Ministeren for videnskab, teknologi og udvikling

Udvalget for Videnskab og Teknologi
Folketinget
Christiansborg
1240 København K

Hermed fremsendes svar på spørgsmål nr. 246 (Alm. del) stillet af Udvalget for Videnskab og Teknologi den 14. september 2010. Spørgsmålet er stillet efter ønske fra Per Clausen (EL).

Med venlig hilsen

Charlotte Sahl-Madsen

1. oktober 2010

Ministeriet for Videnskab
Teknologi og Udvikling
Bredgade 43
1260 København K
Telefon 3392 9700
Telefax 3332 3501
E-post vtu@vtu.dk
Netsted www.vtu.dk
CVR-nr. 1680 5408

Sagsnr. 10-094495
Dok nr. 1528640

Spørgsmål nr. 246 stillet af Udvalget for Videnskab og Teknologi den 14. september 2010 til Ministeren for videnskab, teknologi og udvikling (Alm. del).

Spørgsmål 246

Kan ministeren bekræfte, at den digitale signatur NemID er lavet efter KeyEscow-princippet, som i 1997 blev forkastet i diskussionerne i videnskabsministeriet og Teknologirådet, fordi det betyder, at man lægger en bagdørsnøgle hos en central instans og, at dette betyder, at staten har mulighed for at bryde koden og læse personlig kommunikation, hvor man bruger NemID til at gemme denne.

Svar

Ministeriet for Videnskab
Teknologi og Udvikling
Bredgade 43
1260 København K
Telefon 3392 9700
Telefax 3332 3501
E-post vtu@vtu.dk
Netsted www.vtu.dk
CVR-nr. 1680 5408

Sagsnr. 10-094495
Dok nr. 1528640

Til besvarelse af spørgsmålet har jeg indhentet følgende udtalelse fra IT- og Telestyrelsen:

"DanID er underlagt de certifikatpolitikker, der gælder for udbydere af OCES-certifikater (Offentlige Certifikater til Elektronisk Service). I certifikatpolitikkerne stilles en række krav til udbyderens (CA'ets – certificeringscenterets) udstedelsesprocesser, nøglehåndtering, certifikathåndtering, anvendelse af algoritmer samt styring og drift af det tekniske miljø og de organisatoriske procedurer.

NemID med tilknyttet offentlig digital signatur udstedes i henhold til OCES-certifikatpolitikken version 4.0, hvori det under afsnit 7.2.4 fremgår, at "*CA må ikke foretage nøgledeponering af certifikatindehavers nøgler*". I certifikatpolitikkens afsnit 3.1 er nøgledeponering defineret som følgende: "*Nøgledeponering ("Key Escrow"): Lagring af nøgler, med henblik på at give tredjemand adgang til disse for at kunne foretage dekryptering af information*".

NemID med tilknyttet offentlig digital signatur er således designet med henblik på at forhindre Key Escrow.

Eksterne statsautoriserede systemrevisorer reviderer årligt, at DanID's systemer lever op til kravene i certifikatpolitikken.

IT- og Telestyrelsen påser via systemrevisorerne, at kravene i certifikatpolitikken overholdes."

Idet jeg samtidig henholder mig til ovenstående udtalelse fra IT- og Telestyrelsen, kan jeg hermed afvise påstande om, at NemID giver staten mulighed for at bryde koden og læse personlig kommunikation, hvor man bruger NemID til at gemme denne.