BILAG III

Krav til sikre elektroniske signaturgenereringssystemer

1. Sikre signaturgenereringssystemer skal ved hjælp af passende og tekniske og proceduremæssige midler i det mindste sikre, at:

   a) signaturgenereringsdata, der anvendes til signaturgenerering, i praksis kun kan fremtræde én gang, og at de med rimelig sikkerhed forbliver hemmelige

   b) signaturgenereringsdata, der anvendes til signaturgenerering, med rimelig sikkerhed ikke kan udledes, og at signaturen er beskyttet mod forfalskning under anvendelse af eksisterende teknologi

   c) signaturgenereringsdata, der anvendes til signaturgenerering, på pålidelig vis kan beskyttes af den retmæssige underskriver mod andres brug.

2. Sikre signaturgenereringssystemer må ikke ændre de data, som skal underskrives, eller hindre, at disse data vises for underskriveren forud for signaturprocessen.

BILAG IV

Anbefalinger vedrørende signaturverificering

I løbet af signaturverificeringsprocessen bør der skabes rimelig sikkerhed for, at:

a) de data, der anvendes til verificering af signaturen, svarer til de data, som vises kontrolløren

b) signaturen verificeres på pålidelig vis, og at resultatet af denne verificering vises korrekt

c) kontrolløren om nødvendigt på pålidelig vis kan fastslå indholdet af de underskrevne data

d) certifikatets ægthed og gyldighed, som kræves på tidspunktet for signaturverificeringen, verificeres på pålidelig vis

e) resultatet af verificeringen og underskriverens identitet vises på korrekt vis

f) anvendelsen af pseudonym klart fremgår

g) eventuelle sikkerhedsrelevante ændringer kan spores.
