SAKSFRAMLEGG

Forum: Skate Møtedato: 31.05.2017

Sak 09-2017 Identitetsforvaltning
Beslutningssak

Historikk/bakgrunn

I årsplan for Skate 2017 er identitetsforvaltning satt opp som sak til Skate-møtet 31. mai. En arbeidsgruppe med deltakere fra Difi, SKD, UDI og POD har utarbeidet en presentasjon og et saksframlegg. Arbeidet har vært styrt av Skates arbeidsutvalg (AU) gjennom møter den 29.3, 20.4 og 10.5. Det er AU som fremmer saken for Skate.

Forslag til beslutning:

Skate ber KMD ta opp med JD og ev. andre relevante departementer

1. at forvaltningen og relevante private aktører ved behov **må kunne** gjennomføre **sterk identitetskontroll** av personer som er bosatt i Norge eller som skal ha større økonomiske ytelser fra det offentlige. Dette innebærer
   - Alle i ovennevnte målgruppe må kunne få et **sterkt identitetsbevis**, enten nasjonalt id-kort eller et annet. Beviset må kunne brukes for å få e-ID.
   - Aktørene må gjøres i stand til å **avdekke falske identitetsbevis og bruk av andres identitetsbevis**, eksempelvis gjennom en taps- og verifikasjonstjeneste med fingeravtrykkssjekk (match-on-card)
   - Relevante aktører må få lovhjemmel til å gjennomføre sterk identitetskontroll, alternativt at rettslige begrensninger for dette må fjernes

2. at man vurderer om aktører bør få **plikt** til å gjennomføre identitetskontroll, for å redusere misbrukstilfeller hos andre aktører

3. at **biometri må kunne** registreres i ett eller flere sentrale registre, på en slik måte at gode biometrisøk er mulig (en-til-mange-søk). Dette vil redusere faren for registrering av fiktive identiteter og danne grunnlag for at personen registreres med status «unik» i folkeregisteret.
   - Det må vurderes nærmere hvilken type biometri som er egnet, og nærmere innretning av registeret og søket – herunder vurdering av risikoreduserende effekt og nødvendig ressursinnsats for manuell håndtering av tvilstilfeller og maskinelle feilvurderinger.

4. at punktene over sees i sammenheng og at de relevante departementene samlet og koordinert er tydelige i kommunikasjonene om hva som kommer på plass når

For å sikre koordinering av identitetsforvaltningsarbeidet anbefaler Skate at det etableres en **koordineringsgruppe** på direktoratsnivå. SKD bes ta initiativ til å opprette en slik gruppe og foreslå forankring.

Presentasjon av saken

Begreper

I dette arbeidet bruker vi begrepet **sterkt identitetsbevis** om

- et fysisk identitetsbevis som er egnet for en sterk identitetskontroll og som dessuten gir knytning til en norsk identifikator (f-/d-nummer).

En **sterk identitetskontroll** innebærer effektiv kontroll av

- at identitetsbeviset er ekte (i praksis forutsetter dette chip i kortet),
- at det er innehaveren, og ikke noen andre, som benytter identitetsbeviset (i praksis forutsetter dette sjekk av at brukerens biometri samsvarer med innehaverens biometri)

Dessuten må identitetsbeviset være basert på en sikker utstedelsesprosess.

Sterk identitetskontroll kan benyttes ifbm andre tjenester fra forvaltning og privat sektor, inkl. til å utstede e-ID.

0-alternativet – dagens situasjon

Mangelfull utbredelse av sterke identitetsbevis og sterk identitetskontroll

Norske pass og det kommende nasjonale id-kortet oppfyller ovennevnte krav til å være et sterkt identitetsbevis. Det er uklart hvilken personkrets, ut over norske statsborgere, som vil kunne få utstedt nasjonalt id-kort. Det er således i utgangspunktet mange som verken har eller kan skaffe seg et sterkt identitetsbevis.

Sterk identitetskontroll utføres i dag bare av grensekontrollmyndighetene.

Risikobaserte krav

Det er opp til den enkelte offentlige virksomhet (og andre risikoeiere) å velge nivå på identitetskontrollen de har behov for – veie effektivitetstapet ved økt kontroll opp mot gevinsten av redusert misbruk. Misbruk av elektroniske identitetsbevis i ID-porten må antas å være minimalt, basert på tilbakemeldinger til Difi fra innbyggere og tjenesteeiere. Løsningene er imidlertid ikke sikrere enn utstedelsesprosessen. Eventuell sviktende identitetskontroll ved utstedelse vil imidlertid følge med e-ID-en, jf. utfordringene nevnt over.

For bruk av elektroniske identitetsbevis (e-ID) finnes veiledning i rammeverk for autentisering og uavviselighet.

Det kan være uklart i hvilken grad forvaltningen kan kreve personer gjennomgår identitetskontroll, eller at personer er registrert som «unik» i folkeregisteret. Utgangspunktet er at forvaltningen må sikre at saksbehandlingen er forsvarlig, krav til identitetskontroll må ha tilstrekkelig hjemmel (jf. legalitetsprinsippet) og ev. forskjellsbehandling må være saklig begrunnet. For elektronisk kommunikasjon finnes hjemmel til å stille krav om identitetskontroll (bekreftelse på identitet/fullmakter) eller bruk av sikkerhetstjenester i eforvaltningsforskriften § 4 annet ledd.

Misbruk

Vi kjenner ikke til gode anslag for hvor stor del av kriminaliteten som er knyttet til bruk av uriktig identitet. Det er imidlertid på det rene at det i dagens identitetsforvaltning finnes hull her som utnyttes av kriminelle.

En rapport fra 2013[1] anslo at trygdebedragerier årlig beløp seg til om lag 6 milliarder kroner. For svart arbeid finnes anslag på unndragelser i størrelsesorden 6-10 pst av BNP. Bruk av fiktiv eller falsk identitet inngår i en andel av sakene, og representerer en særlig utfordring ifbm. å få stilt den kriminelle for retten (iretteføring) og for innkreving av tilbakebetalingskrav. Dessuten er identitetsrelatert svindel en forutsetning for noen av misbrukstypene. Beløpene er til dels betydelige.

Vi vil her gi tre eksempler på typer identitetsrelatert svindel.

1. Et barn blir født – flere ganger. I perioden 2004-2012 ble 74 fødselsnummer slettet pga bedrageri i fødselsmeldingen. Det nyfødte barnet ble av flere kvinner utgitt for å være født hjemme, og det ble derfor tildelt flere fødselsnummer. Hvert barn gav rett til ytelser fra NAV. Hovedkvinnen i saken ble

[1] Trygdesvindel i Norge, rapport 2013-05 fra Proba samfunnsanalyse, for Arbeidsdepartementet, januar 2013.

pålagt å tilbakebetale ca 8 millioner kroner; bl.a. var en av hennes voksne døtre uriktig oppført i folkeregisteret med 8 barn.

2. Registrering av flere identiteter i folkeregisteret ved hjelp av falske identitetsdokumenter. En snekker fra Armenia fikk ved hjelp av falske identitetsbevis registrert 7 EØS-borger-identiteter i folkeregisteret, og med to av dem svindlet han NAV for til sammen ½ million kroner.[2]

3. Arbeidsgivere lyver om identiteten til ansatte. Fra 2014 har Skatteetaten avdekket et nytt misbruksmønster: Identiteten til EØS-borgere gjenbrukes/misbrukes av arbeidsgivere, både ved at denne identiteten brukes for å innrapportere lønn m.v. på andre ansatte (eks. illegale innvandrere), og dels også for andre typer kriminalitet. Det utstedes også identitetsbevis fra arbeidsgiver med EØS-borgerens d-nummer/fødselsnummer og øvrige personalia, men med en annens bilde. I noen tilfeller er EØS-borgeren med på svindelen, dansk politi har avdekket vederlag i størrelsesorden 30 000 DKR for slikt identitetsutleie.

Ovennevnte tilfeller representerer noe av bredden i utfordringsbildet. Et fellestrekk er her at det er brukt falske identitetsbevis eller at personer har opptrådt som en annen (men uten at identitetsbevis er krevd fremlagt).

Noen tiltak er iverksatt eller i kjømda

Det er iverksatt tiltak for å hindre at en fødsel registreres flere ganger (krav om DNA mor-barn ifbm. hjemmefødsel). Folkeregisterloven er også vedtatt endret slik at det kan registreres opplysninger om identitetsgrunnlag (unik, kontrollert). Passloven er foreslått endret for å tillate biometriske en-til-mange-søk, som kan understøtte registrering av feltet «unik».[3] Registeret inneholder imidlertid bare ansiktsbilde, ikke fingeravtrykk.

Nasjonalt ID-senter utarbeider en veileder i krav til fysisk identitetskontroll. Det er usikkert når denne ferdigstilles. Den vil kunne hjelpe virksomheter med å stille egnede krav til identitetskontrollen.

Det er imidlertid fortsatt utfordringer mht. å hindre at personer kan registreres flere ganger i folkeregisteret, og å hindre identitetsmisbruk ved hjelp av falske identitetsbevis eller ved at beviset brukes av personer som ligner på rette vedkommende (såkalt imposter-bruk).

En taps- og verifikasjonstjeneste for identitetsbevis er besluttet etablert, men vil i utgangspunktet kun dekke kontroll av ekthet og om beviset er meldt tapt. Når tjenesten etableres er usikkert. Vern mot imposter-bruk[4] er pt. ikke inkludert.

Nasjonale identitetskort vil bli utstedt til norske statsborgere fra 1.4.2018. Utstedelse til andre er planlagt fra årsskiftet 2018/2019, men det er ikke avklart hvem som skal kunne få.

Forslag til strategisk beslutning

Vi anbefaler at det legges bedre til rette for **sterk identitetskontroll.**

- Sterke identitetsbevis må gjøres mer tilgjengelig. Alle relevante grupper må kunne få nasjonalt ID-kort eller annet sterkt id-bevis.
- Sterk identitetskontroll må gjøres mer tilgjengelig
    - Hindre bruk av falske identitetsbevis. Taps- og verifikasjonstjeneste må etableres, og gjøres tilgjengelig for aktuelle aktører
    - Hindre imposter-bruk av ekte identitetsbevis. En tjeneste for identitetskontroll (samsvar mellom bruker og biometrien i id-beviset) må etableres.

---

[2] Tilståelsesdom Oslo tingrett, omtalt i http://www.aftenposten.no/norge/Snekker-med-syv-falske-navn-svindlet-Nav-for-over-en-halv-million-102153b.html

[3] Høring med frist 17.2.2017. Justisdepartementets høringsnotat pkt. 5.2.2 og 5.2.4 omhandler knytning til nasjonalt id-kort og folkeregisteret.

[4] Kontroll av at bruker og innehavers biometri stemmer tilstrekkelig overens, såkalt «match-on-card», en-til-en-sammenligning.

Vi anbefaler at det legges bedre til rette for å redusere muligheten for **fiktive identiteter i folkeregisteret**.

- Det må etableres biometriregister som støtter gode en-til-mange-søk, som gir grunnlag for status «unik». Det må vurderes nærmere hvilken type biometri som er egnet, og nærmere innretning av registeret og søket – herunder vurdering av risikoreduserende effekt og nødvendig ressursinnsats for manuell håndtering av tvilstilfeller og maskinelle feilvurderinger. Se vedlegg.

Identitetsforvaltningsarbeidet har mange aktører og må koordineres bedre.

Restrisiko

Hvis ovennevnte tiltak gjennomføres vil forvaltningen stå vesentlig bedre rustet til å hindre misbruk av identiteter, både fiktiv identitet og identitetskrenkelse.

Det vil imidlertid fortsatt være en restrisiko knyttet til utlån eller utleie av identitet, i alle fall for elektronisk forvaltning (e-ID er lett å låne ut). Dessuten vil muligheten til å gjennomføre sterk identitetskontroll ikke nødvendigvis føre til at viljen til å gjennomføre slik kontroll øker. I situasjoner hvor aktuell kontrollaktør (f.eks. arbeidsgiver) har svak interesse i å gjennomføre en sterk identitetskontroll, må andre tiltak vurderes, f.eks. kontroll fra tredjepart (eks. arbeidstilsynet) eller skjerpede sanksjoner (erstatning, straff) mot sviktende kontroll.

Saken vil bli framlagt av Skates arbeidsutvalg /Skatesekretariatet og arbeidsgruppen
Saksframlegget er utarbeidet av Skates arbeidsutvalg og arbeidsgruppen fra Difi, SKD, UDI og POD

Oslo, 15.05.2017

1 vedlegg

Vedlegg

Kort om biometri

Biometriske sikkerhetsløsninger baserer seg på maskinell avlesing og sammenligning av personers fysiologiske karakteristika. Ettersom to avlesninger aldri er identiske, heller ikke for samme person, må gjenkjenningsløsningene baseres på at en passende avveining mellom nivået for feilaktige gjenkjenninger (at personen gjenkjennes som en annen)[5] og feilaktige avvisninger (at personen ikke gjenkjennes, selv om han finnes i registeret)[6].

Ved oppsett av systemet må man velge hvor mye to avlesninger skal ligne på hverandre. Settes lista for høyt, vil man ofte oppleve feilaktige avvisninger (Pål gjenkjennes ikke, selv om han finnes i registeret). Settes den lavt, vil man ofte få feilaktige gjenkjenning (Per gjenkjennes som Pål).

Feilratene er lavere for fingeravtrykk enn for ansiktsbiometri. Bruk av flere typer biometri i kombinasjon gir lavere feilrater.

I dag gir gode system basert på ansiktsbiometri feilaktige avvisninger for i underkant av 5%, når det aksepteres feilaktige gjenkjenninger på ca 10%.[7]

Til sammenligning er feilratene vesentlig lavere i et system basert på fingeravtrykk. Gode systemer kan ha feilaktige avvisninger for 0,1% (1:1000), når det aksepteres feilaktige gjenkjenninger på omkring 0,05% (1:2000).[8]

Merk at oppgitte feilrater baserer seg på helautomatisk gjenkjenning og nåværende teknologi. Det kan legges opp til manuelle rutiner som gir bedre resultater, eks. at man krever ny avlesning av biometri i tvilstilfeller, eller at øvrige egenskaper ved personen sammenlignes med tidligere registreringer (alder, kjønn, høyde, nasjonalitet) m.v.

Det er ikke kjent hvordan et optimalt regime bør være mht. type biometri, avveining mellom feilaktige gjenkjenninger og avvisninger, kompenserende tiltak, ei heller hvilken ressursbruk et slikt regime forutsetter og hvilken risikoreduksjon det vil gi. Slike analyser må ligge til grunn for valg av regime for bruk av biometri for å redusere faren for fiktive identiteter i folkeregisteret.

---

[5] Også kalt falske positive
[6] Også kalt falske negative
[7] Figur 6 for beste algoritme E30C i NIST-rapport 8009 av mai 2014 «Face Recognition Vendor Test (FRVT)»; ved FPIR på 0,1 (=10%) er beste FNIR på ca 0,04 (=4%); liknende resultater fremgår av NID-senterets rapport s 13 - https://www.nidsenter.no/globalassets/vedlegg/nid-rapporter/face-it---uten-iso-standarder.pdf
[8] Figur 83, s. 97 i NIST 8034 Fingerprint Vendor Technology Evaluation (FpVTE 2012) av januar 2015, leverandør I, ti fingre.