Oslo, 22 August, 2022

Viser til høring om "utkast for ny strategi for eID i offentlig sektor".

Mobai er en spin-off fra Norwegian Biometrics Laboratory ved informasjonssikkerhetsmiljøet ved NTNU og gir følgende innspill til høringen:

Kap 2 og Kap 3:

Som leverandør av teknologi til eID-aktører tilslutter vi oss situasjonsbeskrivelse hvor eID funger utmerket i en rekke situasjoner, og at enkelte grupper er begrenset av manglede mulighet til å bruke eID eller manglende evne. Dagens eIDer er vanskelig å bruke for særlig eldre, og enkelte brukergrupper blir stående utenfor uten mulighet til å bruke eID (eks: utenlandske brukere). (Primært kommentar til 2.5 og 3.2)

Re-etablering av tillitt ved tap av "credentials" er en utfordring i dagens verdikjede, hvor man i mange tilfeller ringer en support-telefon og besvarer et sett med kontrollspørsmål for å få tilgang til eID. Dette er typisk brukere med mindre teknisk kompetanse, men også fordi varierende bruk av eID kan medføre situasjoner hos også digitalt kompetente brukere hvor de har mistet tilgang (mistet kodebrikke, ikke brukt slik at løsning er deaktivert noe som kan være vanlig ved bankbytte, etc). Her vil økt bruk av biometri gi en mulighet for å etablere en sikker kommunikasjon til en bruker som har mistet øvrige credentials. Når en bruker først står der midlertidig uten en eID, så bør det også være enkelt å få tilbake sin tilgang uten fysisk oppmøte eller venting på aktiveringskode/tokens per post f.eks ved at et ID-dokument og ansikt sammenlignes i en selvbetjent løsning. (Primært kommentar til 2.5 og 3.2)

Dagens europeiske regelverk åpner for bruk av digital ID-kontroll, men det er ikke praksis i utstedelse av eID i Norge i dag. Næringen er avhengig av at nasjonale myndigheter setter klare føringer og rammeverk for hvordan løsninger tilfredsstiller kravene til bruk i utstedelse av eID. I et land med store geografiske avstander bør Norske myndigheter være et foregangsland for trygg digital ID-kontroll(Primært kommentar til 2.5 og 3.2)

Dagens fysiske ID-kontroll ifbm utstedelse av eID er sårbar, hvor det er stor variasjon i kvalitet på ID-kontrollen grunnet varierende opplæring og varierende (medfødte) evner hos personene som utfører en ID-kontroll. Feilraten i å gjennomføre en menneskelig ID-kontroll, hvor man sammenligner et ID-ansiktsbilde med en person kan ha så høy feilrate

som 40 %. Videre er dagens prosess sårbar for sosial manipulasjon og utro tjenere sammenlignet med en digital ID-kontroll. Strategien bør anerkjenne forbedringspotensialet som finnes både gjennom forbedring av fysisk ID-kontroll (økt bruk av maskinell støtte for ID-kontrollen ved f.eks ansiktskontroll) eller/og bruk av digital ID-kontroll. (Primært kommentar til 2.5 og 3.2)

Tilslutter refleksjon om risiko for misbruk av eID ved tap av "credentials". Vår erfaring er at brukere vil stjele eller miste credentials på et tidspunkt. Vi ønsker å framheve at målrettede phishing-angrep med hensikt å stjele credentials er økende, og dette bør framheves, og risikoen for misbruk av eID er ikke tilstrekkelig forstått i befolkningen i dag. De aller fleste sikkerhetsangrep og datatap innebærer eller skyldes phishing / tap av passord (75-91% i følge Google, BlackHat Conference), og suksessraten for en enkelt phishingforsøk er meget høy allerede (40%+ i følge Google, BlackHat Conference). Vår erfaring er at under COV19 så har angrepene blitt mer målrettet og gjennomførte mot eIDer, og i framtiden vil deep fakes gjøre disse enda mer troverdige (teknologi for å ringe med en annen person sin stemme finnes i dag allerede). Løsningene bør i mye større grad stille krav til periodisk verifikasjon av identitet (bruk av biometri) og ideelt sett bruke biometrisk kontroller i transaksjonsøyeblikket, slik at selv om en bruker sine credentials blir på avveie så er man avhengig av at personen faktisk deltar i en transaksjon. (Primært kommentar til 2.5 og 3.2)

Offentlig sektor bør tilrettelegge for at offentlig sektor og privat bruk av eID enkelt kan verifisere at rettmessig eier gjennomfører en transaksjon ved bruk av biometrisk kontroller (Merk: må være kontroller utover phone-built-in-biometrics, slik at faktisk identitet verifiseres). (Primært kommentar til 3)

Nasjonale myndigheter bør stille krav til at det gjennomføres periodiske digitale ID-kontroller ved et transaksjonsøyeblikk av en viss risiko eller etter en bestemt tidsperiode. (Primært kommentar til 3)

Strategien bør i større grad forankre og ha dedikerte tiltak for å sikre hjemmel for behandling av biometriske data for ID-kontroll i utstedelse, samt bruk av biometrisk data for å sikre at rettmessig bruker gjennomfører en autentisering/transaksjon. Vår opplevelse er at bruk av biometri til dette formålet nettopp bør gjøres for å beskytte identiteten til en person (bekjempe ID-tyveri og svindel), men vår opplevelse er at det er varierende kompetanse rundt det personvernfaglige for bruk av slik teknologi og i enkelte tilfeller manglende behandlingsgrunnlag. Strategien bør legge føringer og gjennomføre tiltak som sikrer behandlingsgrunnlag i hensiktsmessige bruksområder. (Primært kommentar til 3)

Strategien har en klar ambisjon om at alle brukere skal ha et klart forhold til (sin) eID og eID som et konsept. Vil det være realistisk å oppnå? Eller bør man i enkelte situasjoner lage så gode og brukervennlige løsninger hvor en bruker "bare får tilgang" eller kan "godkjenne i kraft av å være seg selv", og at ambisjonen ikke innebærer å tilgjengeliggjøre selve eIDen til en bruker. Eksempelvis: ansatte i kommunal sektor trenger å autentisere seg og godkjenne transaksjoner, men er det en egenverdi at de som brukere har et bevisst forhold til hvordan oppnå dette? Så lenge de har min biometri og PIN-kode eller har registrert enheten sin og kan vise ansiktet sitt? (Primært kommentar til 3)

Leverandøren ønsker å påpeke at det er viktig at det legges til rette for innovasjon og konkurranse også i eID-markedet, hvor det i enkelt tilfeller kan være mer hensiktsmessig med flere konkurrerende eIDer enn kun en. Eksempel; Er en felles kommunal eID beste løsning eller bør det være konkurranse? (men krav om integrasjon slik at løsningsleverandører i sum vil skape en helhetlig opplevelse for en sluttbruker som bytter jobb i kommunal sektor).

Det er forøvrig et meget godt strategidokument.