdi som dokumentasjon er en funksjon av den betydning dokumentet har for i ettertid å kunne framskaffe informasjon om og bevis for hva som er skjedd.
        - Spørsmålet om dokumentasjonsverdi må alltid knyttes til de originale saksdokumentene som sådanne, [… og det] gjelder generelt at originale saksdokumenters dokumentasjonsverdi ikke kan erstattes av opplysninger som blir registrert på annen måte.
        - Originale saksdokumenter har bl.a. en autentisitet og dermed en primær bevisverdi som ikke kan erstattes gjennom registrering av opplysninger i interne dokumenter eller saksbehandlingssystemer. Slike opplysninger vil bare ha sekundær dokumentasjonsverdi.
    - Kommentar: Slik KUD beskriver dokumentasjonsverdi, er dette nært knyttet til bevisverdi og autentisitet, og det følger at dette er egenskaper ved det originale dokumentet.
    - Dagens arkivlov har en negativ avgrensning, dvs. at alt skal arkiveres, med mindre det kan arkivbegrenses. I KUDs forslag til ny lov (høringsnotat av 5. oktober 2021) er det foreslått å videreføre omfanget av hva som skal arkiveres, men nå som en positiv avgrensning: Dokument som har inngått i saksbehandlingen eller har dokumentasjonsverdi, skal arkiveres.
        - Det er presisert at dokumentasjonsverdien ikkje skal vere tilfeldig, men knytt til saksbehandlinga eller oppgåveløysinga til organet. Dette følgjer for så vidt allereie av kravet om at dokumentet skal vere skapt eller motteke som del av verksemda. Omgrepa skal forståast på same måten som i dag. […] Kva som har verdi som dokumentasjon, vil måtte vurderast ut frå dokumentasjonsbehovet og kva som er formålet med dokumentasjonen. Viss hensikta er å oppnå ei forvaltning som er forsvarleg og kan etterprøvast, så bør ein arkivere dokumentasjon som viser kva som blei gjort, kva, kven som gjorde det, og korleis, kva det blei lagt vekt på, osv.
        - Målet er å sikre at dokumentasjon som er blitt arkivert i offentlege organ, skal vere tilgjengeleg som autentiske og uforfalska kjelder til kvar tid. […] Arkiva må sikrast, slik at ein kan ha tryggleik for at informasjonen til kvar tid er identisk med han som opphavleg blei skapt. Det må liggje føre nødvendige metadata, kontekstinformasjon om kvar materialet er blitt til, kven som skapte det, og i kva samanheng.
    - Både gammel og ny arkivlov sier at det er dokumenter som skal "arkiveres", med den presisering at det er dokumenter knyttet til saksbehandling og oppgaveløsning. Arkivdanning, i betydningen dokumentasjonsforvaltning, innebærer med andre ord registrering av informasjon om en virksomhets handlinger og transaksjoner, slik at denne registrerte informasjonen skal kunne brukes som vitnesbyrd og bevis om virksomhetens transaksjoner og forpliktelser.
        - Funksjoner for datafangst skal dokumentere dokumentenes opphavssammenheng, dvs. at de ble brukt der og da.
- Arkivforskriften §12 sier at organet skal utarbeide rutiner for oppretting, mottak, utveksling, arkivering, vedlikehold og bruk av dokument som skal inngå i arkiv. Rutinene skal sikre at det går fram hvem som har opprettet og registrert dokumentene, og at det kun er personer med riktig autorisasjon kan gjøre dette,"
    - Formålet med bestemmelsen er autentisitetsstøtte - det skal være mulig å påvise hvem som har opprettet eller sendt et dokument, og når det skjedde. Dette skjer

gjennom autorisasjoner av brukere og logging av hvem som foretar ulike registreringer.

- Riksarkivars forskrift kapittel 3 stiller krav til arkivsystemer og elektronisk behandling av arkivdokument.
    - § 3-2 sier det skal utarbeides en instruks som beskriver ansvar, rutiner og rettigheter knyttet til opprettelse, mottak, utveksling, vedlikehold og bruk av arkivdokument i arkivsystem, herunder ansvar for tildeling og ajourhold av brukerrettigheter, hvilke spesifikke rettigheter som tildeles brukere av systemet, ansvar og rutiner for kvalitetssikring, mv.
        - Dette er utfyllende bestemmelser til arkivforskriften § 12, som er mer konkret på hvilke rutiner og autorisasjoner som skal dokumenteres.
    - I tillegg skal det dokumenteres regler og rutiner for signering og autentifisering av dokumenter, herunder bruken av digital signatur.
        - Det er ikke krav om bruk av digital signatur, og kravet om autentisitetssikring forutsetter ikke bruk av digital signatur. Men dersom virksomheten kommer frem til at dette er nødvendig for å sikre dokumentasjonsverdien ved et dokument, skal bruken av digital signatur dokumenteres.
        - Dersom digital signatur og kryptering benyttes, er utgangspunktet i Noark-standarden og avleveringsbestemmelsene i samme forskrift kapittel 5, at slike sikkerhetsfunksjoner skal være deaktivert ved avlevering. "Arkivdokumenter kan være påført digitale signaturer basert på offentlig nøkkelkryptografi. Dersom de digitale signaturer inngår i et ikke godkjent format må det inngås avtale med Arkivverket." (RAF § 5-16 tredje ledd)
- ISO-standardene sier at autentisitet kan fastsettes på grunnlag av bevis, dvs. at autentisitet er noe som kan bevises.
    - I norsk rett gjelder prinsippet om fri bevisførsel. Partene i en rettssak fører bevis for å overbevise dommeren om faktiske forhold som er relevante i saken. Dommerne i saken vil, basert på bevisene som er ført, ta stilling til om det relevante faktiske forhold er godt nok bevist. Kontradiksjonsprinsippet innebærer at enhver part skal få mulighet til å imøtegå bevis som motparten har ført. Man har både en rett til å påpeke svakheter i motpartens bevisføring og til å føre egne motbevis.
    - Prinsippet om den frie bevisbedømmelse vil si at det ikke gjelder regler for hvor høy bevisverdi de ulike bevismidlene har. I stedet gjør dommeren en selvstendig vurdering i hver enkelt sak om hvor sterkt det faktiske forholdet er underbygget av de bevisene som er ført. Dommeren skal gjøre en helhetsvurdering av det samlede bevisbilde i saken, og dommeren skal vurdere om det faktiske forholdet er godt nok bevist til at beviskravet er oppfylt.
    - Loven stiller ingen krav om at dommerne må følge en bestemt metode i bevisbedømmelsen, men noen metoder for å vurdere bevis har blitt utviklet og anbefalt fra teoretikere.

# Rammer

## Risiko- og verdivurdering

Hvilke krav som stilles til autentisitet for et dokument, en gruppe dokumenter eller et arkiv avhenger av hvilken verdi det har, og hvilke risikoer man må hensynta. Det er derfor nødvendig å gjøre en verdivurdering og en risikovurdering for å sikre at autentisitet blir ivaretatt på hensiktsmessig vis.

## Hvordan vurdere verdi

En verdivurdering for forvaltning av dokumentasjon innebærer en analyse av konteksten forretningsaktiviteter foregår i, i den hensikt å

- fastsette dokumentasjonskrav
- forstå hvilke forretningsområder som blir vurdert som kritiske for måloppnåelse av interessentene
- identifisere og vurdere risiko for dokumentasjon

Resultatet av verdivurderingen bør brukes proaktivt i design av kontrollfunksjoner og prosesser for dokumentasjon, slik at de støtter forretningsaktivitetene og teknologien, slik at omforente dokumentasjonskrav kan imøtekommes over tid. Formålet er at dokumentasjonsforvaltningen designes helhetlig for å ivareta både forretningsmessige og andre formål.
Verdivurderingsprosessen består av en rekke ulike analyser, som kan utføres etter hverandre eller parallelt. Blant annet:

- skaffe forståelse for konteksten verdivurderingen utføres på, inkludert organisatoriske, teknologiske og forretningsrelaterte trekk,
- analyse av selve forretningsfunksjonene,
- analyse av dokumentasjonskrav fra både et forretningsmessig, juridisk og samfunnsmessig perspektiv,
- identifisering og analyse av risiko knyttet til opprettelse, fangst og forvaltning av dokumentasjon.

Metodikk for verdivurdering for dokumentasjonsforvaltning er nærmere beskrevet i ISO 21946. [En tilpassing/kontekstualisering av denne til norske forhold kan være relevant som framtidig produkt fra StandardLab]

## Hvordan vurdere risiko

Alle virksomheter har behov for å identifisere og håndtere risiko som påvirker driften. En sentral del av dette i dokumentasjonsforvaltning er identifisering og håndtering av risiko knyttet til dokumentasjonsprosesser og –systemer, som ikke må forveksles med å identifisere og håndtere risiko knyttet til forretningsutøvelsen, herunder det å skape og forvalte adekvat dokumentasjon.

Virksomhetens metodikk for risikohåndtering knyttet til dokumentasjonsprosesser bør ta utgangspunkt i å identifisere risikoer der konsekvensen av uønskede hendelser er tap av eller skade på dokumentasjonen, på en slik måte at den ikke lenger er brukbar, pålitelig, autentisk, komplett eller uendret, og derfor ikke lenger kan støtte virksomhetens behov. Risiko identifiseres på grunnlag av potensialet til å underminere disse egenskapene ved dokumentasjonen.

En risikovurdering vil bestå av tre hovedaktiviteter:

1. Identifisere risiko
   Hensikten er å finne ut hva som kan skje, eller hvilken situasjon som kan oppstå som påvirker virksomhetens dokumentasjonsforvaltning. Identifisere årsak eller kilde til risiko, hendelse, situasjon eller omstendighet som kan påvirke. Kategoriseres i kontekst/omgivelser, systemer og prosesser
2. Risikoanalyse
   Potensielle konsekvenser og sannsynlighet for at identifisert risiko blir en realitet. Sannsynlighet kan knyttes til hyppighet, frekvens
3. Evaluere risiko
   Beslutningsgrunnlaget, basert på resultat av risikoanalyse. Hvilke risikoer bør håndteres, prioritering av tiltak for å møte risiko

Man bør gjøre risikovurdering på tvers av hele dokumentasjonsforvaltningen, herunder prosessene for:

a. Fangst
b. Forvaltning
c. Bruk
d. Avhending

Metodikk for risikovurdering for dokumentasjonsforvaltning er nærmere beskrevet i ISO 18128. [En tilpassing/kontekstualisering av denne til norske forhold kan være relevant som framtidig produkt fra StandardLab]

### Risikofaktorer for autentisitet

Enkelte typer risikoer, risikofaktorer og risikoutløsende aktiviteter er spesielt viktig å være oppmerksom på når det gjelder autentisitet. Dette inkluderer:

a. Utilstrekkelig fangst av dokumenter eller deres metadata
    i. Som følge av utilstrekkelig systemdesign eller manglende interoperabilitet mellom systemer med avhengigheter til hverandre
    ii. Som følge av utilstrekkelige rutiner
    iii. Som følge av endringer i systemer med avhengigheter til hverandre
b. Uautoriserte/utilsiktede endringer av dokumenter eller deres metadata
    i. Som følge av intensjonell ødeleggelse fra eksterne eller utro tjenere
    ii. Som følge av menneskelige feil
    iii. Som uønsket effekt av bruk av dokumentene
    iv. Som uønsket effekt av vedlikehold av dokumentasjonen
    v. Som uønsket effekt av teknologiskifter
    vi. Som uønsket effekt av avhendingsprosesser

Relevante tiltak for å redusere disse risikoene går fram av denne standarden. Virksomheten må fortløpende vurdere hvilket tiltaksnivå som er relevant ut fra verdivurderingen av den aktuelle dokumentasjonen.

### Autentisitet vs andre egenskaper

Det vil kunne oppstå situasjoner der behovet for autentisitet må veies opp mot andre egenskaper ved dokumentasjonen. Et eksempel på en slik situasjon kan være beslutning av hvilket format dokumentasjonen skal bevares i, der autentisitet vil styrkes av at det originale produksjonsformatet bevares, mens andre formater kan være bedre tilrettelagt for å ivareta anvendelighet. Det er ikke hensiktsmessig å gi en generell regel for veiing av de ulike egenskapene mot hverandre, men som tommelfingerregel kan man ta utgangspunkt i at dokumentasjonens verdi er avhengig av at man balanserer de ulike egenskapene opp mot hverandre i tråd med virksomhetens verdi- og risikovurderinger.

En annen avveining som kan være nødvendig er mellom behovet for å kunne bevise autentisitet på et gitt nivå og kostnadene ved å opprettholde den. Eksempelvis kan strenge krav til dokumenterbar autentisitet medføre at mye metadata må fanges og vedlikeholdes. I en slik avveining må verdi- og risikovurdering legges til grunn for å fastslå hvilket nivå av autentisitet som er relevant for virksomheten.

## Roller og ansvar

Det er flere roller som har et ansvar for at autentisitetsstøttende metadata og logging skjer, og at autentisitet opprettholdes. Eksempler på de ulike ansvarene:

a) Arkivansvarlige er ansvarlige for påliteligheten, autentisiteten, anvendbarheten og integriteten til metadata knyttet til records, og for opplæring av brukere i å fange, administrere og bruke metadata.
b) Alle saksbehandlere er ansvarlige for at metadata som registreres ved fangst er et nøyaktig og (tilstrekkelig) komplett vitnesbyrd om hendelsen eller handlingen som er dokumentert.
c) Ledere er ansvarlige for at internkontroll er på plass slik at man kan stole på dokumentasjonen som produseres. Dette skjer blant annet gjennom å definere krav og policyer for øvrige roller.
d) Systemansvarlige er ansvarlige for at systemene har kapabiliteter for å fange autentisitetsstøttende metadata, og at autentisiteten opprettholdes over tid i systemet. De har også ansvar for at autentisitet ikke går tapt ved teknologiskifter.

Det er også andre roller som har interesse av at autentisitet er ivaretatt. Et eksempel på dette er juridisk personell som må kunne stole på at dokumentasjonen er det den gir seg ut for å være.

# Hvordan etablere og opprettholde autentisitet

## Løsninger og overganger

Autentisitet i dokumentasjonen krever at løsningene for å lage, fange, lagre, forvalte og avhende informasjonen alle er tilrettelagt for å støtte denne autentisiteten. Det er også nødvendig at overganger mellom ulike løsninger, og teknologiskifter innad i en løsning.

### Løsninger

I denne sammenheng defineres løsning som en eller flere komponenter eller systemer, sammen med rutiner og policyer for hvordan løsningen skal brukes, som til sammen er organisert slik at de kan utføre en gitt funksjon eller sett av funksjoner. Summen av virksomhetens løsninger omtales som deres løsningsarkitektur. Det er denne løsningsarkitekturen som må ivareta behovene for autentisitet.

I dokumentasjonsforvaltning skilles det ofte mellom forretningsløsninger (business systems) som er lagd for at virksomheten skal kunne utføre sine forretningsoppgaver (saksbehandling, tjenesteyting mv.), og dokumentasjonsløsninger (records systems) som er lagd for at virksomheten skal kunne ivareta sine dokumentasjonsbehov. Det er dog ikke et krav at dette er separate løsninger – den samme løsningen kan være forretningsløsning og dokumentasjonsløsning for en prosess eller et fagområde.

### Overganger

I løpet av dokumentasjonens levetid vil den kunne/måtte utsettes for ulike former for overganger, der det er viktig å ivareta autentisiteten til dokumentasjonen. Disse overgangene kan være

a) mellom forretningsløsninger innad i virksomheten
b) mellom forretningsløsninger som skaper dokumentasjon og dokumentasjonsløsninger som tar vare på dokumentasjonen
c) mellom dokumentasjonsløsninger innad i virksomheten
d) mellom virksomheter i forbindelse med utføringen av forretningsoppgaver
e) mellom virksomheter i andre sammenhenger enn utføringen av forretningsoppgaver – for eksempel overføring av ansvar for dokumentasjonen
f) mellom ulike versjoner av dokumentasjonsløsninger eller -formater

Det skilles mellom to hovedtyper overganger:

1. **Migrering** – prosesser der dokumentasjon, inkludert eksisterende karakteristikker, flyttes fra en løsning til en annen uten at formatet endres
2. **Konvertering** – prosesser der dokumentasjonen flyttes fra et format til et annet på vis der karakteristikker ivaretas

I praksis vil de fleste overganger ha aspekter av både migrering og konvertering. For å ivareta autentisitet er det viktig å være klar over hva slags overgang som skal gjennomføres.

### Eksempler

I et direktorat produseres dokumentasjon i et saksbehandlingssystem (forretningsløsning), som er integrert med et arkivsystem (dokumentasjonsløsning) som brukes til å forvalte dokumentasjonen. Dette er en overgang av type b i listen over. Som del av integrasjonen flyttes autentisitetsstøttende metadata om dokumentasjonen (hvem som har opprettet den og når) uendret fra saksbehandlingssystemet til arkivsystemet (migrering), mens dokumentet som skapes (en utsendt e-post) konverteres fra e-postformat til PDF-A for bevaring. Informasjonsinnholdet i e-posten er uendret gjennom konverteringen. Autentisitet opprettholdes for både dokumentinnholdet og metadata.

En kommune oppgraderer sitt arkivsystem (dokumentasjonsløsning) til nyeste versjon, og flytter samtidig dokumentene til en skyløsning. Den nye versjonen av arkivsystemet inneholder informasjon om tidssone som del av datoer, noe den gamle versjonen ikke gjorde. Metadata som er datoer konverteres dermed fra dato uten tidssoneangivelse til dato med tidssoneangivelse. Dokumentene som migreres forblir uendret i format, form og innhold. Autentisitet opprettholdes for dokumentet og metadata, men tilføres ikke selv om nytt datoformat er mer nøyaktig.[1]

## Etablere autentisitet

Autentisitet kan i liten grad tilføres dokumentasjonen. Det er derfor en forutsetning at nødvendige virkemidler for å vurdere og bevise autentisiteten oppstår i det dokumentasjonen skapes og/eller fanges. Hvilken dokumentasjon som skal fanges er dels spesifisert i ulike lover og forskrifter, dels opp til virksomhetens egen vurdering av hvilken dokumentasjon som gir verdi.

De viktigste verktøyene for denne autentisitetsstøtten er metadata som sier noe om hva dokumentasjonen er, og logging som beviser hvilke handlinger som har funnet sted. Hvilke krav som skal stilles til metadata og logging for det enkelte dokument henger sammen med risiko- og verdivurderingene av dokumentasjonen.

### Metadata for autentisitet (ved fangst)

For at autentisitet skal være dokumentert, vil det kunne være nødvendig med metadata som sier noe om

a. **Dokumentets identitet** – at det er et unikt dokument
b. Beskrivende metadata
c. Bruksmetadata
d. Hendelsesplanmetadata
e. **Hendelseshistorikkmetadata** – hvilke hendelser som har skjedd, når det skjedde, hva som var årsak til det, hvem som utførte – til sammen; hvordan dokumentet oppsto / ble fanget
f. **Relasjonsmetadata** – konteksten til dokumentet (prosesser, løsninger og andre dokumenter)

For hendelseshistorikkmetadata er autentisitet til dels knyttet til i hvilken grad man kan være sikker på for hvem som utførte handlingen. Her kan autentisering av brukere og digitale signaturer være nyttige hjelpemiddel, som man må vurdere verdien av å dokumentere hvis man tar i bruk.

### Logging

For at autentisitet skal kunne verifiseres, bør det foreligge logging av hva som har skjedd med det enkelte dokumentasjonsobjektet, og av hva som har skjedd med løsningene som har behandlet dokumentasjonen som helhet.

Loggen for det enkelte dokumentasjonsobjektet oppstår som følge av at objektet blir fanget. Den første loggoppføringen vil dokumentere tidspunkt for fangst, i tillegg til metadata om dokumentet som er fanget. Loggoppføringer er fryst for å unngå utilsiktede endringer. Påfølgende hendelser blir nye oppføringer i loggen.

## Opprettholde autentisitet i tid

### Hva menes med autentisitet over tid

Etter at informasjon er fanget som en registrering, skal den tas vare på og forvaltes som aktiv dokumentasjon, slik at den fortsatt støtter organets bruksbehov. Å opprettholde autentisitet over tid handler om å ivareta autentisitet innen en løsning i organets aktive dokumentasjonsmiljø.

- Skillet opprettholde i tid – handler om å opprettholde i tid som fravær av handling eller ikke-bevisst handling – mens opprettholde gjennom overganger handler om at du har villet handling
- Opprettholde i tid handler også om at autentisitet skal ivaretas mens records er i bruk – men skal vi tilnærme oss dette i et continuum?

### Opprettholde autentisitet innen en løsning

All arkivinformasjon har et informasjonsinnhold og ulike typer metadata, som blant annet sier noe om identitet, kontekst, struktur og tilgang, med mer.

Den største risikoen for å svekke autentisiteten til elektronisk informasjon, er når den endrer tilstand, dvs. når kontroll med informasjonen overføres til et annet system. Så lenge informasjonen beholdes innenfor en systemomgivelse eller en løsning, er det fullt mulig å implementere tiltak som sikrer autentisitet innenfor løsningen.

- Det er mulig å spore enhver tilgang til informasjonen i en løsning, og enhver handling utført på informasjonen som er lagret i løsningen. Sporingsinformasjonen, eller loggen, må være beskyttet mot uautorisert tilgang og endring.
- Løsningen kan designes slik at når informasjon først er lagt inn og lagret i løsningen, så kan den aldri tas ut av løsningen, unntatt som kopi. Originalen som ligger i løsningen, vil dermed alltid kunne beholdes uendret - så lenge den er lagret i løsningen.
- Løsningen kan designes slik at endringer på informasjonsinnhold og metadata ikke er mulig fra et gitt tidspunkt, med mindre det utføres av en autorisert person.
- Det er også mulig å designe løsningen slik at autoriserte brukere får varsel ved forsøk på uautorisert endring eller tilgang til informasjon.

Slike kontrollmekanismer virker kun innenfor løsningens grenser. Når informasjon tas ut av løsningen, eller når det gjøres endringer i løsningen, innebærer det en risiko for denne systematiske kontrollen.

(Ta vare på kontekst av dokumentasjonen (alle dokumentene) (ulike formater))

*Hvordan opprettholde autentisitet over tid i en løsning (Hvordan oppnå resultatet)*

- Prosesser og prosedyrer for risikovurdering og intern kontroll
    - Hjelper med: Beskytte mot endringer
- Logging – hjelper med:
    - Ta vare på kontekst av dokument
    - Å vite hva har skjedd
    - Å vite hvem har gjort hva og når
    - Loggen må også tilgangsstyres
- Katalog av skjemaer (schema) - 16125 forutsetter at metadata er definert. F eks av en nasjonal metadatastandard (TBD)
    - Hjelper med: Ta vare på kontekst

*Eksempler på fremgangsmåter*

*Risikoer og tiltak – Autentisitet over tid i en løsning*

- *Tiltak jf risikoer i ramme-kapitlet: risikoer som bør dekkes av tiltak som omtales her*
    - Manglende samsvar mellom dokumentasjon i fagsystem og arkivsystem (TBD)
    - Utilstrekkelig fangst av dokumenter og metadata (TBD)
    - Uautoriserte eller utilsiktede endringer (intensjonell ødeleggelse eller menneskelige feil) (TBD)
    - Uønsket effekt av bruk, vedlikehold og avhendingsprosser
        - Audit log i løsning fra en eller annen leverandør
        - Brukere i systemet er identifisert og autorisert i tilstrekkelig grad - for de handlingene som gjøres og at dette logges.
        - Loggen må også tilgangsstyres

*Informasjonssikkerhet*

- ISO 27000 (TBD)

*Autentisitet for filer vs. autentisitet for metadata - jf. Frysing*

- Beskytte mot uautoriserte endringer (alteration/modification) og/eller sletting. (TBD)

## Opprettholde autentisitet gjennom teknologiskifter

### Hva er teknologiskifte

Dokument/Dokumentasjon forvaltes i systemer/løsninger som er en sammensetting av teknologiske, organisatoriske og juridiske komponenter. I hovedsak er det snakk om 3 typer av teknologiskifter;

- **Systembytte**: Oppgradering til annen stor versjon av løsning, gjerne fra samme leverandør. Et eksempel her er overgang fra utdatert versjon av SAP HR til siste utgaven.
- **Utfasing av system**: En løsning tas ut av bruk, en ny løsnings fases inn istedenfor den gamle. Eksempel her er overgang fra sak- og arkiv system fra leverandør A til leverandør B. Den nye løsningen er ansvarlig for samme oppgaver som den gamle. Den bevaringsverdige dokumentasjonen deponeres.
- **Forandring på oppgaver**: Sammensetting av oppgaver forandres mellom løsninger. F eks virksomhet går fra å bruke en integrert løsning for HR, Lønn og CRM til tre separate løsninger. Da flyttes oppgavene på tvers av løsningene.

Risikoen for tap av autentisitet ved disse 3 hendelsene er ulikt, og vi kommer tilbake til dette.

### *Systembytte*

Systembytter finner plass når de nye teknologiske løsningene løser oppgaver som er veldig like det som har vært løst av de tidligere. Dette kan bli sett på som oppgradering av løsning med stor ny versjon, hvor ansvarsområde for løsningen forandrer seg ikke, men det teknologiske grunnlaget blir forandret.

Forståelse av hva er gjenstand for overføring av dokumentasjon (hva er dokument) er ganske tydelig her. Slik overgang har vært forhåpentligvis vært gjennomført av leverandør flere ganger, og de kjenner til de fleste fallgruver ved prosessen. Det er viktig likevel å ha oversikt over hvordan løsningen brukes akkurat i deres virksomhet, og hva er forskjell mellom den "standarde" oppsett av løsningen som den som er i bruk hos dere.

Risiko for tap av autentisitet er lavest blant alle teknologiskifter her.

### *Utfasing av system*

Forståelse av hva er dokument er relativ stabilt, men kan forandre seg noe. Det er kjent at f.eks. NOARK5 standard tillater viss frihet i bruk av sine objekter (saksmappe og journalpost er eksempel på begrep som går ofte inn i hverandre). Ved slik overgang er det viktig å være bevisst på hvordan løsningen brukes hos dere, og hva er de viktigste dokumentene hos dere, og hvordan disse dokumentene skal uttrykkes i den nye løsningen.

Det er sannsynlig at leverandør av den nye løsningen kan hjelpe dere med å forstå og tolke begrepene fra den nye løsningen.

### *Forandring av oppgaver*

Teknologiskifte er konvertering når de nye teknologiske løsningene løser andre oppgaver enn tidligere. Eksempel av dette kan være at den nye løsningen skal forene flere oppgaver, eller oppgavene skal blir tydeligere delt mellom løsninger. Avlevering eller deponering er også en konvertering, siden oppgavene som løses i depot er annerledes enn de som har vært i de opprinnelige løsningene.

Det er viktig for dere å ha god forståelse av forretningsprosesser og oppgaver som foregikk tidligere, og som kommer, siden forståelse av dokument kan forandre seg radikalt og uforutsigbart når både prosesser og løsninger er i bevegelse.

Risiko for tap av autentisitet er høyest blant teknologiskifter her.

### Hva skal vi ta vare på når vi tar vare på autentisitet?

Vi ønsker først og fremst å ta vare på innhold som uttrykkes ved dokumentasjon, dvs vi vil at dokumenter som gjennomgår teknologiskifte skal kunne gjenbrukes for å løse oppgavene som de skal (det er veldig ofte samme oppgaver som tidligere), f.eks. brukes som bevis, finnes igjen og leses.

Det viktigste er ikke å ta vare på formatet ("PDF/A'en) av dokumentasjonen, men innholdet samt metadata om registreringen slik at man kan verifisere at registreringen er hva den utgir seg for å være. Vi står fritt til å forandre på formen eller formatet av dokumenter, så lenge metodikken som ligger til grunne for å sikre at informasjon ikke går tapt i en migrasjonsprosess (en oppfriskning til nyere format er fremdeles en omformingsprosess) vil støtte opp under både autentisitet og integritet som beskrevet i ISO 18829 - **4.2.2.2 - Data conversion from hardcopy format into electronic format.** Går metadata om registrering tapt er det vanskelig å verifisere at registreringen er hva den utgir seg for å være.

### Hvordan tar vare på autentisitet ved teknologiskifte?

Det avgjørende er å ha tydelig forståelse av metadata for å løse oppgaver fra tidligere og nytt system. Dere må ha beskrevet hva er dokument/registrering før og etter teknologiskifte, hvordan dere har migrert metadata (inkludert tekniske endringer og tilpasninger som har vært gjort), hvordan endringslogger og andre verktøy for å opprettholde autentisitet har vært overført.

**Uløste spørsmål:** *Hva burde vi si: Dokument eller dokumentasjon? Eller registrering? Dokument fremkaller koblinger til PDF med en gang, og dokumentasjon har ingen avgrensninger (det finnes ett stykke dokumentasjon, og det er vanskelig å snakke om dokumentasjonens metadata for autentisitet)*

## Hvordan vurdere og påvise autentisitet

### Hvordan vurdere autentisitet for dokumentasjon

Enkelte situasjoner kan kreve at man er i stand til å vurdere hvorvidt dokumentasjonen er autentisk. Ofte vil behovet da dreie seg om å kunne påvise at dokumentasjonen er det den gir seg ut for å være, slik at man kan ha tillit til informasjonen som dokumentasjon. Hva som utløser dette behovet vil kunne variere, og siden det ligger i framtida er det til dels uforutsigbart hva det kan være, og hvem som vil ha behovet. Ulike situasjoner vil stille ulike krav til hvordan og i hvilken grad autentisitet kan bevises.

En vurdering vil ofte ta utgangspunkt i metadata og logging rundt dokumentet, i tillegg til informasjonsinnholdet i dokumentet. Det forutsetter at integriteten til dokumentasjonen er opprettholdt – det vil si at innholdet i dokumentene og metadata er sikret mot uautoriserte endringer. At slike endringer ikke har forekommet kan verifiseres ved sammenligning av ulike versjoner av dokumentet, gitt at disse er tatt vare på. Det vil uansett i de aller fleste tilfeller være en restrisiko for at det kan sås tvil rundt autentisiteten. Dermed vil det kreves en viss grad av tillit til systemer og aktører.

- Logging og metadata – og til ivaretakelsen av dette ved teknologioverganger og over tid (TBD)

### Internkontroll

- Internkontrolls rolle som autentisitetsstøtte – at den forekommer motvirker svekket autentisitet (TBD)

## Begrep

Begrep for standard er beskrevet her:
github.com/arkivverket/standardlab/blob/f004fe89a734cfd20b89d1bc949c015ccb00cbe4/standarder/autentisitetsst%C3%B8tte-begrep.md