Nasjonal kommunikasjons-myndighet

Veiledning til selvdeklarasjon av eID-ordning

Veiledning for tilbydere av eID-ordninger etter selvdeklarasjonsforskriften

Versjon 1.0

27. april 2020

Nasjonal kommunikasjons-myndighet

Denne veiledningen er utarbeidet for å gi tilbydere av eID-ordninger veiledning i hvordan de skal dokumentere kravene i selvdeklarasjonsforskriften er oppfylt, jf. forsriftens § 7.

Meldingsskjemaet for selvdeklarasjon av eID-ordning bør derfor suppleres med tilstrekkelig dokumentasjon for at Nasjonal kommunikasjonsmyndighet (Nkom) skal kunne kontrollere om kravene i selvdeklarasjonsforskriften er oppfylt. Dette innebærer at meldingsskjemaet må følges av tilstrekkelig dokumentasjon.

Det norske kravsettet bygger på de europeiske sikkerhetsnivåene for eID. Det er et formål med selvdeklarasjonsordningen at selvdeklarerte eID-ordninger skal kunne meldes til EU-kommisjonen og slik sikres anerkjennelse av meldte eID-ordninger i hele EU/EØS-området.

Nkom anbefaler derfor at dokumentasjonen utformes slik at den kan gjenbrukes ved en eventuell senere norsk melding til EU-kommisjonen i henhold til eIDAS-forordningen, jf. artikkel 9 nr. 1.

Nkom anbefaler at følgende dokumentasjon følger meldingsskjemaet:

- **Dokument med en overordnet beskrivelse av eID-ordningen («white paper»), som med fordel kan inneholde følgende:**
  - Kort omtale av aktørene som inngår i eID-ordningen og dens utbredelse, markeds- og bruksområder og brukergrupper.
  - Overordnet beskrivelse av eID-løsningen (PKI-basert, særtrekk, dataflyt)
  - En gjennomgang av brukerreisen, med innrullering, utlevering av identifikasjonsmidler, bruksfasen, eventuell suspensjon og revokering. For online-løsninger kan skjermdump være hensiktsmessig. Er det flere alternative brukerreiser bør alle beskrives.
- **Dokument som viser etterlevelse av krav i meldingsskjemaet («LoA-mapping»), som med fordel kan inneholde følgende:**
  - Dette er et dokument som følger strukturen i meldingsskjemaet, men som gir flere detaljer ved behov. Det er viktig at man er tydelig på hvilke krav man dokumenterer etterlevelsen av, inkludert hvilke alternativer i de krav som har mange alternativer (f.eks. 2.1.2 om innrullering).
  - Tekniske detaljer, herunder sikkerhetsmessige krav som vern mot brute-force-angrep, kryptostyrke og bruk av HSM.
  - Organisatoriske detaljer, herunder aktører/underleverandører, krav til opplæring, tiltak for å hindre at enkeltpersoner kan kompromittere eID-løsningen og intern håndtering av livsløpet for eID-en.

Dokumentene ovenfor bør vise til relevante deler av annen dokumentasjon som vedlegges, herunder sertifikatpolicyer for PKI-basert løsninger eller tilsvarende for ikke-PKI-basert løsninger, revisjonsrapporter og samsvarsvurderingsrapporter.

Dokumentstrukturen må selvsagt tilpasses den konkrete eID-løsningen.

Nkom anbefaler at dokumentene utformes med nummererte kapitler (n.n.n.) og at dokumentene gis forkortede navn for å gjøre det enkelt å gi presise og entydige henvisninger, f.eks. G1-Gn for generelle dokumenter, T1-Tn for tekniske dokumenter, P1-Pn for policydokumenter etc.

Dersom vedlagt dokumentasjon er godt utformet, vil meldingsskjemaet i hovedsak kunne baseres på erklæring av at kravet er oppfylt med henvisninger til relevante deler i dokumentasjonen.