hvorefter medlemslandene kan fastsætte specifikke krav om forbud mod eller begrænsning af opbevaring af fakturaer i tredjelande, som ikke opfylder de nævnte betingelser.

Fakturaer, der fremsendes ad elektronisk vej, skal accepteres af medlemsstaterne på betingelse af, at ægtheden af deres oprindelse og integriteten af deres indhold garanteres. Dette kan ske:

1. Enten ved hjælp af en avanceret elektronisk signatur, jf. artikel 2, nr. 2), i Europa-Parlamentets og Rådets direktiv 1999/93/EF af 13. december 1999 om en fællesskabsramme for elektroniske signaturer. Medlemslandene kan dog kræve, at den avancerede elektroniske signatur er baseret på et kvalificeret certifikat og genereret ved hjælp af et sikkert signaturgenereringssystem, jf. artikel 2, stk. 6 og 10, i ovennævnte direktiv.
2. Eller ved hjælp af elektronisk dataudveksling (EDI) som defineret i artikel 2 i Kommissionens henstilling 1994/820/EF af 19. oktober 1994 om de retlige aspekter af elektronisk dataudveksling, når kontrakten om denne udveksling fastsætter, at der skal anvendes procedurer, som garanterer ægtheden af dataenes oprindelse og deres integritet. Medlemslandene kan dog i henhold til betingelser, de selv fastsætter, bestemme, at en supplerende oversigt på papir er nødvendig.

Efter direktivet om harmonisering af krav til momsfakturering kan momsfakturaer dog fremsendes ad elektronisk vej efter andre metoder end ovenstående under forudsætning af, at den eller de berørte medlemsstater accepterer disse.

Ved ægtheden af dataenes oprindelse forstås to forhold: dataenes autenticitet og dataenes uafviselighed.

Sikring af dataenes autenticitet kan ske ved brug af en digital signatur med tilhørende certifikat fra et nøglecenter/certificeringscenter (CA).

Overordnet opdeles certifikaterne i to typer; de kvalificerede certifikater, der efter lov om elektroniske signaturer kræver personligt fremmøde og klasse II certifikater, hvor sikring af brugerens identitet sker på anden vis.

I de tilfælde hvor der udstedes klasse II certifikater (se også nedenfor om OCES CP) benyttes normalt kendt viden om brugeren ved udstedelsen, for eksempel CVR adresse eller anden registrering, som giver større sikkerhed for ægthed i oprindelsen (her forstået som brugerens autenticitet). Told- og Skattestyrelsen benytter et pinkode system til blandt andet indberetning af moms og A-skat. Sikkerheden i udstedelsen baserer sig på, at man allerede kender brugeren fra andre registre, for eksempel CVR- og CPR-register, samt kender brugerens skattemæssige registreringer.

Den anden del af ægthed i oprindelsen, uafviseligheden, dvs. at en afsender ikke kan nægte at have sendt en bestemt meddelelse og en modtager ikke kan nægte at have modtaget en modtagelse, sikres normalt ved uafhængig tidsstempling, tidsstemplede kvitteringer hos en godkendt tredjepart og/eller logfiler hos myndigheden.

Integriteten af indhold, der sendes via Internettet uden brug af digital signatur sikres typisk via en såkaldt SSL kryptering som de fleste nyere standard Internet browsere, for eksempel MS Internet Explorer og Netscape, understøtter. Nyere browsere understøtter en kryptering på mindst 128 bits.

Direktivets regler om sikkerhed ved elektronisk momsfakturering giver ikke anledning til ændringer i gældende danske regler herom. De gældende danske certifikatpolitikker (CP) OCES (Offentlige Certifikater til Elektronisk Service) er offentliggjort den 2. september 2002 på IT- og Telestyrelsens hjemmeside på **https://www.signatursekretariatet.dk.** CP'erne kan downloades i pdf format fra hjemmesiden. Følgende introduktionstekst fremgår af hjemmesiden:

»For at fremme udbredelsen af digitale signaturer og for at etablere en standard på området har Videnskabsministeriet initieret implementeringen af OCES-certifikater (Offentlige Certifikater til Elektronisk Service).

Via OCES-certifikatpolitikkerne er der etableret en standard for certifikatudbydernes håndtering af certifikaterne og for indholdet i disse. Certifikatpolitikkerne, der har været til høring hos alle interesserede parter, udstikker det sikkerhedsniveau, der som minimum skal overholdes, hvis certifikatudbyderne vil kalde sig OCES-CA. OCES-certifikatet kan principielt anvendes til al kommunikation mellem myndigheder og mellem myndigheder og virksomheder eller borgere. Det er desuden tilstræbt, at OCES-certifikater også med fordel kan bruges i den private sektor.«

Til nr. 6

Med den foreslåede affattelse af § 66 gennemføres en særordning for virksomheder uden for EU (tredjelandsvirksomheder), som sælger elektroniske tjenesteydelser til private forbrugere i et EU-land, jf. i øvrigt afsnittet »Elektroniske tjenesteydelser« i bemærkningerne til nr. 1 ovenfor.

Reglerne om særordningen er fastsat i 6. momsdirektivs artikel 26 c som affattet ved artikel 1, nr. 3, i Rådets direktiv 2002/38/EF.