



Entydig identifisering

Veiledning for tilbydere av offentlig nummerbasert person-til-person-kommunikasjonstjeneste

Versjon 1.0

23. juni 2025

Innledning

I denne veiledningen tar Nasjonal kommunikasjonsmyndighet (Nkom) sikte på å klargjøre reglene om entydig identifisering i ekomlov og – forskrift. Veiledningen vil være et levende dokument som vil oppdateres med ytterligere vurderinger etter hvert som disse aktualiseres.

Nkom har i tiden etter ikrafttredelse av ny ekomlov og -forskrift 1. januar 2025 mottatt flere spørsmål og henvendelser knyttet til entydig identifisering. Nkom anser at svarene og vurderingene vil ha nytteverdi for hele bransjen. Nkom er i tildelingsbrev for 2025 også gitt i oppdrag å gjennomføre tilsyn med reglene om entydig identifisering. Kjennskap og kunnskap om regelverket er av stor viktighet for tilbydere av offentlig nummerbasert person-til-person-kommunikasjonstjeneste. Dette er bakgrunnen for veiledningen.

I veiledningen skal begrepet «tilbyder» forstås som «tilbyder av offentlig nummerbasert person-til-person-kommunikasjonstjeneste».

Veiledningen inneholder en gjennomgang av relevant regelverk. Etter hvert emne har vi samlet diverse spørsmål & svar (Q&A). Disse spørsmålene er delvis basert på konkrete henvendelser fra bransjen, delvis utformet av Nkom selv.

Ved spørsmål til veiledningens innhold eller forslag til ytterligere tema oppfordres det til å ta kontakt med Nkom på e-post firmapost@nkom.no. Henvendelsen bør merkes med «Veiledning entydig identifisering».

Regelverk

Av ekomloven 2003 § 2-4 fremkom det at tilbyder av offentlig telefontjeneste ved «inngåelse, endring eller opphør av avtalen skal sikre at sluttbruker er entydig identifisert» og at tilbyderen «skal kunne dokumentere» identitetskontrollen. Det har altså vært krav til entydig identifisering lenge. Med ny ekomlov og -forskrift er kravene strammet inn og konkretisert.

Formålet med reglene om entydig identifisering er å sikre at den reelle identiteten til sluttbruker knyttes til telefonnummeret, herunder å redusere omfanget av forveksling, misbruk av andres identitet og identitetstyveri. Hensyn knyttet til Politiets arbeid med kriminalitetsbekjempelse er også et sentralt element i denne sammenheng. I tillegg er overføring av korrekt informasjon om abonnenten ved nødansrop viktig for nødetatenes håndtering av hendelser.

Det følger klart av ordlyden både i ekomloven og i ekomforskriften at det er tilbyder som har ansvaret for at kravet om entydig identifisering er oppfylt. Begrepet entydig identifisering er en rettslig standard som må tolkes i lys av den teknologiske utviklingen.

Innstrammingen av reglene om entydig identifisering ble foreslått allerede i 2019. En versjon av de nå vedtatte reglene var på høring publisert av daværende Kommunal- og moderniseringsdepartement (KMD) den 3. september 2019. Bakgrunnen for høringen var å tydeliggjøre kravet til entydig identifisering ved inngåelse, endring og oppsigelse av avtale. Rent konkret hadde det i 2019 vært avdekket tilfeller av såkalt mobilkapring hvor uvedkommende porterer telefonnummer uten eiers viten og vilje.

Forslaget fra 2019 bygget på allerede gjeldende rutiner hos tilbyderne, samt Nkoms erfaring fra tidligere tilsyn. Forslaget er i hovedsak tilsvarende det som i dag er vedtatt og gjeldende, med noen ordlydsforskjeller. Høringsnotatet fra 2019 er følgelig en viktig tolkningskilde og kan finnes på departementets nettsider her: [Høring om endringer i ekomloven og ekomforskriften med forslag om lovhjemmel for leveringsplikt for bredbånd og tydeligere krav til entydig identifisering av sluttbrukere - regjeringen.no](#)

De nye bestemmelsene om entydig identifisering som ble sendt på høring i 2019 ble ikke vedtatt på det tidspunktet. Ny ekomlov og -forskrift ble sendt på høring 2. juli 2021. Under merknadene til bestemmelsene om entydig identifisering i forskriften skriver departementet at reglene er modifisert og justert basert på innkommende høringsinnspill i 2019.

Høringsrundene har medført beskjedne endringer og reglene om entydig identifisering som ble hørt i 2021 er i hovedsak like de reglene som ble vedtatt i 2024. Det grunnleggende kravet til entydig

identifisering er fastslått i ekomloven § 2-8. Regler om hvordan slik entydig identifisering skal gjennomføres finnes konkretisert i ekomforskriften §§ 1-8 og 1-9.

Ekomloven § 2-8 lyder:

§ 2-8. Entydig identifisering av sluttbruker

Tilbyder av offentlig nummerbasert person-til-person-kommunikasjonstjeneste skal ved inngåelse, endring eller opphør av avtalen sikre at sluttbrukeren er entydig identifisert. Tilbyder skal kunne dokumentere identitetskontrollen.

Departementet kan gi forskrift om krav til entydig identifisering av sluttbruker, herunder identitetskontroll.

Ekomforskriften § 1-8 lyder:

§ 1-8. Entydig identifisering av fysiske personer

Sluttbrukere som er fysiske personer, skal identifiseres entydig, jf. ekomloven § 2-8, på en av følgende måter:

- a. fremleggelse av originalt og gyldig pass, nasjonalt ID-kort eller norsk førerkort – og hvis personen ikke har norsk fødselsnummer eller D-nummer, identitetsbevis med fødselsdato, fødested, fotografi og statsborgerskap,
- b. bruk av elektronisk identifikasjon som er selvdeklartert til eID-nivå «betydelig» eller «høyt» etter selvdeklarasjonsforskriften.

Tilbyder skal registrere hvilken type identitetsbevis som er benyttet ved identifikasjonskontroll og identitetsbevisets kontrollnummer, for å dokumentere hvordan kravet til entydig identifisering er oppfylt.

Endringer i abonnementstype og prisplan krever ikke entydig identifikasjon, med unntak av hemmelig nummer, jf. § 4-13

Ekomforskriften § 1-9 lyder:

§ 1-9. Entydig identifisering når sluttbruker er et foretak mv.

Når sluttbrukeren er et foretak, skal entydig identifisering, jf. ekomloven § 2-8, skje ved at det innhentes foretaksnavn, organisasjonsform, organisasjonsnummer, adresse og navnet på daglig leder og styremedlemmer, eller personer i tilsvarende stilling. Tilsvarende opplysninger skal innhentes og egnede tiltak etter denne bestemmelsen skal gjennomføres så langt det passer når sluttbrukeren er en annen juridisk person enn et foretak.

Fysiske personer som handler på vegne av et foretak eller annen juridisk person, skal identifiseres i samsvar med § 1-8.

Elektronisk identifikasjon ved elektronisk segl er gyldig som identifikasjon av foretaket når identiteten ikke bekreftes etter første og andre ledd. Det elektroniske seglet må tilfredsstillende kravene til kvalifisert sertifikat i henhold til eIDAS-forordningen artikkel 38, og være inkludert i tillitslisten, jf. artikkel 22, som gjennomført i lov 15. juni 2018 nr. 44 om elektroniske tillitstjenester.

Opplysninger som nevnt i første ledd, skal bekreftes ved oppslag mot eller utskrift fra et offentlig register eller firmaattest, som ikke er eldre enn tre måneder. Retten til å handle på vegne av foretaket skal også bekreftes.

Nkom viser også til hvitvaskingsregelverket. Det ble sett hen til dette området og dets regler om kundekontroll ved utforming av reglene. Nkom har derfor også vurdert dette regelverket i vår tolkning. Som vi kommer tilbake til har også Finanstilsynets veileder til hvitvaskingsloven overføringsverdi, se: <https://www.finanstilsynet.no/nyhetsarkiv/rundskriv/2022/veileder-til-hvitvaskingsloven/>

Generelle krav om entydig identifisering

Ekomloven § 2-8 oppstiller hovedregelen om entydig identifisering. For å tydeliggjøre bestemmelsens virkeområde kan vi dele den opp:

PLIKTSUBJEKT:

Kravet om entydig identifisering retter seg mot **tilbyder av offentlig nummerbasert person-til-person-kommunikasjonstjeneste**. Nummerbasert person-til-person-kommunikasjonstjeneste er definert i ekomloven § 1-5, nr. 6, jf. nr. 5. Tilbyder er definert i samme bestemmelse nr. 11. At en tjeneste er «offentlig» innebærer at den er tilgjengelig for eller beregnet til bruk for allmennheten, sml. ekomloven § 1-5, nr. 9 om offentlig elektronisk kommunikasjonstjeneste.

En person-til-person-kommunikasjonstjeneste er nummerbasert når den etablerer forbindelse til ett eller flere nummer i nasjonale eller internasjonale nummerplaner, eller muliggjør

kommunikasjon med ett eller flere nummer i nasjonale eller internasjonale nummerplaner.

Motstykket til definisjonen er de nummeruavhengige person-til-person-kommunikasjonstjenestene, jf. Ekomloven § 1-5, nr. 7. Eksempler på nummeruavhengige person-til-person-

kommunikasjonstjenester, som altså ikke er omfattet av reglene om entydig identifisering, er typisk WhatsApp, Facebook Messenger o.l.

NÅR KREVES ENTYDIG IDENTIFISERING:

Entydig identifisering skal sikres ved **inngåelse, endring eller opphør** av avtalen. Hensynet bak bestemmelsen om entydig identifisering tilsier at alle større handlinger knyttet til en sluttbrukers avtaleforhold og telefonnummer bør beskyttes ved krav om entydig identifisering.

Det klare utgangspunktet er at man ved **inngåelse** av avtale skal kjenne sin kunde og at slike avtaledisposisjoner må medfølge kundekontroll. Det å binde en fysisk eller juridisk person til en kontrakt kan ha store konsekvenser. En avtale om abonnement kan, særlig for store bedriftsabonnement, medføre store kostnader. Reglene om entydig identifisering medfører en viss brems i kjøpsprosessen slik at sluttbruker kan få tid til å områ seg. Det samme gjelder ved **opphør** av avtalen. Hensynet bak bestemmelsen tilsier at en sluttbruker ikke skal måtte tåle at en uvedkommende sier opp abonnementet deres. Telefonnummer er i dag så tett knyttet til vår person at det å miste det vil kunne medføre store vansker og ubehag. Kravet til entydig identifisering gjelder også ved portering av telefonnummer, det fremkommer av merknadene til ekomloven § 2-8.

Når det gjelder krav om entydig identifisering ved **endring** av abonnement er det i forskriften § 1-8, tredje ledd gjort en operasjonell begrensning i kravet. Fjerde ledd stadfester at endring i

abonnementstype og prisplan ikke krever entydig identifikasjon, med unntak av hemmelig nummer. Unntaket i § 1-8, fjerde ledd gjør at tilbyderne kan gjennomføre alminnelig kundesentervirksomhet over telefon uten at kravene om entydig identifisering fører til store praktiske utfordringer. Det vil naturlig nok være en grense mellom hva som utgjør en endring som tilsier at det i praksis inngås en ny avtale, og som derfor skal entydig identifiseres. Nkom anbefaler at det i de enkelte tilfellene foretas en konkret vurdering sett opp mot formålet med entydig identifisering og hensynene bak. Enkeltspørsmålene som er besvart i dette dokumentet avklarer en rekke av disse praktiske situasjonene.

Under følger relevante eksempelspørsmål:

Q: Vil salg av et nytt abonnement til nye eller eksisterende kunder kreve entydig identifisering når salget gjennomføres per telefon?

A: Alle salg krever entydig identifisering, uavhengig av salgsmetoden.

Q: Ved kredittsjekk av kunde, vil det være nødvendig at entydig identifisering er gjennomført før slik kontroll?

A: Det vil ikke være behov med entydig indentifisering før kredittsjekk. Bare ved oppstart, endring eller opphør av avtale.

Q: Ved salg av terminalutstyr som medfører binding av eksisterende abonnement, vil dette kreve entydig identifisering?

A: Salg av terminalutstyret krever ikke entydig identifisering i selg selv, spørsmålet er om tilførelsen av bindingstid på tjenesten krever entydig identifisering. Her kan det være tvilstilfeller, om det er snakk om endring av abonnementstype eller en de facto ny avtale. Når abonnementet endres fra uten bindingstid til med bindingstid mener Nkom det vil være behov for entydig identifisering.

Q: Hva er reglene der sluttbruker bestiller nytt SIM-kort eller ekstra tvilling-SIM?

A: Her kan det være tvilstilfeller, men faller tilbake til det klare utgangspunktet. Etablering av nye SIM-kort vurderes som endringer utover abonnementstype og prisplan. Der det gjøres en slik bestilling skal sluttbruker entydig identifiseres. Urettmessig etablering av tvilling-SIM er sårbarhet som de nye reglene er ment å adressere. Her vil man også konkret i det enkelte tilfelle måtte vurdere når en endring er så omfattende at det må ses som inngåelse av en ny avtale.

Q: Er en kunde nødt til å identifisere seg med elektronisk identifikasjon (f.eks. BankID) hver gang de skal gjennomføre en "handling" som krever entydig identifisering. Om kunden allerede er identifisert den dagen og denne fremdeles er gyldig, er det behov for ny identifisering?

A: Kunden er nødt til å identifisere seg med elektronisk identifikasjon hver gang de skal gjennomføre en handling som krever entydig identifisering dersom kontakten har vært avsluttet i mellomtiden.

Dette for å unngå misbruk av kundens identifisering. Dersom kunden gjennomfører flere «handling» i samme «samtale» med tilbyderer er det tilstrekkelig med identifisering en gang.

Q: Utløser endring av abonnement og/eller pris krav om entydig identifisering?

A: Nei, etter tilbakemelding fra bransjen i høringsrunden ble reglene i forskriften oppmykt slik at endring i prisplan og abonnementstype, med unntak av hemmelig nummer, ikke krever entydig identifisering.

Q: Kan vi fjerne sikkerhetstjenester eller sperrer uten entydig identifisering?

A: Nei, dette er endringer som er omfattet av ekomloven § 2-8 og ekomforskriften § 1-8 og krever entydig identifisering. Det er kun endringer i abonnementstype og prisplan som ikke er omfattet. Opphevelse av regionsperrer vil ha en klar sårbarhet mot svindel.

Q: Dersom en eksisterende kunde flytter og dermed melder inn ny adresse, må disse endringene følges av entydig identifisering?

A: Regelverket sier ikke noe konkret om endring av adresse. Reglene krever at kunden skal entydig identifiseres ved inngåelse og endring. Etter ekomloven § 2-9 skal tilbyder ha et register over sluttbrukere, herunder med adresse. For at det skal være noe realitet i dette registeret må det oppdateres når sluttbruker flytter. En endring av adresse omfattes ikke av unntaket i ekomforskriften § 1-8, fjerde ledd om abonnementstype og prisplan og må følgelig sikres ved entydig identifisering. En uønsket adresseendring kan også være et element i svindel.

Q: Dersom en portering kanselleres, må sluttbrukeren entydig identifiseres som ved alminnelig oppsigelse?

A: Nei, her vil kunden måtte være entydig identifisert ved nyinngåelse av avtale hos originalt avgivende tilbyder. Hensynet bak er følgelig oppfylt.

Q: Noen kunder ønsker å si opp abonnementet sitt uten at det porteres ut, må kunden entydig identifiseres?

A: Hensynet bak reglene om å entydig identifisere gjør seg også gjeldende ved opphør av avtalen. Reglene skal hindre at noen andre kan si opp telefonnummeret ditt uten din viten. Ved oppsigelse over telefon vil tilbyderer måtte informere sluttbruker om at entydig identifisering må gjennomføres enten ved bruk av elektronisk ID eller dokumentkontroll – det samme gjelder henvendelser som kommer via e-post. Regelverket gjør her ingen unntak.

Q: I tilfeller der eierskifte skal gjennomføres, er det tilstrekkelig å kun entydig verifisere ny eier av abonnementet eller krevers det at også tidligere eier entydig identifiseres.

A: Her vil det være snakk om inngåelse og opphør av avtale og begge parter må entydig identifiseres for å forhindre urettmessig «kapring» av telefonnummer.

HVEM SKAL ENTYDIG IDENTIFISERES?

Ekomloven § 2-8 krever at tilbyder skal sikre at **sluttbrukeren** er entydig identifisert.

Sluttbruker er definert i ekomloven § 1-5 nr. 26 som en bruker som inngår avtale om, men som ikke tilbyr andre, tilgang til offentlige elektroniske kommunikasjonsnett eller offentlige elektroniske kommunikasjonstjenester. Definisjonen er vid og omfatter både fysiske og juridiske personer.

Sluttbruker er avtaleparten når det inngås avtale om nummerbaserte person-til-person-kommunikasjonstjenester. Dette kan være en fysisk person som skal entydig identifiseres i tråd med ekomforskriften § 1-8. Sluttbruker kan også være et foretaksom inngår avtale om bedriftsabonnement med flere telefonnummer for sine ansatte. I et slikt tilfelle vil sluttbrukeren, avtaleparten, være foretaket, selv om det er de enkelte ansatte som bruker numrene. Virksomheten skal da entydig identifiseres som en juridisk person i tråd med ekomforskriften § 1-9. De ulike reglene for entydig identifisering av henholdsvis fysisk person etter ekomforskriften § 1-8 og juridisk person etter ekomforskriften § 1-9 vil bli mer uttrykkelig gjennomgått senere i veiledningen.

Det er altså ikke nødvendigvis sammenfall mellom hvem som er sluttbruker og hvem som er faktisk bruker av telefonnummeret. Slik reglene er utformet er det ikke krav om å entydig identifisere alle faktiske brukere, kun sluttbruker.

Dette er en aktuell problemstilling også der mindreårige er brukere av telefonnummer, mens avtalen er inngått av en foresatt – som sluttbruker. Her vil den foresatte måtte entydig identifiseres. Ekomregelverket inneholder en bestemmelse i § 2-9 om kunderegister, som gjelder sluttbrukere. Likevel er det slik at tilbydere har krav om å sperre for enkelte typer innhold for brukere under visse aldersgrenser, dette tilsier at tilbydere fører en oversikt over hvem som er faktiske brukere uten at ekomloven har direkte krav om det. Krav om å registrere alder dersom tilbyder har et register over faktiske brukere fremkommer av ekomforskriften § 1-10.

Q: Vi har en kunde i bedriftsmarkedet som skal inngå avtale om flere telefonnummer til sine ansatte. Kreves det entydig identifisering av selskapet eller av de enkelte ansatte?

A: Kravet til entydig identifisering gjelder sluttbruker, som avtalepart. Dere skal derfor entydig identifisere selskapet i tråd med bestemmelsen i ekomforskriften § 1-9.

DOKUMENTASJON AV IDENTITETSKONTROLL

Nkom minner også om at tilbyder har plikt etter ekomloven § 2-8 til å dokumentere identitetskontrollen, herunder hvilken type identitetsbevis som er benyttet og dets kontrollnummer. Dette gjelder for entydig identifisering etter både ekomforskriften §§ 1-8 og 1-9.

Q: Når det gjelder dokumentasjon av identitetskontrollen, er det nødvendig å lagre eksterne referanser fra elektronisk kommunikasjon, f.eks. BankID? Hvor lenge må dokumentasjonen lagres?

A: Det er nødvendig å ha dokumentasjon som kan etterprøves i revisjon/ kontroll på et senere tidspunkt. Slike eksterne referanser skal derfor lagres. Når det gjelder lagring av dokumentasjonen henviser Nkom til at dette er et krav som kommer frem av ekomloven § 2-8 og skal derfor lagres så lenge det er nødvendig for å oppnå formålet, typisk vil dette være avtaleforholdets varighet. Vi henviser videre til Datatilsynet for de praktiske reglene omkring lagring.

Q: Hvilke krav til dokumentasjon av identifikasjonskontrollen kreves når kunde er verifisert gjennom fysisk legitimasjon?

A: For å kunne dokumentere identitetskontrollen er det nødvendig å registrere hvilken type identitetsbevis som ble brukt, kontrollnummer i tillegg til dato og tidspunkt.

Entydig identifisering når sluttbruker er en fysisk person

Ekomforskriften § 1-8 inneholder regler om metoden for entydig identifisering av sluttbruker som er en fysisk person.

I hovedsak skal kundekontrollen etter ekomforskriften § 1-8 gjennomføres på en av to måter:

- a) Fremleggelse av originalt og gyldig identifikasjonsbevis
- b) Bruk av elektronisk identifikasjon på et visst sikkerhetsnivå.

Etter bokstav a) skal tilbydereren kontrollere at identitetsbeviset og personen som ønsker å inngå, endre eller avslutte avtalen er den samme og den vedkommende utgir seg for. Det er tilbyders ansvar å sørge for at identitetsbeviset blir tilstrekkelig kontrollert og verifisert. Tilbyder må vurdere om identitetsbeviset er forfalsket, om det er ansikts- og bildeklighet og om andre opplysninger stemmer overens med vedkommende som identifiseres.

Identitetsbevis er etter bestemmelsen, for personer med norsk fødselsnummer eller D-nummer

- pass, nasjonalt ID-kort eller norsk førerkort.

For personer uten norsk fødselsnummer eller D-nummer skal identitetsbeviset ha opplysninger om

- fødselsdato, fødested, statsborgerskap og fotografi.

At identitetsbeviset er originalt og gyldig betyr at identitetsbeviset ikke kan være utgått på dato ved fremleggelsen og at det ikke er en kopi som presenteres.

Likestilt med kontroll av identitetsbevis etter bokstav a) er bruk av elektronisk identifikasjon etter bokstav b). Eksempel på dette er BankID, som er svært utbredt i Norge.

BRUK AV DIGITALE LØSNINGER ETTER BOKSTAV A)

Nkom har etter en vurdering av ordlyd, forarbeider og hensyn bak reglene kommet til at ekomforskriften § 1-8, første ledd, bokstav a) ikke utelukker identitetskontroll uten personlig fremmøte. Nkom legger vekt på følgende:

En alminnelig tolkning av ordlyden «fremleggelse» utelukker ikke at dette kan gjøres digitalt.

Nkom mener at ordlydsendringen i etterkant av 2019-høringen og fjerning av henvisningen til «personlig fremmøte» kan tas til inntekt for en forståelse av regelverket som mer teknologinøytral og fremtidsrettet. Videre fremstår det for Nkom som tydelig at en trygg digital løsning for identifikasjonsverifisering ikke var vurdert i forbindelse med høringen i 2019.

Bestemmelsene i ekomforskriften er utformet i likhet med tilsvarende bestemmelser i hvitvaskingsforskriften. Hvitvaskingsregelverket åpner for at identifikasjonskontroll kan skje uten personlig fremmøte, uten at dette elementet fremkommer uttrykkelig i ekomregelverkets versjon av regelsettet. Nkom finner det lite rimelig at ekomregelverkets regler om entydig identifisering skal være strengere enn tilsvarende regler i hvitvaskingsregelverket.

Vi legger også vekt på uttalelsene fra Stortingets Transport- og kommunikasjonskomite i innstillingen til ny ekomlov hvor et flertall legger vekt på at ny teknologi kan tas i bruk dersom det vurderes som sikkert og formålstjenlig.

Nkom har på denne bakgrunn kommet til at ekomforskriften § 1-8 første ledd bokstav a) ikke utelukker at entydig identifisering ved fremleggelse av identifikasjonsdokument kan skje uten personlig fremmøte, for eksempel ved digital løsning. Dette betyr ikke at hovedregelen og utgangspunktet fremdeles er fysisk fremleggelse. Dette betyr heller ikke at alle løsninger vil være tilfredsstillende. Nkom mener at Finanstilsynets veileder til hvitvaskingsregelverket om godkjente fremgangsmåter for entydig identifisering uten personlig oppmøte har overføringsverdi og bør vektlegges. Den skisserte løsningen Nkom nå presenterer er bygd opp på tilsvarende måte som Finanstilsynets veileder. Det vises særlig til Finanstilsynets vurdering av hva som anses som tilfredsstillende digitale løsninger.

Det betyr for det første at det er opp til tilbyder å vurdere om løsningens omfang og art er tilstrekkelig for å utgjøre en like sikker eller sikrere identifisering enn personlig fremmøte. Nkom viser til at tilbyder må kunne godtgjøre hvilken metode som er benyttet, hvordan løsningen er tilfredsstillende og at slik vurdering faktisk er foretatt.

For digitale løsninger må det kreves at det gjøres ytterligere tiltak for å kontrollere at legitimasjonen tilhører vedkommende kunde. Det kreves altså noe mer enn ved personlig, fysisk fremmøte. Løsninger kan for eksempel bruke biometri fra legitimasjonsdokumentet og må ha funksjonalitet som kontrollerer ektheten og gyldigheten av legitimasjonsdokumentet

I likhet med hvitvaskingsregelverket vil Nkom kreve at den tekniske løsningen, som et minimum, må:

- etterleve de generelle kravene til fremleggelse og registrering av identitetsbeviset, blant annet om hvilke legitimasjonsbevis som er akseptable og krav til dokumentasjon
- gjennomføre «ytterligere tiltak» ved å kontrollere legitimasjonsdokumentet
- kontrollere at det er kunden som initierer identifiseringen, for eksempel ved biometrisk kontroll eller tilsvarende sikker løsning

Biometrisk kontroll kan f.eks. gjøres ved filming av personen ved hjelp av håndsettet. Nkom understreker at det er tilbyders ansvar å i første omgang vurdere om løsningene er like sikre eller sikrere enn legitimasjonskontroll ved personlig fremmøte.

Tilbydere må ha et bevisst forhold til risikoen ved identitetskontroll. Dersom det er tvil, må enda flere tiltak settes i verk, og undersøkelsene må tilpasses risikoen. Dette kan inkludere å kontrollere informasjonen mot andre kilder, som offentlige registre. Når man bruker offentlige registre og andre informasjonstjenester, må tilbyderne vurdere hvor pålitelige disse registrene og informasjonen er. Informasjonen i norske offentlige registre kan vanligvis anses som pålitelig.

PERSONER SOM HANDLER ELLER DISPONERER PÅ VEGNE AV SLUTTBRUKER

Ekomforskriften inneholder ikke konkrete regler om hvordan entydig identifisering skal håndteres der sluttbruker representeres av andre, for eksempel ved fullmakt eller vergemål.

Nkom finner at det for slike tilfeller må kreves entydig identifisering av personen som handler på vegne av sluttbrukeren, i kombinasjon med en bekreftelse av retten til å handle på vegne av sluttbrukeren. Dette betyr en alminnelig identitetskontroll av personen som er gitt fullmakt, samt en sjekk av disse opplysningene opp mot bevis på fullmakt, som for eksempel skriftlig fullmakt fra sluttbruker, vergemålsoppnevning eller skifteattest.

KRAV OM OPPLYSNING OM FØDESTED

Nkom har vurdert ekomforskriften § 1-8 første ledd bokstav a), andre delsetning og kravet om at gyldig identifikasjonsbevis for personer uten norsk fødselsnummer eller D-nummer skal, blant annet, inneholde informasjon om «fødested».

Som nevnt tidligere er flere av reglene om entydig identifisering inspirert av hvitvaskingsregelverket. Også for dette temaet finner vi en tilsvarende formulering i hvitvaskingsforskriften § 4-3, andre ledd. Den eneste forskjellen er at bestemmelsen i hvitvaskingsforskriften også krever opplysninger om «kjønn».

Finanstilsynets veileder til hvitvaskingsloven er derimot mer pragmatisk enn ekomregelverket fremstår i dag. I veilederens punkt 4.3.1.9 om personer som ikke har gyldig legitimasjon – utenlandske statsborgere, anser Finanstilsynet at hvitvaskingsregelverket åpner for at visse sårbare kundegrupper uten legitimasjon som oppfyller alle kravene kan være tilstrekkelig identifisert ved annen kontroll.

Nkom finner at ekomregelverket ikke bør være unødvendig rigid på området og foreslår en linje lik den Finanstilsynet legger for hvitvaskingsregelverket. Dette betyr konkret en mer pragmatisk tilnærming til legitimasjon i konkrete enkeltsaker for særlige sårbare grupper uten norsk fødselsnummer eller D-nummer. Når det kommer til utenlandske statsborgere uten fullgode identifikasjonsbevis i

ekomforskriften forstand kan dette avhjelpes ved ytterligere kontroll av identiteten gjennom andre kilder.

Nkom understreker at dette ikke skal forstås som hovedregelen, men skal utgjøre en snever unntaksvis tilnærming for sårbare grupper for å sikre deres tilgang til grunnleggende norske telefonitjenester. Tilbydere må i de konkrete tilfeller hvor forskriftens krav til «fødested» avvikes kunne dokumentere vurdering og hvilke alternative tiltak som ble iverksatt. Dette innebærer også at slike situasjoner må defineres og beskrives i interne retningslinjer.

Nkom finner at en slik løsning er innenfor ekomregelverkets handlingsrom. Likevel vil vi vurdere å anbefale departementet å klargjøre dette i en kommende revisjon av det nye regelverket.

DIGITALT FØRERKORT

En praktisk problemstilling er hvorvidt digitalt førerkort skal anses som gyldig legitimasjon etter ekomforskriften § 1-8, første ledd bokstav a). Ordlyden i bestemmelsen henviser konkret til «norsk førerkort». Nkom mener det er gode grunner for å godta digitale førerkort som gyldig legitimasjon ved entydig identifisering etter ekomregelverket. Det digitale førerkortet inneholder den samme informasjonen som det fysiske. Sluttbruker må også identifisere seg for å få tilgang til eget digitalt førerkort. Nkom viser også til at Helsedirektoratet har kommet til at digitale førerkort kan brukes som gyldig legitimasjon på apotekene. Digitalt førerkort er også gyldig legitimasjon ved valg. Vi mener det er gode grunner for at entydig identifisering etter ekomregelverket skal følge samme praksis.

Spørsmål og svar om entydig identifisering av sluttbruker som er en fysisk person:

Q: Må vi kreve entydig identifisering for kunder som ikke har elektronisk identifikasjon grunnet alder eller digital kompetanse?

A: Når det gjelder entydig identifisering er Nkom klar over utfordringene slike regler utgjør for de digitalt sårbare. En balansert tilnærming der hensynene til sikkerhet og praktiske løsninger får plass er etter Nkoms syn rette veien. Det er derimot ikke slik at eldre eller digitalt sårbare er mindre rammet av svindel eller lignende. Nkom er derfor skeptisk til en generell lettelse av reglene om entydig identifisering, som nettopp skal sikre at rett person foretar handlingene. Bruk av digitale hjelpere og fullmakt er eksempler på avhjelpende tiltak som er beskrevet tidligere i veiledningen og som kan benyttes. Det arbeides kontinuerlig med digital inkludering. Entydig identifisering og bruk av elektronisk identifikasjon er stadig tema i slike fora.

Q: Kan dere gi eksempler på hva som vil utgjøre gyldig legitimasjon?

A: Eksempler på gyldig legitimasjon etter reglene om entydig identifisering er:

- norsk og utenlandsk pass (ikke nødpass)

- Fødselsattest der sluttbruker er mindreårig¹
- norsk førerkort, inkludert digitalt førerkort
- norsk nasjonalt ID-kort
- nasjonalt ID-kort utstedt av et annet EØS-land
- norsk utlendingspass (grått pass)
- norsk reisebevis for flyktninger (blått pass)

¹ Barnets foresatte, verger eller andre som disponerer eller handler på vegne av barnet skal identifiseres med gyldig legitimasjon

Entydig identifisering når sluttbruker er en juridisk person

Ekomforskriften § 1-9 inneholder regler om metoden for entydig identifisering av sluttbruker som er et foretak mv.

Som nevnt over er virkeområdet for reglene om entydig identifisering vidt, og gjelder alle sluttbrukere. Sluttbruker kan også være juridiske personer. Ekomforskriften § 1-9 gjelder altså for tilfeller der et foretak eller juridisk person er avtalepart for en nummerbasert person-til-person-kommunikasjonstjeneste. Bestemmelsen er derfor særlig relevant for bedriftsmarkedet.

Entydig identifisering av et foretak skal skje ved at det innhentes relevante opplysninger om foretaket:

- Foretaksnavn
- Organisasjonsform
- Organisasjonsnummer
- Adresse
- Navn på daglig leder og styremedlemmer, eller personer i tilsvarende stilling

Disse opplysningene skal så bekreftes ved oppslag mot eller utskrift fra offentlig register eller firmaattest, som ikke er eldre enn tre måneder, jf. § 1-9, fjerde ledd. Registerutskrift inkluderer elektronisk utskrift i form av skjermbilde.

Dersom en virksomhet ikke er registrert i foretaksregisteret eller enhetsregisteret så kan en gjøre oppslag og utskrift fra andre offentlige registre. I praksis vil dette typisk gjelde utenlandske foretak. En må i slike tilfeller ha en risikobasert tilnærming og oppslag mot utenlandsk register kan ikke være det eneste tiltaket for å bekrefte opplysninger om en juridisk person.

Der man avviker fra identifiseringen må en foreta ekstra tiltak basert på risikovurdering der tilbyderne må kunne dokumentere hvilke risikomomenter de har lagt til grunn. Blant annet kan en se på virksomhetens art og omfang, geografiske forhold og kunder og kundegrupper etc. Det er tilbyderen som har ansvar for å gjennomføre en rimelighetsvurdering på om opplysninger og dokumentasjon fra kunden fremstår som korrekte og troverdige.

Videre skal personer som handler på vegne av den juridiske personen identifiseres i tråd med metoden i ekomforskriften § 1-8. At en person har rett til å handle på vegne av foretaket skal kontrolleres og bekreftes, jf. § 1-9, fjerde ledd.

Etter § 1-9, tredje ledd kan elektronisk segl også benyttes for entydig identifisering av foretaket. Vi går ikke nærmere inn på dette alternativet her.

I praksis så skal tilbyder ved inngåelse, endring eller opphør av avtale med et foretak samle inn en rekke opplysninger om selskapet. Disse opplysningene skal så verifiseres. Neste steg er å sikre at personen som handler på vegne av selskapet har de nødvendige rettigheter til å disponere. Tilbyder må derfor kontrollere slik disposisjons- eller signaturrett opp mot entydig identifisert fysisk person.

Nkom understreker, for inngåelse av avtale, at reglene om entydig identifisering kommer til anvendelse på tidspunktet for avtaleinngåelse. Regelverket åpner ikke for at identifisering kan skje i etterkant av avtaleinngåelsen.

Spørsmål og svar om entydig identifisering av sluttbruker som er en juridisk person:

Q: Vi bruker gjerne telefon for salg og inngåelse av abonnement i bedriftssegmentet. Er det virkelig nødvendig å både samle inn opplysninger om foretaket og entydig identifisere personen vi snakker med?

A: Ja, reglene om entydig identifisering for foretak er klare og strenge og det oppstilles ingen unntak for kontakt over telefon eller ved nysalg. Nkom antar at det for flere tilbydere vil være nødvendig å endre på rutiner for salg slik at disse inkluderer steg for entydig identifisering og verifisering av opplysninger og fullmakter. Det har tidligere vært en risiko for at avtale inngås med representant for selskapet som ikke har fullmakter til å binde foretaket til slike avtaler, ved entydig identifisering av person og kontroll av fullmakt vil dette avhjelpes

Q: Dersom det er et selskap under stiftelse eller et selskap uten organisasjonsnummer, hvordan kan vi entydig identifisere de?

A: I disse tilfellene må det innhentes informasjon som bekrefter at den juridiske personen eksisterer. Den fysiske personen må videre gi en skriftlig erklæring på at de innhentede opplysningene om den juridiske personen er korrekte.

Q: Hva gjør vi dersom kunden ikke kan eller vil fremskaffe informasjonen eller dokumentasjonen vi etterspør?

A: Dersom kunden ikke vil eller kan fremskaffe forespurt informasjon så kan ikke tilbyder gjennomføre en sikker entydig identifisering. Det vil innebære at inngåelse, endring eller opphør av avtale ikke kan gjennomføres.