BUYPASS AS
Nydalsveien 30A, PO Box 4364 Nydalen
N-0402 Oslo, Norway

t: +47 22 70 13 00
e: kundeservice@buypass.no
w: buypass.no

Nærings- og fiskeridepartementet
Postboks 8014 Dep

0032 Oslo

Deres ref:	*Vår ref:*	*Dato:*
15/4361	*Gunnar Lindstøl*	*29. februar 2016*

Høringsuttalelse – Gjennomføring av EUs forordning om elektronisk identifisering (eID) og tillitstjenester

Vi viser til Deres høringsbrev av 30. november 2015, med tilhørende forslag til ny lov som gjennomfører forordningen, og kommer i dette brev med vår høringsuttalelse.

Buypass er en ledende leverandør av eID, eSignatur og andre tillitstjenester til den nasjonale infrastrukturen. Vi er positive til at denne type løsninger og tjenester nå skal underlegges et felles regelverk for EU/EØS-området for å understøtte økt elektronisk samhandling mellom næringsdrivende, borgere og offentlige myndigheter på tvers av landegrenser. Vi ser også dette som en mulighet for å nå et større europeisk marked med våre løsninger og tjenester.

Overordnet mener Buypass at den nye forordningen representerer en viktig og riktig endring for å understøtte samarbeid og handel mellom aktører i EU/EØS-området. Videre er Buypass enig med departementet i at det er mest hensiktsmessig å vedta en ny lov som erstatter eksisterende «*Lov om esignatur*» med tilhørende forskrifter.

Under følger våre kommentarer til enkelte punkter i høringsnotatet.

Kapittel 2, punkt 1

Det fremgår i fortalen at medlemsstatene oppfordres til å muliggjøre bruk av notifiserte eID-er også i privat sektor. Buypass mener at det i denne sammenheng er viktig å få avklart hvorvidt bruk av offentlige utstedte autentiseringsmekanismer i private tjenester kan være problematisk ift statsstøtte/konkurranselovgivning.

Kapittel 6 - Avgrensning mot lukkede systemer

Buypass er enig i departementets vurdering i at forordningen ikke bør få anvendelse på lukkede systemer. Dette vil være helt i hht intensjonen med forordningen og bidra til at det norske regelverket er avstemt med regelverket i EU.

Kapittel 7.1 – Anerkjennelsesplikt og tolkningen av denne

Buypass mener at anerkjennelsesplikten bør oppfattes i hht underpunkt 2, nemlig at norske myndigheter har anerkjennelsesplikt uavhengig av om norske løsninger er notifiserte. Men det forutsetter at tilgang til tjenestene er definert i fht eIDAS-nivåene betydelig eller høyt (ref artikkel 6 punkt 1 c)).

Kapittel 7.2 – Eksisterende norske sikkerhetsnivåer

Det norske rammeverket for autentisering og uavviselighet dekker både autentisering og signering og det er i hovedsak sikkerhetsnivå 3 og 4 som brukes i Norge i dag.

For privatpersoner er nivå 4 ekvivalent med «*Person Høyt*» fra «*Kravspesifikasjon for PKI*». «*Person Høyt*» er igjen basert på kvalifisert sertifikat etter eSignaturloven, og det synes naturlig å videreføre nivå 4 for privatpersoner med en kobling mot kvalifisert sertifikat for elektronisk signatur i forordningen. Tilsvarende vil det være hensiktsmessig å knytte nivå 4 for virksomheter mot kvalifisert sertifikat for elektroniske segl i forordningen. Dette vil være svært fordelaktig for den omfattende sikkerhetsinfrastrukturen som er etablert i norsk helsesektor, inkl. kommunale helsetjenester. Noen eksempler på etablerte løsninger som benytter sikkerhetsinfrastrukturen er sykemeldinger, legeattester, oppgjørsmeldinger, eResept og Kjernejournal.

Det kan være en utfordring å skille mellom a) autentisering og tilhørende krav til eID og b) signering og kravene til denne tillitstjenesten. Begge er tett koblet i «*Kravspesifikasjon for PKI*» og «*Rammeverk for autentisering og uavviselighet*», spesielt for sikkerhetsnivå 4.

Buypass ønsker også å påpeke at forskjellen mellom nivå 3 og nivå 4 ikke er begrenset til krav om personlig fremmøte, men at det også er ulike teknologiske løsninger som aksepteres på de to nivåene. Nivå 4 krever PKI, mens nivå 3 ikke gjør det.

Som tilleggsinformasjon til siste avsnitt i samme kapittel er det verdt å merke seg at av totalt 67 millioner pålogginger i ID-porten i 2015, ble tilnærmet halvparten utført med eID på nivå 4 (BankID, Buypass, Commfides). Det betyr at svært mange pålogginger til nivå 3-tjenester blir gjennomført med eID på nivå 4.

Kapittel 8.1.2.1 - Kvalifiserte og ikke-kvalifiserte tillitstjenester

Forordningen opererer både med kvalifiserte og ikke-kvalifiserte tillitstjenester. De kvalifiserte tillitstjenestene, inkludert kvalifiserte sertifikater, er veldefinert og det er relativt greit å forstå hvordan disse er regulert. Når det gjelder ikke-kvalifiserte tillitstjenester og tilhørende ikke-kvalifiserte sertifikater, er det mer utydelig hvordan dette treffer oss som leverandør av tillitstjenester og utsteder av digitale sertifikater. En avgrensning på dette området vil være nyttig å få på plass, også i fht tilsynsmyndighetens arbeidsoppgaver.

Kapittel 8.1.1.5 - Bruk av kvalifiserte sertifikater for webside autentisering

Buypass er utsteder av SSL/TLS-sertifikater for autentisering av nettsider og våre rotsertifikater er allerede akseptert og forhåndsinstallert i alle aktuelle nettlesere og andre relevante applikasjoners rotsertifikatlager.

eIDAS innfører kvalifiserte sertifikater for webside autentisering basert på allerede etablerte bransjestandarder, Extended Validation (EV) Certificates fra CA/Browser Forum. Vi får dermed det vi kan benevne *kvalifiserte EV SSL-sertifikater* som er underlagt det nye felles europeiske regelverket og som samtidig tilfredsstiller bransjens egne standarder for SSL-sertifikater på høyeste tillitsnivå (EV).

Ved å benytte denne type sertifikater oppnår man å skape tillit overfor sluttbrukerne (med grønn adresselinje) samtidig som dette er forankret i et nytt felles europeisk rammeverk som skal ivareta tillit hos alle berørte parter. Sistnevnte håndheves ved at tilbydere av kvalifiserte EV SSL-sertifikater skal være registrert i tillitslisten i det landet tilbyderen opererer i.

EU-kommisjonen ønsker å skape et nytt marked for denne type SSL-sertifikater og vi oppfordrer norske myndigheter til å følge opp dette initiativet overfor norske offentlige virksomheter. Det er grunn til å tro at TLS (eller HTTPS) og dermed bruk av SSL-sertifikater vil bli obligatorisk for alle tjenester som nås av sluttbrukere via nettlesere.

Kapittel 8.1.1.6 – Krav til tilbyderne, eID ved utstedelse av kvalifiserte sertifikater

I siste avsnitt sies det at eID på nivå betydelig og høyt kan benyttes som identitetskontroll for utstedelse av kvalifisert sertifikat dersom personlig oppmøte har vært gjennomført. Dette forutsetter at det er tilgjengelig informasjon om hvorvidt det har vært gjennomført et personlig fremmøte ved den opprinnelig utstedelsen av eID på nivå betydelig.

Kapittel 8.1.2.1 - Tillitstjenester, signaturfremstillingssystem

I 3. avsnitt sies det at den som skal tilby kvalifisert elektronisk signatur kan velge å benytte seg av et sertifisert signaturfremstillingssystem fra et annet medlemsland. Buypass er enig i dette, men det må tillegges at tilbyder også kan sertifisere signaturfremstillingssystemet gjennom et sertifiseringsorgan i et annet medlemsland.

Kapittel 8.2.2.3 – Krav til signaturformater ved bruk i offentlig sektor

I 3. avsnitt hevdes det at det i liten grad stilles krav til avanserte elektroniske signaturer eller segl i norsk forvaltning. Dette er ikke korrekt. Av de over 169 millioner elektroniske meldinger i Norsk Helsenett i 2015, ble majoriteten signert med sertifikattypene Person Høyt og/eller Virksomhet.

Kapittel 8.2.2.4 - Særhjemmel om esignatur i offentlig sektor

Når «*Lov om esignatur*» erstattes av «*Lov om gjennomføring av EUs forordning om elektronisk identifisering og tillitstjenester for elektroniske transaksjoner på det indre marked*» er det etter Buypass sin vurdering ikke behov for å fastsette nærmere regler om kvalifiserte elektroniske signaturer. Hvis det mot formodning skulle vise seg nødvendig med ytterligere regulering er det åpning for dette i «*Forvaltningsloven*» § 15a, underbokstav a), e) og f).

Kapittel 8.3 - Tilsynsorgan

Buypass har i løpet av mer enn 10 år som leverandør av kvalifiserte sertifikater i hht eSignaturloven erfaring med at Nasjonal Kommunikasjonsmyndighet (Nkom) har fungert godt som tilsynsmyndighet. Vi ser ingen grunn til å vurdere andre myndigheter enn Nkom i rollen som tilsynsorgan etter forordningen.

Kapittel 8.6 - Gebyr

NFD foreslår at kostnadene til tilsyn i hht forordningen skal dekkes inn gjennom gebyr fra de som omfattes av regelverket. I denne sammenheng er det viktig å definere hvilke tilsynsoppgaver som skal dekkes av tilsynsmyndigheten og hvem som omfattes av dette regelverket. Forordningen introduserer mange nye tillitstjenester, blant annet ikke-kvalifiserte tillitstjenester, og arbeidsomfanget for tilsynsmyndigheten vil kunne variere fra tjeneste til tjeneste. En god og rettferdig fordeling av gebyr fra de som omfattes av regelverket kan være en utfordring.

Kapittel 9 - Selvdeklarasjonsordning og kravspesifikasjon for PKI i offentlig sektor

Kravspesifikasjonen er hjemlet i «*Forskrift om frivillige selvdeklarasjonsordninger for sertifikatutstedere*» som igjen er hjemlet i «*Lov om esignatur*», § 16a. Kravspesifikasjonen har primært vært et verktøy som er brukt for selvdeklarering av markedsaktører på sertifikattypene «*Person Høyt*» og «*Virksomhet*». Markedsaktørene er pålagt å gjennomføre selvdeklarering for å kunne tilby sertifikattjenester og tilhørende tjenester i offentlig sektor. Videre er kravsettet kun knyttet til PKI og er dermed ikke teknologinøytralt.

Den nye EU-forordningen dekker mye av kravsettet som fremgår i «*Kravspesifikasjon for PKI*», spesielt under tillitstjenester og kvalifiserte sertifikater, spesielt vinklet mot bruksområdet signering. Markedsaktører vil, som også høringsnotatet understreker, bli underlagt strengere og mer omfattende krav. Dette skal dokumenteres i en samsvarsrevisjonsrapport gjennomført av et myndighetsgodkjent samsvarsvurderingsorgan.

Den nye forordningen er teknologinøytral og introduserer nivåene «*Substantial*» og «*High*» i fbm autentisering. I den grad det er behov, foreslår Buypass at eventuelle kompletterende retningslinjer for offentlige tjenesteytere kan fremgå i en ny og oppdatert versjon av «*Rammeverk for autentisering og uavviselighet*», da med et tydeligere skille mellom bruksområdene autentisering og signering.

På bakgrunn av ovenfor nevnte mener vi at det ikke er nødvendig å opprettholde selvdeklarasjonsordningen og tilhørende kravspesifikasjon for PKI. Videre foreslår vi at § 2 i foreslått lovtekst strykes.

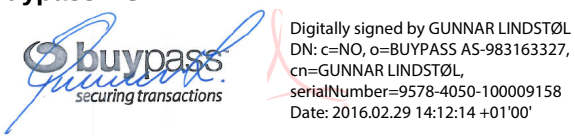
Kapittel 10 - Overgangsordninger for kvalifiserte tillitstjenester

Forordningen trer i kraft i EU allerede 1.juli 2016 og alle medlemsland vil fra da kunne utvide sine tillitslister med nye tillitstjenester etter hvert som tilbyderne legger frem samsvarsvurderings-rapporter for tillitstjenester i hht forordningen.

Siden forordningen etter gjeldende plan vil bli innført først 1. januar 2017 i Norge vil dette kunne virke diskvalifiserende for norske tilbydere som ønsker å posisjonere seg i fht et nytt og åpent europeisk marked. Buypass er som utsteder av SSL/TLS-sertifikater for eksempel interessert i å kunne tilby kvalifiserte SSL/TLS-sertifikater i EU, men dette forutsetter at vi er registrert som utsteder av slike på den norske tillitslisten. Det er uklart når en slik oppdatert versjon av tillitslisten vil være på plass i Norge. Vi oppfordrer derfor norske myndigheter til å etablere en tillitsliste med nye tillitstjenester gjeldende fra 1. juli 2016.

Med vennlig hilsen

Buypass AS



Gunnar Lindstøl

Administrerende direktør