Direktoratet for forvaltning og IKT

Vår dato	Vår referanse
24.09.2009	10/980-2
Deres dato	Deres referanse
21.06.2010	201007547 EP KSI/mk

29 SEP 2010

Justis- og politidepartementet
Postboks 8005 Dep
0030 Oslo

Høring – elektronisk tinglysing

Vi viser til høringsbrevet av 21.06.2010.

Arbeidsgruppen har etter vårt skjønn gjort et grundig arbeid som bør kunne lede frem til regelverksendringer som sikrer tilstrekkelig klarhet og økt bruk av elektronisk kommunikasjon.

Vi har i vårt høringssvar konsentrert oss om spørsmål knyttet til elektronisk kommunikasjon, herunder informasjonssikkerhet og bruk av elektronisk ID/signatur, jf. at disse områder faller inn under Difi gjennom direktoratets tildelingsbrev.

Difi etablerer en infrastruktur på e-ID-området. I målbildet ligger etablering av løsninger for elektroniske signaturer.

Våre merknader følger kapitteloppbygningen i rapporten.

Kapittel 5

Vi vil gi utvalget honnør for å ha utarbeidet en risikoanalyse for bruk av elektroniske signaturer i tinglysningssammenheng (jf. også kapittel 8.3). En slik analyse gir grunnlag for å kunne velge akseptabelt risikonivå, og et gjennomgående synspunkt fra arbeidsgruppen er at risikoen ved elektroniske signaturer bør sammenlignes med risikoen i dagens system. Vi slutter oss til dette synspunkt. 100 % sikkerhet er ikke mulig å oppnå – spørsmålet er hva som er "godt nok", eller akseptabel risiko.

Utvalget legger til grunn at et system med elektroniske signaturer samlet vil gi lavere risiko enn det nåværende systemet.

Difi har ikke spesiell kjennskap til risikobildet på tinglysingsområdet, men fremstillingen av muligheten for falsk med konvensjonelle signaturer, jf. i kapittel 4.3.2, gir et godt utgangspunkt for analysen. Selv om det ikke sies eksplisitt, oppfatter vi det slik at svært mange personer vil være i stand til å skrive falske

Direktoratet for
Forvaltning og IKT (Difi)
Postboks 8115 Dep, 0032 Oslo
Telefon: 22 45 10 00

Besøksadresse Oslo:
Grev Wedels plass 9
Telefaks Oslo: 22 45 10 01

Besøksadresse Leikanger:
Skrivarvegen 2
Telefaks Leikanger: 57 65 50 55

postmottak@difi.no
Org.nr.: NO 991 825 827
www.difi.no

tinglysningsdokumenter. Avanserte elektroniske signaturer har etter vårt skjønn et noe avvikende trusselbilde, hvor angrep i større grad er begrenset til særlig kompetente personer/miljøer som har tilgang til (deler av) signaturfremstillingssystemene.

Arbeidsgruppen opplyser imidlertid at falsk i liten grad forekommer (5.3). Dét kan, på bakgrunn av ovennevnte, fremstå som overraskende. Arbeidsgruppen drøfter ikke nærmere hva som kan være mulige årsaker til den lave forekomsten. Vi vil anbefale at dette spørsmål analyseres i det videre arbeid.

Lovgivningen gir rettighetshaveren et meget sterkt rettslig vern når falsk konstateres (jf. tingll § 27 annet ledd), men en falskner skulle likevel kunne tenkes å oppnå kortsiktige gevinster – eksempelvis ifbm. videresalg eller urettmessig belåning, basert på falske dokumenter. Når falsk likevel sjelden forekommer, antar vi at det her er andre hindre som er effektive; en nærmere analyse som anbefalt over vil kunne avdekke om slike hindre også vil avverge falsk når signaturen er elektronisk. Vi viser til arbeidsgruppens redegjørelse i rapportens kapittel 8.3.

14.2 - vedr. beløpsgrense

Arbeidsgruppens flertall (se rapporten side 49-50) foreslår at beløpsgrensene i sertifikatet skal være styrende for hvilke dokumenter som kan tinglyses. Med de beløpsgrenser som i dag er i bruk, vil dette kravet kunne bli en "show stopper" for e-tinglysing.

Vi ser at hensynet til å sikre staten regressmuligheter ved erstatningsansvar etter tinglysningsloven § 35 kan tale for den foreslåtte regel.

Vi antar et sentralt vurderingstema da vil være om det er vesentlige forskjeller i risikoen for svik ved elektronisk og håndskreven signatur.

I sviktilfellene vil det primære ansvarssubjektet være svindleren. Dersom sviket er muliggjort gjennom falsk, håndskreven signatur, er det – i motsetning til ved bruk av elektroniske signaturer – ingen medhjelper å saksøke. Elektronisk signerte dokumenter gir med andre ord større muligheter for erstatning enn tradisjonelle signaturer, selv om erstatningsansvaret er begrenset oppad.

Vi vil således stille spørsmål ved hvor stort behov det er for å ansvarliggjøre sertifikatutstederen ut over beløpsgrensen.

til § 6

Lovforslaget legger opp til at det skal kreves signering med kvalifisert sertifikat, og at departementet i forskrift kan stille tilleggskrav. Vi kommer tilbake til dette spørsmålet i høring på forskriften, men minner om at Kravspesifikasjon for PKI i offentlig sektor er obligatorisk ved alle statlige anskaffelser av PKI-løsninger, jf. FADs beslutning 29.6.2006[1] (hjemlet i eforvaltningsforskriften § 27).

En ny versjon av kravspesifikasjonen er for øvrig utarbeidet. Den er p.t. til behandling i ESA etter EØS-høring, høringsfristen utløp den 23. september 2010.

---

[1] http://www.regjeringen.no/upload/kilde/fad/nyh/2006/0046/ddd/pdfv/290547-20062009_brev_til_samtlige_statsetater_og_ks.pdf

Vennlig hilsen
for Difi

Tone Bringedal
avdelingsdirektør

Jon Berge Holden

Kopi: Fornyings-, administrasjons- og kirkedepartementet, Postboks 8004 Dep, 0030 Oslo