dermed ikke kunne baseres alene på kvalificerede signaturer.

OCES-signaturen er en såkaldt softwarebaseret signatur, idet den leveres over internettet og lagres på indehaverens computerudstyr. Det giver principielt set mulighed for, at signaturen udstedes til en forkert person. De sikkerhedsmekanismer, der er indbygget i processen i forbindelse med udstedelse af signaturen reducerer dog risikoen herfor betydeligt, idet en uberettiget person både skal være i besiddelse af den berettigedes personnummer og have adgang til dennes post.

De ovenfor omtalte begrænsede risikovurderinger, der foreligger på nuværende tidspunkt, giver ikke Justitsministeriet anledning til at foreslå et krav om, at signaturer, der skal kunne anvendes til tinglysning, skal være udleveret til certifikatindehaveren ved personligt fremmøde, som det kræves ved de egentlige kvalificerede signaturer. Justitsministeriet er dog enig med udvalget i, at der skal foretages en samlet risikoanalyse af det kommende digitale tinglysningssystem, når kravspecifikationen foreligger, og at de sikkerhedsmæssige spørgsmål vedrørende OCES-signaturen skal indgå i risikoanalysen.

Der er endvidere mulighed for uberettiget kopiering af en eksisterende signatur og aflytning af password, hvis ikke signaturindehaveren beskytter sit edb-udstyr forsvarligt. Det kan ske ved angreb med et computerprogram, en såkaldt trojansk hest, som uberettiget installeres på signaturindehaverens computer, og giver den, der har installeret programmet, adgang til den angrebne computer. Dette vil dog forudsætte, at signaturindehaveren ikke på tilstrækkelig måde har beskyttet sit computerudstyr med et antivirusprogram og en firewall. Det adskiller sig helt principielt ikke fra, at også uforsvarlig omgang med en traditionel underskrift vil kunne føre til misbrug. Udviser man også en rimelig grad af forsigtighed ved håndteringen af sin digitale signatur, må riskoen for misbrug tilsvarende anses for minimal.

Ministeriet for Videnskab, Teknologi og Udvikling har over for Justitsministeriet oplyst, at OCES-signaturen teknisk set er opbygget ved brug af en avanceret matematisk algoritme, der i forhold til det nuværende teknologiske udviklingsniveau og den nuværende datakraft almindeligvis formodes at være tilstrækkeligt sikker i 5-6 år frem i tiden. Der er således ikke i dag kendte eksempler på, at det er muligt at bryde de koder, der sikrer autenticiteten og integriteten af et digitalt dokument, der er påført en digital OCES-signatur. Hertil kommer, at gyldighedsperioden for en OCES-signatur er begrænset til 2 år, hvorefter den vil skulle fornys. Leverandøren af OCES-signaturen er i øvrigt forpligtet sig til at tage højde for usikkerhed, der muligvis vil kunne opstå inden for den nævnte 5-6 årige periode.

Det er endvidere relevant at fremhæve, at de her omtalte problemstillinger af sikkerhedsmæssig karakter ikke vil have nogen betydning for allerede tinglyste digitale dokumenter. Disse dokumenter og de anvendte digitale signaturer vil være lagret i tinglysningssystemets databaser uden mulighed for, at uvedkommende efterfølgende kan foretage ændring i dokumenterne. Når et dokument først er tinglyst, er det med andre ord afskærmet fra påvirkning udefra, og det vil således være uden betydning, at den digitale signatur, der er anvendt ved signering af dokumentet, på et senere tidspunkt overhales af den tekniske udvikling.

Ministeriet for Videnskab, Teknologi og Udvikling vil løbende foretage vurderinger af OCES-signaturens sikkerhed. Hvis det skulle vise sig at være nødvendigt, vil der i medfør af den foreslåede bemyndigelsesbestemmelse i tinglysningslovens § 7, stk. 4, administrativt kunne ændres i de tekniske krav, der stilles til digitale signaturer, der anvendes til tinglysning. Det muliggør, at sikkerheden ved digital tinglysning vil kunne fastholdes på et tilstrækkeligt højt niveau.

I et system, der teknisk er baseret på OCES-signaturen, vil der naturligvis også kunne anvendes kvalificerede digitale signaturer fra eksempelvis andre EU-lande, idet de tekniske specifikationer er tilsvarende, og det EU-retlige krav om, at disse signaturer skal anerkendes her i landet, vil dermed være opfyldt.

4.3. Fuldmagtsordning

4.3.1. Indledning

Udvalget har overvejet, om et digitalt tinglysningssystem baseret på digitale dokumenter og den berettigedes digitale signaturer i tilstrækkelig grad vil kunne sikre, at enhver fortsat i praksis har mulighed for at få foretaget tinglysning.

Udvalget finder, at et ubetinget krav om anvendelse af den berettigedes digitale signatur på digitale tinglysningsdokumenter ville indebære en række væsentlige praktiske problemstillinger, idet det må påregnes, at mange vanskeligt eller slet ikke vil kunne skaffe sig eller anvende en digital signatur. Det gælder personer, som ikke er i besiddelse af det nødvendige computerudstyr, der gør dem i stand til over internettet at bestille og anvende en digital signatur, og formentlig mange, som ikke er fortrolige med anvendelse af moderne teknologi.