

Retningslinjer

Rammeverk for identifikasjon og sporbarhet i elektronisk kommunikasjon med og i offentlig sektor

Retningslinjer for offentlige virksomheter som skal sikre digital samhandling i åpne eller lukkede nett.

Utkast

Innhold

1	Innledning.....	4
1.1	Formål.....	4
1.2	Bakgrunn	4
1.3	Endringer fra forrige versjon av rammeverket	5
1.4	Målsetning	6
1.5	Målgruppe for rammeverket.....	7
1.6	Rammeverkets oppbygning	7
2	Sikkerhetsnivå velges basert på risiko	8
3	Om identifikasjon	9
3.1	Hva er autentisering.....	9
3.2	Sikkerhetsnivåer for identifikasjon av fysiske personer	9
3.2.1	Introduksjon.....	9
3.2.2	Forholdet til eIDAS-nivåene.....	10
3.2.3	Oversikt over nivåene – noen sentrale sikkerhetsegenskaper.....	10
3.2.4	Kort om sikkerhetsegenskaper som skiller nivåene.....	11
3.3	Definisjon av sikkerhetsnivåene	12
3.3.1	Krav til alle nivåer	12
3.3.2	Krav til norsk nivå lavt	12
3.3.3	Krav til norsk nivå betydelig	13
3.3.4	Krav til norsk nivå høyt	13
3.4	Eksempler på e-ID-løsninger på ulike norske nivåer.....	14
3.4.1	Sikkerhetsnivå lavt.....	14
3.4.2	Sikkerhetsnivå betydelig.....	14
3.4.3	Sikkerhetsnivå høyt	15
3.5	Veiledning for valg av sikkerhetsnivå	15
3.5.1	Risikovurderinger for valg av sikkerhetsnivå for identifikasjon	15
3.5.2	Praktiske eksempler på tjenester som kan benytte de forskjellige sikkerhetsnivåene.....	17
4	Om sporbarhet	18
4.1	Hva er sporbarhet?.....	18
4.1.1	Produksjon av dokumentasjon.....	18
4.1.2	Lagring og vedlikehold av bevis.....	19
4.1.3	Bevisførsel	19
4.1.4	Virkemidler for å sikre sporbarhet.....	19
4.1.5	Virkemidler fra aktører i markedet (tillitstjenester m.v.).....	19
4.1.6	Offentlige fellesløsninger som understøtter sporbarhet.....	20
4.1.7	Løsninger i virksomheten	21
4.2	Definisjon av sikkerhetsnivåer for sporbarhet/bevissikring	22
	Nivå 1	22
	Nivå 2	22
4.3	Eksempler på løsninger som kan tilfredsstille sporbarhetskrav.....	22

Nivå 1	22
Nivå 2	23
4.4 Veiledning i valg av sikkerhetsnivå.....	23
4.4.1 Risikovurdering for valg av sikkerhetsnivå for sporbarhet.....	23
4.4.2 Praktiske eksempler på tjenester som kan benytte de ulike sikkerhetsnivåene for sporbarhet	25
5 Referanser	26
6 Vedlegg 1 – gjennomføringsrettsakt.....	27

1 Innledning

1.1 Formål

Dette rammeverket for identifikasjon (herunder autentisering) og sporbarhet er et hjelpemiddel for offentlige virksomheter som skal sikre digital samhandling i åpne eller lukkede nett. Rammeverket skal bidra til å gjøre det enklere å gjenbruke identifikasjonsløsninger med tilstrekkelig grad av sikkerhet på tvers av offentlige virksomheter og gjøre det enklere å knytte sammen tjenester, slik at de fremstår som enhetlige for brukeren. Gjenbruk av løsninger vil også redusere kostnader i offentlige virksomheter.

Dette rammeverket for identifikasjon og sporbarhet er et teknologinøytralt sett med overordnede anbefalinger rettet mot hele offentlig sektor. Anbefalingene gjelder valg av sikkerhetsnivå ved behov for identifikasjon av brukere av elektroniske tjenester fra forvaltningen samt brukere i offentlig sektor ved kommunikasjon mellom offentlige virksomheter. Videre inneholder rammeverket overordnede anbefalinger for valg av sikkerhetsnivå ved behov for å knytte en bruker til en elektronisk transaksjon (sporbarhet).

1.2 Bakgrunn

Offentlig sektor skal tilrettelegge for gode elektroniske tjenester til brukere (innbyggere og næringsliv), og tilrettelegge for god elektronisk samhandling med og i offentlige virksomheter.

Forvaltningen er gjennom flere regelverk pålagt å ha tilstrekkelig informasjonssikkerhet, blant annet for å ivareta taushetsplikt. Tiltakene skal være tilpasset risikoen. Dette følger både av eforvaltningsforskriften¹, personopplysningsloven og krav til effektiv drift (for staten: økonomireglementet). Forvaltningen kan stille krav til bruk av sikkerhetstjenester eller produkter, herunder til: å bekrefte partenes identitet (autentiseringstjenester) eller å hindre at data utilsiktet eller urettmessig endres (integritetstjenester), å beskytte informasjon mot innsyn fra uvedkommende (konfidensialitetstjenester) og å dokumentere henvendelser og aktiviteter og hvem som har sendt eller utført dem (sporingstjenester). Dette skal gjøres i henhold til den offentlige virksomhetens egen sikkerhetsstrategi.

Virksomheten skal likevel ikke kreve vesentlig høyere sikkerhet enn det som i henhold til sikkerhetsstrategien er nødvendig for den type informasjon som kommuniseres eller den type handling som tilbys utført elektronisk, så fremt det ikke er andre forhold (rammebetingelser) som skulle tilsi det.

Elektronisk samhandling fører med seg et behov for å koordinere bruk av tjenester for identifikasjon og sporbarhet på tvers av offentlig sektor. Felles sikkerhetsnivåer for dette i offentlig sektor gir mulighet for bruk av felles sikkerhetstjenester eller gjenbruk av sikkerhetstjenester, i kommunikasjon med brukere av offentlige elektroniske tjenester.

Gjenbruk av tjenester gir økt brukervennlighet for brukerne og fører til besparelser i de offentlige virksomhetene.

Dette dokumentet er ikke et komplett sikkerhetsrammeverk, men et rammeverk for sikkerhetstjenestene identifikasjon og sporbarhet. Identifikasjon er entydig å kunne verifisere en påstått identitet som benyttes i elektronisk samhandling. Til verifikasjon av påstanden benyttes en autentiseringstjeneste. Sporbarhet er å kunne sannsynliggjøre at en

handling ble gjennomført på et bestemt tidspunkt, knyttet til en bestemt identitet. Sagt på en annen måte er sporbarhet dokumentasjon for autentisitet og informasjonsintegritet over tid. Denne egenskapen blir tidvis omtalt som ikke-benekting, men dette er et begrep vi ønsker å gå bort fra. Sporbarhet handler om nyanser i grått og grader av sikkerhet, ikke et enten-eller. Norsk rett har fri bevisføring og -vurdering, begrepet «ikke-benektning» underkommuniserer dette.

Rammeverket gjelder i prinsippet uavhengig av hvilken type informasjon som behandles. Sporbarhetstjenester sikrer bevis for hva som har skjedd, og bidrar til at handlingene får de konsekvenser som rettsordenen fastsetter. Identifikasjonstjenester brukes både som grunnlag for tilgangsstyring til informasjon som bare noen skal ha tilgang til å se eller endre, og som delprosess i sporbarhetstjenester.

Det er viktig å være klar over at identifikasjons- og sporbarhetstjenestene kun er en del av det som utgjør sikkerhetsnivået til en offentlig elektronisk tjeneste. I vurderingen av en tjenestes totale sikkerhet må også mange andre forhold vurderes opp mot tjenestens sikkerhetsmål.

Konfidensialitet betyr at informasjon ikke skal bli kjent for uvedkommende. Tilgangskontroll, logging, kryptering og overvåking er de viktigste tekniske mekanismene for å sikre konfidensialitet. Sporbarhets- og identifikasjonstjenester vil være sentrale virkemidler for å sikre dette.

Dette rammeverket for identifikasjon og sporbarhet i elektronisk kommunikasjon med og i offentlig sektor er utformet for å være teknologinøytralt. Rammeverket er veiledende, og beskriver sikkerhetsnivåer og noen bruksområder for de ulike nivåene.

Rammeverket er todelt. Første del omfatter identifikasjon, dvs. entydig påstand om identitet og autentisering (bekreftelse) av påstanden. Rammeverket beskriver krav til identitetspåstanden og bekreftelsen, med utgangspunkt i de sikkerhetsnivåene som er definert i eIDAS-forordningen¹ som er implementert i norsk rett gjennom lov om tillitstjenester² med gjennomføringsrettsakter. Andre del av rammeverket tar for seg sporbarhet i elektronisk kommunikasjon ved bruk av tillitstjenester.

1.3 Endringer fra forrige versjon av rammeverket

Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor ble først publisert i 2008. Da hadde virksomheter i offentlig sektor hver for seg ansvar for å sørge for tilstrekkelig identifikasjon av brukere for sine tjenester. ID-porten ble i 2012 introdusert som et felles offentlig tiltak for innlogging og er i dag en offentlig felleskomponent som er pålagt brukt for statlige tjenester og sterkt anbefalt for kommunale tjenester³.

Denne versjonen av rammeverket skiller seg fra den forrige på flere punkter.

¹ EU-forordning 910/2014. The Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation).

² Lov om gjennomføring av Eus forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (lov om elektroniske tillitstjenester)

³ Digitaliseringsrundskrivet

Det gjelder særlig:

- Omtale av risiko er kortet ned. Rammeverket referer til Difis veiledning i internkontroll.
- Omtalen av løsninger for å sikre dokumentasjon er utvidet, blant annet ved at det er gitt eksempler på hvordan nye tillitstjenester kan tilfredsstille behovet for dokumentasjon. Begrepsbruken er endret og klargjør at tiltakene vil gi ulike grader av tillit, og ikke er et spørsmål om enten-eller (slik begrepene «uavviselighet» og «ikke-benektning» i forrige versjon av rammeverket kunne gi inntrykk av).
- Sikkerhetsnivåene for elektroniske identitetsbevis tar utgangspunkt i sikkerhetsnivåene som beskrives i eIDAS-forordningen med gjennomføringsrettsakter. Det er stilt krav både til identitetspåstanden (individualiseringen) og autentiseringens styrke.
- Kravsettet for e-ID er vesentlig utvidet, ved at det bygges på kravene i eIDAS-forordningen. Det gis nå omfattende, teknologinøytrale beskrivelser på alle sikkerhetsnivåer for identifikasjon. I forrige versjon av rammeverket kunne i praksis bare PKI-baserte⁴ løsninger aksepteres på høyeste nivå, fordi selvdeklarasjon kun var mulig for slike løsninger. Teknologinøytralitet legger til rette for innovasjon og bruk av nye løsninger som markedet måtte tilby, også på lavere nivåer.
- En konsekvens av teknologinøytrale krav til e-ID er at kravspesifikasjon for PKI i offentlig sektor avvikles. Koordineringsbehovet dekkes ved bruk av forvaltningsstandarter for PKI, som vil bli inntatt i Referansekatalogen for IT-standarder⁵ og eventuelt i forskrift om IT-standarder i offentlig forvaltning⁶.
- Det er presisert at identifikasjonspåstanden entydig skal kunne knytte personen til en norsk identifikator som finnes i folkeregisteret (p.t. fødselsnummer eller d-nummer).
- Rammeverket omtaler ikke lenger autentisering av virksomheter. Dette skyldes at behovet for annet enn automatisert pålogging (maskin-til-maskin-kommunikasjon) anses som lavt, og at behovet for identifikasjon, tilgangsstyring og sporing av virksomheter kan håndteres ved hjelp av tillitstjenester for elektroniske segl (tidligere kalt virksomhetssignaturer). Dette gjelder både identifikasjon av nettsteder og andre systemløsninger.

1.4 Målsetting

Hovedmålsettingen med forslag til nytt rammeverk er å legge til rette for felles løsninger og gjenbruk av løsninger for identifikasjon og sporbarhet på tvers av offentlig sektor. Offentlige virksomheter bør gjennomføre risiko- og sårbarhetsanalyser ved etablering av nye, eller revidering av eksisterende, elektroniske tjenester eller ved samhandling. I den sammenheng skal virksomhetene kunne vurdere aktuelle trusler for en elektronisk tjeneste og velge hvilket sikkerhetsnivå som skal benyttes for å ivareta identifikasjons- og sporbarhetsbehov.

Det er viktig å merke seg at rammeverket er veiledende. Hver offentlig virksomhet er selv ansvarlig for de vurderinger og valg som gjøres for å sikre egne elektroniske tjenester og elektronisk kommunikasjon, og for eventuelle følger av disse valgene.

I tillegg skal forslaget til rammeverk understøtte selvdeklarasjon av eID-er mot et gitt identifikasjonsnivå. Lov om tillitstjenester⁷ hjemler forskrift om selvdeklarasjon.

⁴ Løsninger basert på assymetriske nøkler, og som tilrettelegger for offentlig-nøkkel-infrastruktur.

⁵ <https://www.difi.no/referansekatalogen>

⁶ <https://lovdata.no/dokument/SF/forskrift/2013-04-05-959>

⁷ <https://lovdata.no/dokument/NL/lov/2018-06-15-44>

Selvdeklarasjon måtte tidligere gjøres mot Kravspesifikasjon for PKI i offentlig sektor, men ordningen vil nå innrettes på selvdeklarasjon for etterlevelse av nivåer i dette rammeverket. En e-ID-utsteder kan frivillig levere selvdeklarasjon for oppfyllelse av krav til et gitt nivå til Nkom som norsk tilsynsmyndighet, og bli underlagt tilsyn av Nkom.

1.5 Målgruppe for rammeverket

Rammeverket er skrevet for personer som skal arbeide med vurdering av risiko, valg av sikkerhetsnivå for identifikasjon og valg av tekniske løsninger (tjenester) for sporbarhet i elektronisk kommunikasjon med og i offentlig sektor.

1.6 Rammeverkets oppbygning

Kapittel 3 beskriver prinsipper for valg av sikkerhetsnivå, både for identifikasjon og sporbarhet. Kapittel 4 beskriver identifikasjonstjenester, mens kapittel 5 beskriver sporbarhetstjenester. I begge kapitlene beskrives egenskaper som skiller mellom sikkerhetsnivåene, nivåene defineres og det gis veiledning i valg av sikkerhetsnivå.

2 Sikkerhetsnivå velges basert på risiko

Dette rammeverket beskriver tre sikkerhetsnivåer for identifikasjon og to nivåer for sporbarhet. Nivåene tar utgangspunkt i ulike sikkerhetsmål og beskriver løsninger som gir ulike grader av tillit til påstander om identitet. Hvilket sikkerhetsnivå som skal kreves, beror på risikoen i tjenesten, herunder hvilke konsekvenser svikt vil ha samt trusselbildet for den aktuelle tjeneste m.v.

Den enkelte virksomhet er selv ansvarlig for å velge tilstrekkelig sikkerhetsnivå. Valget må tas på bakgrunn av risikovurderinger. Valg av sikkerhetsnivå må stå i forhold til andre sikringstiltak. Autentiseringstjenester er bare en av flere sikringsmekanismer og beskytter bare mot enkelte trusler mot tjenesten. En virksomhet må bruke et sikkerhetsnivå for identifikasjon som er tilstrekkelig ut fra risikovurderingene. Det er samtidig viktig at sikkerhetskravene ikke fører til for tungvinte løsninger, og slik hindrer bruken.

Rammeverket beskriver ikke hvordan risikovurderingen skal gjøres. Vi viser til Difis veiledningsmateriell i internkontroll. Vi gjentar her enkelte punkter som er viktige å vektlegge:

- En trussel kan bli reell dersom det finnes trusselaktører med tilstrekkelig motivasjon til å prøve et angrep på tjenesten. En virksomhet må, ut fra tjenestens funksjon og den informasjon tjenesten gjør tilgjengelig, vurdere hvilke trusselaktører som kan tenkes å prøve seg, hvilke sårbarheter som skal adresseres, og hvilken kapasitet (tilgjengelige virkemidler) en trusselaktør kan ha for å utnytte sårbarhetene.
- I risikovurderingen bør virksomheten vurdere motivasjon og kapasitet for alle aktuelle trusselaktører – både basert på evne/mulighet og motivasjon. To grupper som kan være særlig aktuelle er økonomisk motivert kriminalitet og personer som har en enklere tilgang til e-ID-en eller miljøet hvor opplysningene behandles, herunder nærstående, som familiemedlemmer.
- Virkemidlene som en trusselaktør kan tenkes å bruke, vil vanligvis stå i forhold til den gevinsten trusselaktøren kan forvente å oppnå.
- Noen trusselaktører kan være på «innsiden» hos e-ID-utstederen eller en annen aktør som har en rolle i utstedelsesfasen, eller hos tjenestetilbyderen eller andre som er involvert i bruksfasen.
- I vurderingen av risiko bør virksomheten se på de(t) hendelsesforløp som gir den høyeste risikoen. Risikoen må vurderes basert på hvilke konsekvenser identifikasjons-/sporbarhetssvikt vil ha i ulike hendelsesforløp og sannsynligheten for at slik svikt inntreffer. Trusselbildet for den aktuelle tjenesten vil påvirke både hvilke konsekvenser som er aktuelle å vurdere, og sannsynligheten både for sviktende identifikasjon/sporbarhet, og for at hver av de ulike konsekvensene inntreffer.

3 Om identifikasjon

Identifikasjon betyr "gjenkjenning som den samme", og kommer av latinsk idem, som betyr 'den samme'.

Elektronisk identifikasjon gjennomføres ved at en identitetspåstand bekreftes (autentiseres) ved bruk av elektroniske identifikasjonsmidler (også kalt et elektronisk identitetsbevis eller en e-ID). Sikkerhetsnivået for identifikasjonen beror primært på identitetspåstandens presisjon og sikkerheten knyttet til *utstedelse* og *bruk* av det elektroniske identitetsbeviset.

I rammeverket er det stilt krav om at personen kan identifiseres med fødselsnummer eller d-nummer. Slik identifisering gir mulighet for gjenkjenning av personen i grunndataregistre som folkeregisteret, enhetsregisteret og kontaktregisteret⁸. Det gir også en kobling til opplysningene om identitetsgrunnlaget som lå til grunn for registreringen av personen i folkeregisteret. Fødselsnummer eller d-nummer kan enten fremgå direkte fra e-ID-en eller koplingen kan gjøres indirekte via oppslag i en autoritativ tabell som oversetter mellom e-ID og fødselsnummer eller d-nummer.

For virksomheter som ikke har behov for at personen knyttes til en identitet i folkeregisteret, vil det være mulig å benytte rammeverkets sikkerhetsnivåer med en presisering av at kravet i pkt. 3.3.1.1 er fraveket og eventuelt gitt en alternativ utforming.

3.1 Hva er autentisering

Autentisering er å verifisere en påstått identitet. Dette rammeverket omhandler kun autentisering av fysiske personer (mennesker) ved tilgang til elektroniske tjenester.

Den som skal autentiseres må inneha noe som kan bekrefte identiteten. Dette kalles autentiseringsfaktorer. En bruker kan ha en eller flere av disse avhengig av sikkerheten i løsningen. Det finnes tre forskjellige typer autentiseringsfaktorer:

- Noe personen **vet** - for eksempel et passord (kunnskapsbasert)
- Noe personen **har** - for eksempel en passordkalkulator (besittelsesbasert)
- Noe personen **er** - for eksempel et fingeravtrykk (attributtbasert, biometrisk)

Autentiseringsfaktoren(e) må på et tidspunkt bli knyttet til en bruker og dennes identitet - brukeren må også ha rådighet over autentiseringsfaktoren. Disse prosessene kan gjøres av en tredjepart eller av en tjenesteyter selv.

3.2 Sikkerhetsnivåer for identifikasjon av fysiske personer

3.2.1 Introduksjon

Sikkerhetsnivåene angir ulike grader av tillit til at påstanden om identitet, i en elektronisk kommunikasjon, er korrekt. Identitet er i dette rammeverket begrenset til å gjelde fysiske personer.

⁸ Jf. [efvf § 29](#)

Elektroniske identitetsbevis utstedes ved at en person – etter egnet identitetskontroll – gis rådighet over autentiseringsfaktorer, eller at egenskaper ved personen registreres som biometriske identifikasjonsmidler. Personen kan senere bruke disse autentiseringsfaktorene overfor en autentiseringsordning, f.eks. ID-porten.

Hvilket sikkerhetsnivå som skal kreves, beror på risikoen i tjenesten, herunder hvilke konsekvenser identifikasjonssvikt vil ha samt trusselbildet for den aktuelle tjeneste m.v.

3.2.2 Forholdet til eIDAS-nivåene

I dette rammeverket er det definert tre sikkerhetsnivåer. De bygger på eIDAS-nivåene lavt, betydelig og høyt, men det er gitt noen tilleggskrav samt noen eksempler på hvordan kravene kan tilfredsstilles i dette rammeverket. De tre sikkerhetsnivåene tar utgangspunkt i følgende eIDAS-nivåer:

- Nivå lavt – eIDAS LAVT
- Nivå betydelig – eIDAS BETYDELIG
- Nivå høyt – eIDAS HØYT

Som det fremgår av gjennomføringsrettsakt 2015/1502 er vilkårene kumulative, dvs. at krav til lavere nivåer også må oppfylles på høyere nivåer, med mindre annet eksplisitt fremgår.

Sikkerhetsnivåene 2, 3 og 4 etter rammeverket fra 2008 nivåene tilsvarer i utgangspunktet nivåene LAVT, BETYDELIG og HØYT etter dette rammeverket, som igjen bygger på eIDAS LAVT, eIDAS BETYDELIG og eIDAS HØYT.

Det er lagt til rette for at e-ID-løsninger kan utvikles slik at de oppfyller både norske krav til nivå høyt (eIDAS-krav pluss tilleggskrav) og eIDAS-krav til nivå høyt i den grad de ikke allerede gjør det.

I dette rammeverket er det gitt enkelte presiseringer/tilpasninger for å klargjøre hvor de norske nivåene ligger. Dette skyldes dels at eIDAS-nivåene foreløpig ikke har «satt seg», de er søkt utformet teknologinøytralt og nivåbasert – det gir fleksibilitet, men også uklarhet. Videre har vi gode erfaringer med e-ID-løsninger på tidligere nivå 3 og 4, og rammeverket klargjør at e-ID-er på disse nivåer fortsatt skal kunne brukes som e-ID-er på nivå betydelig eller høyt iht. det nye rammeverket.

Når rammeverket bruker begrepsparet «presiseringer/tilpasninger», er det ment å tydeliggjøre at de norske nivåene er autonome, dvs. at det er den norske beskrivelsen av nivåene som bestemmer om en e-ID-løsning oppfyller de norske kravene. For bruk i Norge er skillet mellom presiseringer og tilpasninger av nivåene ikke viktig.

Forordningen innfører en anerkjennelsesplikt. Offentlige tjenester som benytter eIDAS-nivå betydelig eller høyt, må akseptere e-ID-er fra meldte e-ID-ordninger i andre EØS-land på lik linje med norske e-ID-er på disse nivåene, jf. forordningen artikkel 6.

3.2.3 Oversikt over nivåene – noen sentrale sikkerhetsegenskaper

Tabellen under gir en enkel oversikt over noen sentrale krav for de ulike norske

sikkerhetsnivåene.

Norske nivå	Antall autentiseringsfaktorer	Utleveringskrav	Revisjonskrav
Lavt	En autentiseringsfaktor	Som for betydelig eller høyt	Intern
Betydelig	To autentiseringsfaktorer	Utlevering kan baseres på kontaktinformasjon i folkeregisteret/kontaktregisteret	Intern
Høyt	To autentiseringsfaktorer	Utlevering baseres på personlig fremmøte	Ekstern

Utleveringskrav innebærer utlevering, aktivering og utstedelse i en sammenhengende prosess.

3.2.4 Kort om sikkerhetsegenskaper som skiller nivåene

Sikkerhet i løsninger for autentisering og sporbarhet kan beskrives ved hjelp av forskjellige sikkerhetsegenskaper. En sikkerhetsegenskap er en faktor som påvirker sikkerhetsnivået i løsningen hvis den endres.

Et eksempel på slik faktor er "utlevering til bruker". For en passordløsning vil "utlevering til bruker" beskrive hvordan passordet i praksis deles ut til brukeren. Er passordene delt ut til bruker på bakgrunn av fysisk legitimering, er det vanskelig å skaffe seg et passord i andres navn. Deles passordene ut over Internett på bakgrunn av **påstått** identitet er det lett å skaffe et passord i andres navn.

Dette viser at to forskjellige krav til samme sikkerhetsegenskap endrer graden av hvor vanskelig det er å kompromittere løsningen.

Sikkerhetsnivåene i dette rammeverket er, jf. forskrift om fastsettelse av tekniske minstespesifikasjoner og minstekrav til framgangsmåter for sikkerhetsnivåene for elektroniske identifikasjonsmidler⁹, definert på bakgrunn av følgende sett av egenskaper:

- Søknad og registrering
- Krav til identitetskontroll
- Krav til autentiseringsfaktor(er) – egenskaper og antall
- Krav til utstedelse, utlevering og aktivering
- Krav til tilbakekalling, og eventuelt suspensjon og reaktivering
- Krav ved fornyelse
- Krav til autentiseringsmekanismene - hvordan autentiseringsfaktoren(e) kontrolleres forut for tilgang til tjenester
- Krav til ledelse og organisering av e-ID-tjenesten

Egenskapene er beskrevet på en teknologinøytral måte.

⁹ gjennomføringsrettsakt EU 2015/1502

3.3 Definisjon av sikkerhetsnivåene

3.3.1 Krav til alle nivåer

3.3.1.1 Personkrets og krav til sikker og entydig kobling til folkeregistrert person

Identitetspåstanden må gjelde en person som finnes i folkeregisteret. e-ID-utstederen må kunne gi en sikker og entydig kobling til denne personens identifikator i folkeregisteret (fødsels- eller d-nummer). At koblingen er sikker og entydig innebærer at koblingen ikke kan baseres på personens navn eller andre kjennetegn som kan være i bruk av flere personer.

3.3.1.2 Offentlig kontroll

e-ID-løsningene skal enten være underlagt tilsyn fra offentlig myndighet eller forvaltes direkte av et statlig organ.

Tilsynsmyndigheten har kompetanse til å avgjøre om kravsettet er oppfylt. Tilsynsmyndigheten skal vurdere alle relevante forhold, inkludert erfaringer med denne og tilsvarende løsninger (herunder sikkerhetsbrudd).

Tilsynsmyndigheten skal ha sanksjonsmuligheter dersom kravsett ikke oppfylles.

3.3.1.3 Tilsynsmyndighetens dispensasjonsadgang basert på konkret risikovurdering

Kravene til alle egenskaper er i utgangspunktet kumulative, dvs. at en e-ID-løsning som skal tilfredsstille ett sikkerhetsnivå, må oppfylle alle kravene som er satt for alle egenskapene på dette nivået.

Tilsynet kan dispensere fra dette kravet basert på en dokumentert risikovurdering. Forutsetningen for dispensasjon er at avviket fra kravet anses kompensert av andre risikoreduserende tiltak, slik at løsningen samlet sett likevel tilfredsstiller det aktuelle sikkerhetsnivået.

3.3.1.4 Om henvisninger i kravsettene

Henvisninger til *nivåer* i dette rammeverket skal forstås som henvisning til de norske nivåene, med mindre annet framgår av sammenhengen. Videre vil henvisninger i lov om tillitstjenester til bekreftelser på e-ID-nivå fra et samsvarsorgan tilfredsstilles av selvdeklarte løsninger iht. dette rammeverket, jf. eIDAS pkt 2.1.2.

3.3.2 Krav til norsk nivå lavt

Kravsettet for eIDAS lavt gjelder, med de tilpasninger som fremgår nedenfor.

Informativt: De norske nivåene krever – i likhet med eIDAS lavt – kun én autentiseringsfaktor. I Norge er imidlertid utleveringskravene til nivå lavt strengere, ved at det for utlevering henvises til eIDAS-nivå betydelig, slik det fremgår nedenfor.

3.3.2.1 Presiseringer og tilpasninger for norsk nivå lavt

Utleveringskravet til nivå betydelig gjelder, jf. eIDAS-pkt. 2.1.2 betydelig i tabellen nedenfor.

EIDAS pkt. 2.1.2 betydelig:	Kravet til å besitte et bevis kan oppfylles ved at personen godtgjør at han/hun har tilgang til en adresse (postal eller elektronisk) som er registrert på
------------------------------------	---

	personen i det norske folkeregisteret eller annet register som gir tilstrekkelig sikkerhet, eksempelvis kontaktregisteret. I tillegg må det finnes tiltak for å sikre at riktig person tar e-ID-en i bruk, typisk varsling til annen eller samme adresse.
--	--

3.3.3 Krav til norsk nivå betydelig

Kravsettet for eIDAS betydelig gjelder, med de tilpasninger som fremgår nedenfor.

Informativt: Nivået krever to ulike autentiseringsfaktorer, og utleveringssikkerheten kan baseres på folkeregistrert adresse eller tilsvarende.

3.3.3.1 Presiseringer og tilpasninger for betydelig

EIDAS krav	EIDAS-presisering
EIDAS pkt. 2.1.2 betydelig:	Kravet til å besitte et bevis kan oppfylles ved at personen godtgjør at han/hun har tilgang til en adresse (postal eller elektronisk) som er registrert på personen i det norske folkeregisteret eller annet register som gir tilstrekkelig sikkerhet, eksempelvis kontaktregisteret. I tillegg må det finnes tiltak for å sikre at riktig person tar e-ID-en i bruk, typisk varsling til annen eller samme adresse.
EIDAS betydelig (eIDAS-lovens/forordningens pkt. 2.4.6 nr. 6):	Kravet skal hindre at autoriserte personer alene og uoppdaget kan kompromittere prosessene. Kravet kan eksempelvis oppnås ved bruk av sikrede maskinvaremoduler (HSM) eller kombinasjoner av tilgangsstyring, logging, overvåking og tjenstedeling.

3.3.4 Krav til norsk nivå høyt

Kravsettet for eIDAS høyt gjelder, med de presiseringer som fremgår nedenfor.

Informativt: Nivået krever at identifikasjonsmidler utleveres basert på kontroll av foto eller biometrisk bevis. Identitetskontroll ved utlevering kan også gjøres elektronisk med annen e-ID på dette nivået.

Nivået krever at identifikasjonsmidlene består av to ulike autentiseringsfaktorer (noe du vet, har eller er).

3.3.4.1 Presiseringer og tilpasninger for høyt

EIDAS krav	EIDAS presisering for oppfyllelse av norsk nivå høyt
EIDAS pkt. 2.1.2, nr. 1a, høyt:	Med gyldig identitetsbevis regnes de identitetsbevis som tillates brukt for sterk kundeautentisering etter hvitvaskingsreglene. ¹⁰ Kravet er også oppfylt for e-ID som ble selvdeklarerert på nivå 4 iht. rammeverket av 2008.
EIDAS paragraf 2.3.1, nr. 2, høyt:	Dette kravet gjelder utlevering av identitetsinformasjon ved autentisering. Kravet er ikke til hinder for at identitetsinformasjon, f.eks. fødselsnummer, gjøres tilgjengelig på annen måte, eksempelvis i oppslagstjeneste eller at det lagres i sertifikatet for PKI-baserte e-ID-er. ⁵
EIDAS 2.4.7 høyt	Kan eksempelvis oppfylles ved revisjon iht. ISO 17065, som bl.a. dekker tillitstjenester, med relevante tilleggskrav i ETSI 319403.

3.4 Eksempler på e-ID-løsninger på ulike norske nivåer

3.4.1 Sikkerhetsnivå lavt

Dette nivået gir enkel pålogging, og tilfredsstiller nivået for mange tjenester. Det gir en viss sikkerhet for at personen er rette vedkommende. Eksempler er løsninger basert på:

- Innlogging med passord som er aktivert ved hjelp av melding til personens e-postadresse i kontaktregisteret, eller til folkeregistrert adresse
- Innlogging med brukerkonto som er aktivert gjennom e-post eller SMS-sendt adresse fra kontaktregisteret.
- Et program (app) på mobil enhet som er knyttet til personen gjennom engangskode sendt personens mobilnummer i kontaktregisteret
- Passord, program (app) på mobil enhet eller brukerkonto som er blitt knyttet til personen gjennom innlogging med annen e-ID i tråd med dette rammeverket

3.4.2 Sikkerhetsnivå betydelig

Dette nivået tilfredsstiller behovet for de fleste tjenester. Eksempler på løsninger:

- MinID, opprettet med engangspassord sendt til folkeregistrert adresse
- Tofaktorinnlogginger som måtte tilbys av markedet, men som ikke tilfredsstiller nivå høyt

¹⁰ Per 2018 regulert i hvitvaskingsforskriften § 4-3, og førerkort, bankkort med bilde, pass og nasjonale identitetskort anerkjennes som gyldig identitetsbevis.

⁵ Andre regelverks krav, eksempelvis personopplysningsloven, vil også kunne regulere spørsmålet.

3.4.3 Sikkerhetsnivå høyt

Dette nivået tilfredsstiller også behovet for tjenester med særlig høye krav til sikkerhet.

Eksempler på løsninger

- e-ID basert på personlig fremmøte og sentrallagret privatnøkkel¹¹
- e-ID basert på personlig fremmøte og privatnøkkel lagret på smartkort¹²

3.5 Veiledning for valg av sikkerhetsnivå

3.5.1 Risikovurderinger for valg av sikkerhetsnivå for identifikasjon

Sikkerhetsnivåene for identifikasjon skiller seg fra hverandre primært når det gjelder følgende egenskaper:

- I utstedelsesfasen: Identitetsfastsettelse og utlevering – hvor sikker en kan være på at e-ID utstedes og utleveres til korrekt person,
- I bruksfasen: Autentiseringsfaktorer – en eller flere, og hvor godt disse sikrer at det er korrekt person som bruker dem.

I utstedelsesfasen er trusselen at en angriper klarer å få utstedt e-ID i en annen persons navn eller klarer å stjele autentiseringsfaktoren(e) som skal utleveres til brukeren i forbindelse med korrekt utstedelse av e-ID. I bruksfasen er trusselen at en angriper kan stjele, kopiere, skaffe seg tilgang til eller på annen måte kunne misbruke en annen persons e-ID, for så å utgi seg som denne personen.

I utstedelsesfasen (inkl. utlevering) går det et viktig skille på hvorvidt tjenesten krever personlig fremmøte eller ikke.

Generelt vil nærstående, særlig personer i husstanden, har større mulighet til å misbruke e-ID-en i *bruksfasen* fordi de har lettere tilgang til både autentiseringsfaktorer og utstyr som benyttes for tilgang til elektroniske tjenester. Nærstående kan ha fått låne en annens e-ID for å utføre enkeltoppgaver (for eksempel tilgang til ektefellens bankkonto med bruk av hans e-ID¹³), og kan utnytte dette til å utføre andre handlinger (for eksempel få tilgang til helseinformasjon).

Tjenester som baseres på flere autentiseringsfaktorer (nivå betydelig og høyt), vil generelt være vanskeligere å misbruke enn løsninger som bare benytter én faktor.

I bruksfasen kan en e-ID misbrukes også av en utenforstående som stjeler, kopierer eller på annen måte skaffer seg tilgang. Statistiske autentiseringsfaktorer kan være utsatt for kopiering ved gjetting (for eksempel passord), avlytting av kommunikasjon eller innbrudd i brukerens utstyr. Noe en har (engangspassordkalkulator), smartkort kan stjeles.

Ved innbrudd i brukerens utstyr kan en angriper få tak i autentiseringsfaktorer som er lagret

¹¹ Per 2018 tilfredsstilles dette kravet av BankID

¹² Per 2018 tilfredsstilles dette kravet av Buypass og Commfides. eID på nasjonalt id-kort skal også tilfredsstille dette kravet. .

¹³ Dette er i så fall uautorisert bruk fordi det vil være i strid med utsteders vilkår for bruk av e-ID-en, da disse er strengt personlige.

der, men en angriper kan også plante programkode som oppdager at brukeren selv legitimt bruker e-ID-en, og kopiere og utnytte dette.

Eksempler på hendelser som følge av bruk av falsk e-ID eller kompromittering av e-ID og som bør tas med i en risikovurdering. Hendelsene er beskrevet i tråd med anbefaling i Difis internkontrollveilederen.

- Kriminelle får utstedt e-ID til person på hemmelig adresse, logger inn og ser hvor personen går på skole. Taushetspliktsbrudd. Personen oppspores og utsettes for grov vold.
- En lærer logger seg på en læringsplattform på storskjerm i klasserommet med funksjonen «vis passord» på. En elev noterer seg brukernavn og passord, logger seg senere på og endrer en annen elevs karakter fra bestått til stryk. Integritetsbrudd. Taushetspliktsbrudd (karakterer er taushetsbelagt informasjon). Den andre eleven stryker i faget.
- En arbeidskollega utnytter en glemt utlogging på et sykehus, og får sett helseopplysninger om en nabo. Taushetspliktsbrudd. Stigmatiserende helseopplysninger om naboen spres, og personen utstøtes i lokalmiljøet.
- En elev låner mobilen til en medelev, og logger inn som vedkommende med sms-passord. Eleven sender trakasserende meldinger i den andre elevens navn til flere klassekamerater. Integritetsbrudd. Eleven som får meldingene sendt i sitt navn blir utvist, da skolen har nulltoleranse for mobbing.
- Fremmed stat får utstedt e-ID i helsepersonells navn, og endrer helseopplysningene til politisk sentral person. Integritetsbrudd. Personen får uriktig helsehjelp, og dør.

En risikovurdering av behovet for identifikasjon opp mot sikkerhetsmål må ta i betraktning trusler og tiltak som selve e-ID-en ikke, eller i begrenset grad, kan beskytte mot. Eksempler på slike trusler knyttet til identifikasjon er for eksempel:

- En angriper kan kompromittere brukerens utstyr, slik at bruken av e-ID-en kan kontrolleres av angriperen, for eksempel til å logge på et annet sted enn brukeren er klar over.
- Phishing-angrep kan lure brukeren til å gå til en nettside kontrollert av angriperen, og røpe sine e-ID-hemmeligheter.
- Det legitime nettstedet kan være kompromittert slik at brukerens e-ID kan misbrukes.
- Hvis kommunikasjonen ikke er kryptert, kan den avlyttes slik at e-ID-informasjon kan stjeles.

Beskyttelse mot en del av disse truslene er i hovedsak nettstedets ansvar, for eksempel bruk av kryptering. Nettstedet bør også, som del av beskyttelse mot phishing, sørge for å bruke en god løsning for nettstedssautentisering. Men brukeren selv har også et ansvar for å holde seg unna phishing-nettsteder.

Identifikasjonstjenester øker sannsynligheten for at det er den identifiserte personen som bruker tjenesten. Sikkerhetsnivå for e-ID er en viktig parameter i dette. Sikkerheten i selve bruken av tjenesten, for eksempel hvilke funksjoner og informasjon brukeren skal ha tilgang til (autorisasjoner), må løses med andre mekanismer.

3.5.2 Praktiske eksempler på tjenester som kan benytte de forskjellige sikkerhetsnivåene

Dette er eksempler på hvordan sikkerhetsnivåene kan brukes. Tjenesteeier må gjøre sin egen vurdering av trusselbildet for sin tjeneste, jf. avsnittet ovenfor, herunder vurdere risikoen for sikkerhetsbrudd og konsekvenser ved å kreve et bestemt sikkerhetsnivåer.

Nivå lavt

- Mange tjenester, blant annet skolepålogging som gir innsyn i egne lekser og karakterer. Innsyn for å se skattelisteopplysninger, åpne folkeregisteropplysninger. Innsending av skjema (barnehagesøknad etc), statistikkoppgaver.

Nivå betydelig

- De fleste tjenester med taushetsbelagte opplysninger, blant annet innsyn i selvangivelser. Vaksineoversikter.

Nivå høyt

- Tjenester som gir innsyn i taushetsbelagte opplysninger med særlig beskyttelsesbehov, herunder stigmatiserende opplysninger, forretningskritisk informasjon, sikkerhetskritisk informasjon og de fleste helseopplysninger.

4 Om sporbarhet

4.1 Hva er sporbarhet?

Mens identifikasjon handler om å avklare hvem du samhandler med, går sporbarhet ut på å dokumentere samhandlingen over tid. Krav til sporbarhet beskriver i hvilken grad det i ettertid skal være mulig å sannsynliggjøre at en aktør står bak et informasjonselement eller har utført en handling på et bestemt tidspunkt.

Sporbarhet innebærer at en er i stand til å fremskaffe et bevis med en viss styrke for bestemte handlinger. Denne egenskapen blir tidvis omtalt som ikke-benekting, men dette er en språkbruk vi mener er uheldig. Vi fraråder derfor at man snakker om ikke-benekting fordi sporbarhet handler om nyanser i grått, grader av sikkerhet vurdert opp mot risikoen, ikke et enten/eller.

Vi skiller mellom styrken på identifikasjonen (identifikasjonsstyrke), styrken på koplingen mellom informasjonselementet og identifikasjonen (bindingsstyrke), styrken på beviset samt styrken på hvor godt beviset er vernet mot endringer over tid (integritetsstyrke).

Virksomheten må avgjøre hvilke deler av samhandlingen som skal spores, eksempelvis hva brukeren er gjort kjent med (fått forevist), hva hun har samtykket til eller levert inn. I det følgende brukes for enkelhets skyld begrepet «dokument» for informasjonselementet som beviset/sporet knyttes til, uten at dette er ment som en begrensning.

Sporbarhet består i:

- Produsere dokumentasjon (av en eller annen styrke) for at en bestemt aktør utførte en handling på et bestemt dokument på et bestemt tidspunkt.
- Lagre dokumentasjonen så lenge det er påkrevd, og med tilstrekkelig sikkerhet for at den ikke slettes eller kan endres.

Dokumentasjonsverdien vil blant annet bero på muligheten til - på bevisføringstidspunktet - å sannsynliggjøre at dokumentet er autentisk.

Styrken av et bevis er først og fremst avhengig av hvor pålitelig informasjonen i beviset er. En handling utføres alltid i en kontekst, for eksempel en prosess som ender opp med at brukeren "signerer" et dokument eller klikker "aksepterer" på en nettside. Et bevis vil aldri kunne dokumentere hele konteksten.

Kort tid etter en handling kan det være enkelt å rekonstruere konteksten, for eksempel ved å referere til en nettside som fortsatt eksisterer og ikke er endret. Over tid vil konteksten gradvis "glemmes", og dette vil uvegerlig føre til at bevis uansett vedlikehold vil svekkes over tid.

Det vil så være opp til den som skal vurdere beviset, i siste instans en domstol, å vurdere styrken av beviset.

4.1.1 Produksjon av dokumentasjon

Dokumentasjonen vil gjerne bestå av følgende:

- Hvem har samhandlet? Klarhetshensyn taler for at aktørene identifiseres entydig, eksempelvis med organisasjonsnummer eller fødselsnummer. Tilliten til

identitetspåstanden kan styrkes gjennom at de er autentiserte, jf. sikkerhetsnivåene som er beskrevet tidligere i dokumentet.

- Hva er handlingen? Det bør framgå tydelig av beviset hva konteksten for handlingen er på en eller annen måte, eksempelvis at et dokument er sett, lest, godkjent, sendt inn, videresendt.
- Hvilket dokument knytter handlingen seg til?
- Hva er tidspunktet for handlingen? Som oftest vil det være viktig for vurderingen av dokumentasjonsverdien at tidspunktet for handlingen er kjent. Det vil også gjøre det enklere å knytte beviset til annen dokumentasjon.

Styrken på et bevis avgjøres først og fremst av hvor korrekt og pålitelig informasjonen er for de fire elementene. I tillegg har et bevis en "teknisk styrke" som avgjøres av hvor sterkt selve beviset beskyttes, det vil si hvor vanskelig det er å endre beviset/sporet eller produsere et forfalsket bevis/spor.

4.1.2 Lagring og vedlikehold av bevis

Dersom det er behov for å lagre dokumentasjonen over lang tid, f.eks. flere tiår, må noen særlige utfordringer håndteres. Dokumentasjon forvitrer over tid. Dette skaper tillegg utfordringer knyttet til for eksempel:

- Bevisets lesbarhet over tid, som kan utfordres av bytte av IT-systemer eller IT-leverandører og/eller formater.
- Svekkelse av kryptografiske mekanismer og nøkler, der økt prosessorkapasitet i fremtiden kan føre til at mekanismer som er sikre i dag, blir for svake etter en viss tid.

4.1.3 Bevisførsel

Dersom en trenger å bruke beviset, må det kunne presenteres på en tillitvekkende måte. Det vil si at det må kunne sannsynliggjøres at dokumentasjonen er et sannferdig uttrykk for hva som skjedde. Merk at det i en del tilfeller kan være utfordrende å finne igjen og samle sammen informasjon som skal utgjøre et bevis, for eksempel dersom informasjonen skal hentes fra forskjellige logger.

4.1.4 Virkemidler for å sikre sporbarhet

Sporbarhet kan sikres ved hjelp både av tekniske, organisatoriske og rettslige tiltak. Vi beskriver her kort noen aktuelle løsninger, som kan være etablert av virksomheten selv (egenregi), av aktører i markedet (tillitstjenester) eller av offentlige fellesløsninger.

4.1.5 Virkemidler fra aktører i markedet (tillitstjenester m.v.)

eIDAS-forordningen spesifiserer felles regler for hele EØS-området når det gjelder aksept av elektroniske dokumenter, elektroniske signaturer (signatur av en fysisk person) og elektroniske segl (virksomhetssignatur). For å understøtte bruk av elektroniske dokumenter, signaturer og segl definerer eIDAS ett sett med tillitstjenester som skal kunne tilbys av kommersielle aktører i EUs indre marked. Tillitstjenestene som defineres av eIDAS, er:

- Certifikater for elektronisk signatur, det vil si til fysiske personer
- Certifikater for elektronisk segl, det vil si til juridiske personer (virksomhetscertifikater)
- Elektronisk tidsstempling
- Elektronisk tjeneste for rekommandert sending
- Certifikater for autentisering av nettsteder (web-autentisering)
- Valideringstjenester for elektronisk signatur og elektronisk segl
- Lagringstjenester for elektronisk signatur og elektronisk segl

eIDAS definerer en kvalifisert tillitstjeneste som en av tjenestene ovenfor, tilbudt på en måte som oppfyller kravene i eIDAS. Dette inkluderer krav til tredjepartsrevisjon og tilsyn. Ikke-kvalifiserte tillitstjenester kan underlegges tilsyn i tilknytning til hendelser.

Elektroniske signaturer er i eIDAS definert som mekanismer som binder et dokument til en person som signerer dokumentet. Begrepet elektronisk signatur er i utgangspunktet teknologinøytralt. eIDAS definerer flere typer (tilsvarende for segl):

- Elektronisk signatur: Alle mekanismer som knytter en person til informasjonen som signeres.
- Avansert elektronisk signatur: Krever i praksis PKI-teknologi med certifikater, men med få krav til kvalitet. Signaturen kan også baseres på et kvalifisert sertifikat, da er det stilt krav til utstedelsen og oppbevaring av privat signeringsnøkkel.
- Kvalifisert signatur: Avansert signatur med kvalifisert sertifikat og tilleggskrav til oppbevaring av signeringsnøkkel i sertifisert elektronikk.

Alle ovennevnte signaturløsninger vil kunne tilfredsstille sporbarhetsnivå 2 iht. dette rammeverket.

Samtlige tillitstjenester er relevante for sporbarhet. Signaturer/segl kan brukes til å forsegle dokumentasjonen. I elektronisk leveringstjeneste bevarer tjenestetilbyderen meldinger som er forseglet av avsender.

I tillegg til eIDAS' tillitstjenester vil det kunne finnes andre løsninger i markedet, som kan brukes for å sikre sporbarhet. Identifikasjonsløsninger, jf. beskrivelsen over, og digitale postkasser er eksempler på slike tjenester. I Norge tilbys digitale postkasser – fra private leverandører – som en fellesløsning i offentlig regi. Det vil også kunne etableres andre løsninger som skal bekrefte at informasjon ikke er blitt endret.

4.1.6 Offentlige fellesløsninger som understøtter sporbarhet

Offentlig sektor har etablert flere tillitstjenester som infrastruktur. Tjenestene er til dels etablert av det offentlige selv og til dels basert på løsninger fra markedet. Tjenestetilbudet vil være i utvikling i takt med offentlig sektors behov. Per 2018 fantes følgende offentlige fellesløsninger som kan benyttes for å ivareta sporbarhetsbehov:

- Sikker digital post (digipost, eboks) og meldingsboksen i Altinn for elektronisk meldingsutveksling og lagring av (signerte) dokumenter,
- Difis signeringstjeneste dekker flere funksjoner
 - Avansert elektronisk signatur med kvalifisert sertifikat basert på tjenester fra sertifikatutstedere i markedet.
 - Elektronisk signatur supplert med avansert elektronisk segl fra

- signeringstjenesten for å "forsegle" bevis for elektronisk signering,
 - Tidsstempling knyttet til elektroniske signaturer og segl,
 - Lagringstjeneste for dokumenter med elektronisk signatur eller segl.
- Difis tidsstemplingstjeneste
- Altinns juridiske logg for elektronisk signatur og støtte for avanserte signaturer i forbindelse med skjemainnsending.

4.1.7 Løsninger i virksomheten

Logging av informasjonselementer og handlinger i virksomhetens egne IKT-løsninger kan i mange tilfeller også være et egnet virkemiddel for økt sporbarhet. Bruk av egen logginformasjon fra egne løsninger som bevis fordrer at kvaliteten på informasjonen som er blitt logget er god og at en kan ha tillit til at informasjonen ikke er blitt endret. Virksomheter som er avhengig at denne typen virkemidler bør ha utviklet god internkontroll og et godt utviklet styringssystem for informasjonssikkerhet. For blant annet å kunne forhindre endringer fra egne ansatte, kan ev. integritetssikring ved hjelp av tidsstempling benyttes.

Logginformasjon fra egne systemer som bevisførsel bidrar til å anskueliggjøre informasjonselementer eller handlinger, men erstatter ikke behovet for, eller betydningen av, internkontroll innad i tjenesten som et nødvendig ledd for å sikre tillit til et styringssystem for informasjonssikkerhet. Særskilt bør det for tjenesten vurderes sikringstiltak i henhold til god praksis for logging, eksempelvis som etter ISO 27001 A12.4: Logging and monitoring, hvor det heter i:

- 12.4.1 Handlingslogg (Event logging): Registrér informasjon om tilgang og handlinger av brukere, feil, hendelser etc. i informasjonssystemer.
- 12.4.2 Beskyttelse av handlingslogg (Protection of log information): Loggene må beskyttes, ettersom de ikke skal kunne fjernes eller endres av uvedkommende. Her bør reglene kun tillate endring av loggen av bestemte personer.
- 12.4.3 Adskilt systemadministratorlogg (Administrator and operator logs): Ettersom administratorer ofte har flere privilegier og brukerrettigheter enn vanlige brukere, kan de utføre flere handlinger på systemer. Med tanke på sporbarhetskrav, anbefales det at systemer registrerer lik informasjon om alle brukere, uavhengig av hvilke privilegier de har i systemene.
- 12.4.4 Synkroniserte klokker (Clock synchronization): Alle systemer bør konfigureres med samme tid og dato for å forenkle sporbarhet hvis en hendelse oppstår og det skal utføres en sporbarhetstest av hva som har skjedd i de forskjellige systemene som er involvert.

Ofte vil det være tilstrekkelig at virksomheten er pålagt å ha rutiner som sikrer arkivmateriale.

Teknikker som vil styrke tilliten til løsningene kan være:

- Loggen er sikret mot endringer i ettertid. Ulike former for kryptografiske mekanismer kan benyttes til sikring av logginformasjon. I tillegg kan løsninger som sikrer engangsskrivning av informasjon benyttes.
- Loggen bør oppdateres i sanntid med informasjonselementer og handlinger som utføres
- Løsningen bør fortrinnsvis være utformet med logging av bevis som funksjon slik at informasjonen som logges er tilstrekkelig og sikret for formålet.

- Logget informasjon bør være knyttet til annen aktivitet i virksomheten (daily business practice) slik at det anskueliggjøres at virksomheten selv har tillit til informasjonen.
- Det kan innhentes tredjeparts vurdering av styrken (prosess og metoder) for logging og på at disse følges.
- Implementering av A12.4 tiltak som beskrevet ovenfor.

Riksarkivaren har gjennom NOARK-standardene stilt krav til arkivsystemer, for at kravene i arkivforskriften skal kunne oppfylles. Systemer som følger disse kravene skal sikre integriteten til de journalførte saksdokumentene. Kravene gjelder både for arkivering i særskilte arkivsystemer og for arkivering i fagsystemer.

4.2 Definisjon av sikkerhetsnivåer for sporbarhet/bevissikring

Krav til sporbarhet vil dels bestå av krav til autentisering av handlingen som det skal sikres dokumentasjon for. Her vil det kunne stilles krav til e-ID-nivå iht. beskrivelsen i kapittel 3.3.

I tillegg kan det stilles krav til koblingen mellom (eller forseglingen av) autentiseringen og informasjonselementet og til sikring av integritet og tilgjengelighet for denne dokumentasjonen.

Vi beskriver her to nivåer:

Nivå 1

Det skal foreligge rutiner og logger, som gjør at det er rimelig sikkert at kommunikasjonsparten står bak en handling eller et informasjonselement. Det er ikke nødvendig å bruke tredjepart for å oppnå dette nivået.

Nivå 2

I tillegg til kravene i nivå 1: En part skal ikke i ettertid selv kunne produsere eller endre på et bevis for at den andre part står bak en handling eller et informasjonselement. Dette forutsetter bruk av tredjepart, dvs. tjenester fra markedet (tillitstjenester m.v.), offentlige fellesløsninger eller annet. Tredjeparten må ha tilstrekkelig uavhengighet fra partene.

4.3 Eksempler på løsninger som kan tilfredsstillere sporbarhetskrav

Nedenfor følger eksempler på løsninger som kan tilfredsstillere sporbarhetskrav i henhold til nivåene gitt ovenfor.

Nivå 1

For nivå 1 skal det foreligge rutiner og logger, som gjør at det er **rimelig sikkert** at kommunikasjonsparten står bak en handling eller et informasjonselement. Eksempler på handlinger hvor slik sporing kan anses som rimelig sikker bevisførsel er som følger:

- Innkommet brev som er arkivert i NOARK-system, og hvor det kan sannsynliggjøres at parten stod bak brevet, eksempelvis gjennom annen saksbehandling (herunder utbetalinger) eller kommunikasjon.
- Kopi av utgående brev som er arkivert i NOARK-system, og hvor det foreligger logininformasjon som viser at brevet er sendt.
- Logg i fagsystem for elektronisk innsending av skjema, basert på innlogging med e-ID.

- Logg fra chat med innlogget person, med tidspunkt.
- Tidsstemplet registrering i fagsystem av kontakt (f.eks. fysisk møte) med person hvor identiteten er tilstrekkelig godtgjort.
- Bildebevis hvor personen er gjenkjennbar, som er automatisk lagret i system med logging av tidspunkt.

Nivå 2

En part **skal ikke i ettertid selv kunne produsere eller endre** på et bevis for at den andre part står bak en handling eller et informasjonselement.

Eksempler på løsninger som kan tilfredsstille nivå 2 mht. å sannsynliggjøre at **private** står bak en handling eller et informasjonselement:

- Dokument og autentisering som er bekreftet av tredjepart gjennom bruk av segl eller digital signatur i webløsning, som for eksempel Difis signaturtjeneste.
- Dokument og autentisering som sendes inn og er bekreftet av tredjepart gjennom bruk av segl eller digital signatur.
- Logg i fagsystem, som nær handlingstidspunktet er tidsstemplet av tredjepart.
- Bruk av leveringstjeneste fra tredjepart, som sannsynliggjør avsenders identitet og sendingstidspunkt.
- Logg i Altinns juridiske logg av innsendt skjema.

Eksempler på løsninger som kan tilfredsstille nivå 2 mht. å sannsynliggjøre at **forvaltningen** står bak en handling eller et informasjonselement:

- Bruk av leveringstjeneste fra tredjepart, som sannsynliggjør avsenders identitet og sendingstidspunkt.
- Brev fra forvaltningen formidles via offentlig fellesløsninger for digital post, som sannsynliggjør avsenders identitet og sendingstidspunkt.
- Sending av dokumentet med elektronisk segl med sertifikat utstedt av tredjepart.

4.4 Veiledning i valg av sikkerhetsnivå

4.4.1 Risikovurdering for valg av sikkerhetsnivå for sporbarhet

Valg av sikkerhetsnivå for sporbarhet må baseres på en risikovurdering.

Formålet med sporbarhetskrav er å bidra til at faktum kan sannsynliggjøres, slik at riktig faktum legges til grunn av alle; både partene, forvaltningen og – hvis uenigheten tas inn for retten – av domstolen. Når det er høy sannsynlighet for at riktig faktum vil bli lagt til grunn av domstolen, vil det øke tilliten til forvaltningen og redusere faren for at uriktige krav fremmes for domstolen.

Sporbarhetskrav bidrar primært til at dokumentbevis kan fremskaffes, men vil også kunne suppleres av vitnebevis om hvordan dokumentbeviset er produsert, og hvor robust det er. For rettslige tvister vil også andre forhold kunne være relevante for bevisvurderingen.

Tjenesteeierne må vurdere dokumentasjonskravene opp mot trusselbildet (hvilke andre feil kan skje, hvem har gevinst av at feil skjer/motivasjon for å fremprovosere feil), og hvilken mulighet er det eventuelt for å dokumentere hvem som har fordel av feilen.

Hvor store ressurser som skal brukes på å sikre dokumentasjon av en bestemt handling beror på risikobildet, jf. at ressursene bør brukes der de gir størst effekt. Eksempelvis kan ofte dokumentasjonen av handlingene i den elektroniske løsningen være en liten del av et større bevisbilde, hvor grunnlaget for kravet fremgår andre steder. Eksempelvis ved krav om tilbakebetaling av lån kan andre aktuelle bevis være at eleven gikk på skole, hadde rett til lån, hvilke andre inntekter studenten hadde i perioden, og at beløpet kom inn på konto og ble brukt. Det vil si at behovet for sporbarhet også vil komme an på om handlingen kan dokumenteres indirekte gjennom andre bevis.

Nivå 1 er i mange henseender å anse som god praksis.

Dersom en risikovurdering tilsier at kommunikasjonspartene ikke selv skal kunne produsere eller endre på handlinger eller informasjonselementer, bør det vurderes bruk av en eller flere av mekanismene for sikring på nivå 2.

Det skilles mellom to ulike faser i samhandlingen mellom kommunikasjonspartene, hvor det stilles krav til sporbarhet:

- på selve handlingstidspunktet (logging, gode rutiner, hashing), og
- ved langtidslagring (ulike arkivløsninger, NOARK)

Sikkerhetsnivåene for sporbarhet skiller seg fra hverandre primært når det gjelder følgende egenskaper:

- Handlingstidspunktet: Sporbarhet ved rutiner og logger– hvor sikker en kan være på at logging av handlinger og informasjonselementer ved e-ID ikke kompromitteres ved bruk,
- Langtidslagring: God arkivering – hvor godt disse arkiveringstjenestene sikrer at informasjonen ikke kan endres på et senere tidspunkt.

Trusselen på handlingstidspunktet kan være at en angriper klarer å endre dokumentasjonen om logging av handlinger eller informasjonselementer. En trussel ved langtidslagring kan være at en angriper kan skaffe seg tilgang til informasjonselementer eller endre logging av handlinger på et senere tidspunkt.

En risikovurdering for sporbarhet må også ta i betraktning trusler og tiltak som logging og lagring av handlinger gjennomført med e-ID-en ikke, eller i begrenset grad, kan beskytte mot. Slike trusler knyttet til sporbarhet er for eksempel:

- Den opprinnelige og legitime loggen kan endres av en utro tjener, slik at brukerens e-ID kan koples til feilaktig handlingstidspunkt.

Eksempler på hendelser som kan følge av at en trusselaktør produserer eller endrer på dokumentasjon er:

- En lege endrer en pasientjournal etter å ha blitt kjent med en klage, slik at feilbehandling ikke lenger er dokumentert i journalen. Integritetsbrudd. Pasienten får ikke erstatning for feilbehandlingen.
- En tilbyder leverer forfalsket elektronisk skatteattest i forbindelse med tilbudsinnlevering. Falsk. Tilbyder vinner konkurransen på feilaktig grunnlag, og konkurrent vinner fram med

klage, det offentlige taper tid og penger.

- En bruker har levert en søknad, men søknaden kan ikke gjenfinnes på grunn av kryptovirus. Integritetsbrudd. Bruker må sende inn på nytt.
- En bruker hevder uriktig å ha levert en søknad. Virksomheten er rammet av kryptovirus, og kan ikke gjenfinne søknader. Falsk. Virksomheten velger å stole på brukers påstand, tillater ny innsending, og bruker slipper sanksjon for manglende søknad.
- En administratorbruker utnytter tilgang til eksamensoppgaver og selger dem før eksamen. Han sletter sine loggspor. Integritetsbrudd. Noen kandidater får bedre karakter enn de fortjener, og forbigår mer kompetente søkere i første ansettelsesprosess.
- Teknologiske framskritt muliggjør endring av digitalt signert skjøte. En hjemmelshaver fjerner statens veirett fra skjøtet. Integritetsbrudd. Staten påføres kostnader, vanskelig å oppspore gode vitner.
- En lærer logger seg på en læringsplattform på storskjerm i klasserommet med funksjonen «vis passord» på. En elev noterer seg brukernavn og passord, logger seg senere på og endrer en annen elevs karakter fra toppkarakter til stryk. Integritetsbrudd. Eleven klager, vinner fram, og læreren får refs for uforsvarlig karaktersetting.

Slike hendelser bør tas med i en risikovurdering, men selv om risikovurderingen viser at nivå 1 er tilstrekkelig, er det ikke noe til hinder for at løsninger fra nivå 2 benyttes. I noen tilfeller vil det være rimeligere å benytte løsninger fra nivå 2 for å sikre sporbarheten, enn ved kun å bruke tiltak i virksomheten. Det er imidlertid viktig at man vurderer hele risikobildet, og tar hensyn til både gevinster (risikoreduksjon, reduserte kostnader til å dekke tap) og ulemper (kostnader ved tiltaket, ulemper for brukerne, ev. redusert bruk) ved de valgte sikkerhetstiltak.

4.4.2 Praktiske eksempler på tjenester som kan benytte de ulike sikkerhetsnivåene for sporbarhet

Nivå 1

De fleste tjenester.

Nivå 2

Tjenester hvor risikovurderingen viser en særlig risiko for at partene produserer eller endrer på bevis, eksempelvis tilfeller hvor man har tapt rettssaker på grunn av utilstrekkelig dokumentasjon.

5 **Referanser**

1. [e-forvaltningsforskriften](#)
2. [Digital Identity Guidelines, Nist 800-63-3 22.6.2017](#)
3. [Rammeverket](#) av 2008
4. eIDAS gjennomføringsrettsakt om sikkerhetsnivåer http://eur-lex.europa.eu/eli/reg_impl/2015/1502/oj

6 Vedlegg 1 – gjennomføringsrettsakt

Se https://eur-lex.europa.eu/eli/reg_impl/2015/1502/oj