Fornyings- og administrasjonsdepartementet
Postboks 8004 Dep

0030 OSLO

Dato:
9. januar 2007

Deres dato:

Vår referanse
Birgith Klingenberg

Deres referanse

Bruk av "Kravspesifikasjon for PKI i offentlig sektor"

ZebSign har behov for en avklaring av krav til PKI leverandører og sertifikater, herunder det offentliges bruk av "Kravspesifikasjon for PKI i offentlig sektor", selvdeklareringsordningen og annen regulering som mekanisme for å pålegge leverandørene å gjøre tilpasninger i systemer og tjenester.

Formelle krav til leverandører og sertifikater
Lov om elektronisk signatur stiller krav om at leverandører av kvalifiserte sertifikater skal registres hos Post- og teletilsynet. ZebSign har registrert sine sertifikater i 2001 og 2003. Flere andre leverandører har registrert kvalifiserte sertifikater hos tilsynet, deriblant banker som usteder BankID, Commfides og Buypass.

Det offentlige fant imidlertid ikke registreringsordningen tilstrekkelig og utarbeidet en felles kravspesifikasjon for PKI i offentlig sektor som stiller ytterligere krav til sertifikater, leverandører og tjenester som skal benyttes i offentlig sektor. "Kravspesifikasjon for PKI i offentlig sektor" publisert versjon 1.02 ble publisert i januar 2005. Samme år ble statlige organer pålagt å benytte kravspesifikasjonen ved innkjøp av PKI tjenester i offentlig sektor og kommunesektoren sterkt anbefalt å benytte denne. Fra 1. januar 2006 er det innført en "frivillig selvdeklareringsordning" hvor leverandører som oppfyller krav i kravspesifikasjonen kan registrere seg hos Post- og teletilsynet. Selvdeklarering var dessuten et obligatorisk krav for leverandører som ønsket å levere tjenester gjennom felles offentlig sikkerhetsportal. ZebSign har registrert de tre sertifikatklassene som deklareringsordningen omfatter i løpet av 2006. Andre leverandører som Commfides og Buypass har registrert Person-Høyt og Virksomhetssertifikater.

Bakgrunn for henvendelsen
ZebSign ser med bekymring på utviklingen den senere tid hvor MinSide nå lanseres uten bruk av PKI og hvor det fortsatt hersker usikkerhet om det offentlige på tross av sterke føringer gjennom mange år vil velge å benytte andre sikkerhetsløsninger enn PKI og selvdeklarerte sertifikater også ved utvidelse av portalen.

Større organisasjoner som Helse Øst v/ NyeAhus har i "Tilbud 6783 Sertifikater (PKI) til ansatte", på tross av krav om at leverandører som tilbyr tjenester skal oppfylle kravspesifikasjonens krav, valgt å hovedsaklig benytte ikke-kvalifiserte sertifikater og valgt løsninger som ikke dekkes av selvdeklareringsordningen. Løsningen oppfyller heller ikke, etter vårt syn, anbefalinger som er gitt i "Kravspesifikasjon for PKI i offentlig sektor" om sikring av sensitive personopplysninger ved hjelp av kvalifiserte sertifikater som oppfyller krav til Person-Høyt sertifikater.

Vi stiller spørsmål ved om de foreliggende sakene er å anse som en endring av det offentliges praksis. Dette er fra vårt ståsted i så fall svært betenkelig – da PKI leverandørene gjennom lang tid har mottatt omfattende krav om tilpasninger av sertifikater, systemer og tjenester som vi finner det urimelig at det offentlige kan velge å se bort fra når dette ikke gir den økonomisk mest fordelaktige løsningen. Ut fra et sikkerhetsfaglig ståsted finner vi det dessuten svært betenkelig at borgerens personopplysninger ikke sikres godt nok ved å velge løsninger, som det offentlige gjennom "Kravspesifikasjon for PKI i offentlig sektor" ikke anbefaler.

MinSide og føringer fra FAD
Det er behov for en avklaring av hvor leverandørene står med hensyn til hvilke krav som skal stilles til løsninger som leveres til det offentlige. Flere kommuner og etater avventer kjøp av løsninger inntil avklaringer foreligger.

Det er av stor betydning for et selskap som ZebSign AS at det offentlige holder seg til sin egen kravspesifikasjon for anskaffelse av PKI-løsninger. Det er utført et stort arbeid i bransjen for, på beste måte, å kunne tilby produkter som er i samsvar det offentliges krav. Derfor har man lojalt tatt frem produkter som samsvarer med norsk lov og forskrifter, krav til egenmelding til Post og teletilsynet, gjennomført revisjoner i tråd med offentlige krav, implementert i henhold til offentlig kravspesifikasjon etc. Dersom offentlige virksomheter da ikke følger de samme retningslinjene i sine tilbudsinnbydelser, stiller man hele det forretningsmessige grunnlaget for virksomheten hos leverandøren i tvil. Dette gjelder i særdeleshet for ZebSign, som hittil har vært den ledende leverandøren av kvalitetssertifikater til det norske markedet og som sådan også underleverandør til andre tilbydere. Det økonomiske tapet, dersom det viser seg at virksomheten har en feil innretning ved at man har fulgt offentlige myndigheters oppfordringer, kan bli betydelig.

Helse Øst v/Nye Ahus
Spørsmålet er hvilken frihet offentlige etater og virksomheter har til å fravike kravspesifikasjonen frem til eventuelle nye retningslinjer foreligger.

I dette tilfellet er det stilt krav, men Helse Øst har under prosessen valgt å se bort fra kravet og heller valgt en rimeligere, etter vårt syn mindre sikker løsning.

I "Kravspesifikasjon for PKI i offentlig sektor" punkt 10.7 fremgår det at "Leverandøren av løsning for profesjonell bruk skal tilby en løsning basert på sertifikater av type "Person Høyt". Løsningen er tenkt brukt internt i virksomheter/etater for bl.a. pålogging, til sikker e-post og for personlig signering/autentisering integrert i etatenes fagsystemer.

I vedlegg 1 til kravspesifikasjonen om sikkerhetsnivåer forutsettes det at bruk av Person Standard kan benyttes når det er behov for tilgang til vedtak som finnes på "egnet informasjonssystem", jf. Eforvaltningsforskriften, og som ikke inneholder særlig følsomme opplysninger.

ZebSign har derfor lagt til grunn at det er behov for Person-Høyt sertifikater ved pålogging i interne systemer for å få tilgang til helseopplysninger. Helse Øst har imidlertid hovedsaklig valgt ikke-kvalifiserte sertifikater som skal benyttes ved pålogging og autentisering av ansatte og innleid personell mot helseforetakets nettverk og applikasjoner. Dette på tross av at det vises til punkt 10.7 i tilbudsutlysning. Helseforetaket er uenig i at dette er et absolutt krav og viser blant annet til at det i overordnet kravspesifikasjon fremgår at det hovedsakelig er behov for ikke-kvalifiserte sertifikater. Krav om bruk av "Person-Høyt" sertifikater for tilgang til sensitive personopplysninger støttes blant annet av uttalelse fra Kompetansesenteret for IT i helsesektoren (KITH) ved etablering av løsning ved St. Olavs hospital. KITH ble rådspurt om valg av sertifikatkvalitet, og det ble svart at "Person Høyt" var helt på linje med KITHs anbefalinger. KITH uttalte seg i denne sammenheng som rådgiver for, og på vegne av, Sosial- og helsedirektoratet.

Det er behov for en vurdering av hvordan kravspesifikasjonen skal fortolkes og benyttes av helseforetak og andre som forvalter sensitive personopplysninger.

Vedlagt brev til Datatilsynet til orientering.

Gebyr til Post – og teletilsynet
Samferdselsdepartementet har nylig foreslått å innføre gebyr for Post- og teletilsynets tilsyn med tilbydere som er selvdeklarerte etter forskrift om frivillige selvdeklareringsordninger for sertifikatutstedere. Innføring av eventuelt gebyr bør imidlertid utsettes, da vi mener at det hersker såpass stor usikkerhet til ordningen som sådan. Selvdeklareringsordningen og kravene til tilbydere bør evalueres før det eventuelt innføres gebyr.

Vedlagt følger høringsuttalelse som er sendt til Samferdselsdepartementet til orientering.

Konklusjon

Vi ber om en avklaring fra departementet av følgende:
Hvilke fremtidige krav vil bli stilt til PKI leverandører av FAD, koordineringsorganet for offentlige anskaffelser og andre offentlige virksomheter.
I hvilken grad offentlige etater og virksomheter kan fravike "Kravspesifikasjon for PKI i offentlig sektor" ved tilbuds/anbudsforespørsler.

Vennlig hilsen

Sven Falcke
ZebSign AS

Vedlegg: Brev til Samferdselsdepartementet
Brev til Datatilsynet

Kopi: Post- og teletilsynet
Postboks 447 Sentrum
0104 Oslo

Samferdselsdepartementet