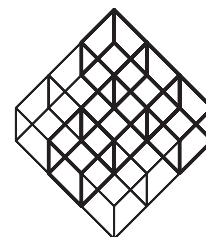


Justis- og politidepartementet
Magnar.aukrust@jd.dep.no



Teknologirådet

Vår ref.: 46.05
Deres Ref.: 2004/11659
Dato: 25. juni 2005

Elektronisk lagring av biometrisk passinformasjon – høringsuttalelse fra Teknologirådet

Teknologirådet er et uavhengig, offentlig organ som skal vurdere den teknologiske utviklingen på ulike samfunnsområder, gi innspill til Stortinget og øvrige myndigheter og stimulere til debatt om muligheter og konsekvenser som ny teknologi skaper.

Teknologirådet har nettopp avsluttet et større prosjekt som vil ha relevans for arbeidet med elektronisk lagring av biometrisk passinformasjon: *Elektroniske spor og personvern*. Prosjektet har blant annet bestått av arbeid i en ekspertgruppe, en åpen høring om personvern og en fokusgruppeundersøkelse om elektroniske spor og personvern. Denne høringsuttalelsen bygger i hovedsak på sluttrapporten fra prosjektet, som er vedlagt her som referanse¹.

Høringsuttalelsen tar utgangspunkt i høringsnotatet fra mars 2005 og fokuserer spesielt på de personvernmessige aspektene knyttet til biometrisk informasjon (fingeravtrykk), lagring av fingeravtrykk i en sentral database og hvordan data i denne databasen skal kunne brukes.

Biometriske data

Det er en rekke personvernrelaterte utfordringer knyttet til bruken av biometriske data, og det kreves derfor spesiell forsiktighet ved utrulling av slik teknologi.

Grunnen til dette er alvorlighetsgraden dersom en biometrisk mal (den digitaliserte og kodede versjonen av de biometriske dataene) blir kompromittert. Dersom noen får tak i et passord eller en PIN-kode kan skaden begrenses ved å

¹ Rapporten kan også leses på
http://www.teknologiradet.no/files/elektroniske_spor_og_personvern_190405_endelig.pdf

Pb 522 Sentrum
0105 Oslo

Prinsensgate 18
Norway

T: +47 23 31 83 00
F: +47 23 31 83 01

www.teknologiradet.no
post@teknologiradet.no

bytte kode. Biometriske kjennetegn er imidlertid permanente, og dersom et eller flere er kompromittert, betyr det at de ikke lenger kan brukes. For den rammede kan slikt identitetstyveri medføre utestenging fra tjenester uten mulighet for å få opprettet en ny bruker. Det finnes eksempler på at forskere har utviklet gode "falske" fingre som har lurt fingeravtrykkslesere i en stor andel av testtilfellene.

I forbindelse med utrulling av pass med elektroniske brikker som inneholder biometrisk informasjon har det vært diskusjoner i flere land omkring sikkerhetsnivået i de løsningene som har vært foreslått. Det er derfor viktig at norske myndigheter ikke forhaster seg i denne prosessen, men forsikrer seg om at de tekniske løsningene som velges er tilstrekkelig sikre i forhold til sensitiviteten på de data som skal beskyttes.

Det vil for eksempel være svært uheldig hvis data fra passets brikke kan leses på avstand, uten at innehaveren av passet er klar over det. Slik fjernavlesning gir et overvåkningspotensial som fra et personvernperspektiv vil være svært uheldig. Dersom passinnehaveren må åpne passet for at det skal kunne leses, vil det være lettere for innehaveren å sikre seg mot uautorisert scanning. Dataene i passet bør også være kryptert, slik at kun autoriserte myndigheter kan tyde dataene ved avlesning.

Fordi informasjonen fra brikken skal kunne leses ved flest mulig grensekontroller er man naturlig nok avhengig av at alle land som tar i bruk teknologien kan dekryptere informasjonen. Anbefalingene fra ICAO er at kryptonøkler skal oppbevares ved ICAOs hovedkontor i Montreal i Canada, samt ved en institusjon utpekt av den enkelte stat. En slik distribusjon av kryptonøkler øker muligheten for sikkerhetsbrudd gjennom menneskelig svikt, og det er derfor spesielt viktig å sikre at informasjonen i passet ikke kan leses av uvedkommende.

Lagring av fingeravtrykk i sentral database

Biometriske systemer bør så langt som mulig designes slik at biometriske maler lagres lokalt og ikke i sentraliserte databaser. Det er flere grunner til dette:

- Sentrale databaser er mer utsatt for sikkerhetsinnbrudd. Gjennom at alle dataene er lagret på et sted, vil et sikkerhetshull kunne få store konsekvenser fordi den biometriske informasjonen til et stort antall mennesker kan bli kompromittert.
- En sentral database gjør det enklere å bruke de innsamlede dataene til sekundære formål (såkalt *function creep*). Det er vanskelig å forestille seg at det ikke vil oppstå et ønske om å bruke et tilnærmet komplett fingeravtrykksregister i etterforskningsøyemed. Gjennom sitt forslag om at data i passregisteret skal kunne brukes av andre institusjoner som usteder ID-kort, har departementet allerede åpnet for tanken om bruk av registeret til sekundære formål.

Som det blir påpekt i høringsnotatet har ikke EU foreslått hjemmel for lagring av biometri i eksterne databaser. Teknologirådet vil stille spørsmål ved om de formålene sentral lagring er ment å oppfylle oppveier de negative konsekvensene en slik sentral lagring av biometriske data kan ha for personvernet.

Tilgjengeliggjøring av data i passregisteret for eksterne utstedere av ID-kort
I høringsnotatet forslås det at den biometriske informasjonen i passregisteret kan benyttes ved utstedelse av andre identitetsbeviser dersom det foreligger samtykke.

Det er i utgangpunktet positivt at departementet ønsker å kreve samtykke for slik bruk, men det er grunn til å stille spørsmål ved hvor reell en slik valgfrihet vil være for brukerne. Hva er alternativet dersom brukeren ikke samtykker? Skal han eller hun kunne nektes bankkort eller PKI for adgang til bruk av offentlige tjenester på nett?

En tjeneste som den som er foreslått vil nødvendigvis måtte medføre oversending av biometrisk informasjon over usikrede nettverk – uansett hvilken av aktørene som skal foreta verifikasjon av identitet. En slik oversending vil kunne utgjøre en sikkerhetsrisiko.

Formålet med biometrisk informasjon i passet er å øke sikkerheten ved grensekontrollen. Det er vanskelig å se at utstedere av identitetsbeviser har det samme behovet for økt sikkerhet som foreligger ved grensekontroll, og at det behovet som eventuelt måtte foreligge er mer tungtveiende enn hensynet til muligheten for kompromittering av sensitiv biometrisk informasjon.

Håndtering av overskuddsinformasjon

Overskuddsinformasjon kan utgjøre en trussel mot personvernet dersom den ikke håndteres riktig. I høringsnotatet foreslås det at overskuddinformasjon skal slettes både etter kontroll og utstedelse av pass.

Det er positivt at overskuddinformasjon i Norge vil bli håndtert på en forsvarlig måte. Gjennom sin deltakelse i de fora som er premissleverandører på dette området, har Norge også mulighet til å påvirke andre land til å håndtere overskuddsinformasjon på samme måte, slik at man også ved passering av utenlandske grensestasjoner kan føle seg trygg på at personopplysninger, inkludert biometrisk informasjon, blir slettet etter bruk.

Gjennomsiktighet og innsyn

Innsyn i egne data, og mulighet til å korrigere feilaktige opplysninger er et viktig personvernprinsipp. Det er positivt at departementet ønsker å sikre rett til å kontrollere og korrigere/slette de opplysningene som finnes i passet og i det sentrale passregisteret.

Med vennlig hilsen

Tore Tennøe
Sekretariatsleder, Teknologirådet