notat

ÅPEN

Til / To	NHD
Kopi / Copy	.
Fra / From	Buypass
Dato / Date	18.12.2012

Forslag til EU-forordning om eID og tillitstjenester – Buypass' høringssvar

I juni 2012 kom Europakommisjonen med et forslag til ny forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i EUs indre marked. Dette er Buypass' svar på høringen som Nærings- og Handelsdepartementet har invitert til.

Buypass er generelt positiv til hovedtrekkene i forslaget til ny EU-forordning om eID og tillitstjenester. Dette gjelder spesielt utvidelsen av virkeområdet i fht dagens eSignatur-direktiv og etableringen av et felles europeisk regelverk som skal implementeres i alle EU/EØS-land, inklusive Norge.

Med et slik felles europeisk regelverk faller mye av behovet for et særnorsk regelverk på området bort og Buypass forventer at det norske regelverket blir harmonisert med det europeiske når denne forordningen skal implementeres i Norge.

Buypass er en ledende leverandør av eID, eSignatur og relaterte tillitstjenester til det offentlige Norge og det regelverk slike produkter og tjenester er underlagt er en viktig premiss for Buypass. Det er viktig at Buypass og andre kommersielle aktører som er med på å etablere en nasjonal infrastruktur rundt slike tjenester tas med i prosessen med harmoniseringen av norsk regelverk.

1 Innledning

Forslaget består av to deler der første del har fokus på gjensidig anerkjennelse av elektronisk identifikasjon (eID) på tvers av landegrenser basert på en innmeldingsordning. Andre del av forordningen består av en regulering av såkalte kvalifiserte tillitstjenester, herunder elektronisk signatur.

Det er verdt å merke seg at det er en ubalanse her i fraværet av regulering av elektronisk identifikasjon i første del sammenlignet med reguleringen av de andre tillitstjenestene i andre del. I dagens norske regelverk er både elektronisk identifikasjon (autentisering) og elektronisk signatur regulert gjennom Kravspesifikasjonen for PKI offentlig sektor og selvdeklarasjonsordningen. Det vil tilsynelatende være vanskelig å videreføre en slik felles modell når forordningen skal implementeres i Norge.

Buypass AS
Nydalsveien 30A, PO Box 4364 Nydalen
N-0402 Oslo, Norway
Tel.: +47 23 14 59 00
Fax: +47 23 14 59 01
E-mail: kundeservice@buypass.no
VAT: NO 983 163 327
www.buypass.no

2 Elektronisk identifikasjon

Forslaget definerer en innmeldingsordning der et EU/EØS-land kan melde inn elektroniske identifikasjonsløsninger eller autentiseringsmekanismer som aksepteres til bruk mot offentlige tjenester i det aktuelle landet. Forordningen krever at slike innmeldte autentiseringsmekanismer må anerkjennes av andre EU/EØS-land for bruk mot offentlige tjenester i deres land.

Autentiseringsmekanismer som kan meldes inn må oppfylle en del betingelser, herunder at de skal være underlagt en form for offentlig kontroll/godkjenning. Buypass legger til grunn at Norge kan melde inn autentiseringsmekanismer også fra private aktører som tilfredsstiller nivåene Person-Høyt og Virksomhetssertifikat i hht Kravspesifikasjonen. Dette vil da inkludere Buypass' produkter og tjenester.

Implementering av forordningen i Norge vil som nevnt innledningsvis ha konsekvenser for norsk regelverk og praksis på området. Dette vil i neste omgang også kunne ha konsekvenser i forhold til autentiseringsmekanismene som aksepteres for bruk mot offentlige tjenester i Norge.

Et EU/EØS-land kan selv velge å melde inn aksepterte autentiseringsmekanismer, men må uansett anerkjenne andre lands innmeldte autentiseringsmekanismer. Dette gjelder uten forbehold og dette synes å være en svakhet ved denne delen av forordningen.

Det bør være mulig å skille mellom ulike sikkerhetsnivåer for tilgang til ulike typer offentlige tjenester. Et EU/EØS-land som for eksempel aksepterer brukernavn/passord for tilgang til sine offentlige tjenester, kan melde inn en slik autentiseringsmekanisme. Det synes urimelig å forvente at alle andre land uten videre skal anerkjenne en slik autentiseringsmekanisme.

For å få til en hensiktsmessig differensiering av autentiseringsmekanismer bør det etableres et felles europeisk rammeverk som definerer aktuelle sikkerhetsnivåer. I STORK-prosjektet er det allerede definert et slikt rammeverk og amerikanske NIST har også definert et rammeverk med interessante egenskaper. Innføring av et slikt rammeverk synes å være en nødvendig forutsetning for å få aksept og anerkjennelse for en slik innmeldingsordning.

Forordningen krever også at et land som har meldt inn aksepterte autentiseringsmekanismer må sørge for at disse mekanismene er tilgjengelig online slik at brukersteder i andre land til enhver tid fritt skal kunne benytte slike tjenester for autentisering/validering. Dersom noen av Buypass' autentiseringsmekanismer meldes inn, så vil dette kunne ha konsekvenser for tilgang til og bruk av våre tjenester. Som en kommersiell aktør vil vi måtte forholde oss til slike konsekvenser på en forretningsmessig måte.

Forordningen åpner for bruk av innmeldte autentiseringsmekanismer også i privat sektor. Det kan i denne sammenheng være viktig å få avklart hvorvidt bruk av offentlige utstedte autentiseringsmekanismer i private tjenester er problematisk ift statsstøtte/konkurranselovgivning.

Forslaget åpner for ytterligere reguleringer og teknisk standardisering for å sikre interoperabilitet mellom ulike land. Dette vil også kunne ha konsekvenser for Buypass' produkter og tjenester og det er viktig at norske myndigheter har et aktivt forhold til dette for å sikre at kommersielle/private tilbydere ikke får urimelige krav til endringer og tilpasninger av eksisterende løsninger.

Forslaget stiller også krav til unik identifisering av både fysiske og juridiske personer. Spesielt med tanke på fysiske personer er det viktig at personvernhensyn blir ivaretatt og at krav til bruk av fødselsnummer for eksempel håndteres på en god måte.

3 Tillitstjenester

I denne delen av forordningen utvides virkeområdet i fht eSignatur-direktivet til å omfatte flere tillitstjenester utover elektronisk signatur for fysiske personer. Buypass er positive til at også juridiske personer nå skal dekkes av forordningen og at andre tjenester inkluderes, herunder SSL-sertifikater.

Tilsynsmyndigheter får utvidede plikter og ansvarsområder med forordningen og det kreves bla at de skal overvåke tilbydere av tillitstjenester (artikkel 13 pkt 2 (a)) generelt for å sikre at disse oppfyller krav i artikkel 15. Det er imidlertid noe uklart hvilke tilbydere og tjenester som er dekket i dette punktet. Dette synes å gjelde tilbydere og (ukvalifiserte) tillitstjenester som ikke direkte er omfattet av forordningen, dvs tilbydere av kvalifiserte tillitstjenester og deres tjenester.

Forslaget stiller krav til årlig revisjon av tilbydere av kvalifiserte tillitstjenester og at en slik skal utføres av en uavhengig part. Det blir viktig å få klarlagt roller og ansvarsfordelingen mellom revisorer, godkjenningsmyndigheter og tilsynsmyndigheter. Buypass er pt underlagt revisjon i fht ETSI 102 042 og vi forventer at en slik revisjon kan tilpasses og videreføres under et regime som tilfredsstiller den nye forordningen.

Artikkel 19 beskriver krav til identitetskontroll i fbm utstedelse av kvalifiserte sertifikater både for fysiske og juridiske personer. Det stilles krav til personlig fremmøte eller at personen identifiserer seg elektronisk ved bruk av innmeldt autentiseringsmekanisme. Her forutsettes det altså at personen kan autentisere seg med en innmeldt autentiseringsmekanisme, men uten å stille ytterligere krav til sikkerhetsnivå på en slik autentiseringsmekanisme (med et viktig unntak om krav til personlig fremmøte). Det synes også her å være hensiktsmessig å kunne si noe om sikkerhetsnivået på autentiseringsmekanismer som kan aksepteres, se tilsvarende kommentar under Elektronisk identifikasjon.

Det kan i denne anledning også nevnes at artikkel 20 benytter begrepet ’Security Assurance Level’ om sikkerhetsnivå i forhold til elektronisk signatur. Dette burde vært sett i sammenheng med behovet for sikkerhetsnivå på elektronisk identifisering som nevnt over.

Forordningen inkluderer også det vi kan kalle kvalifiserte SSL-sertifikater (artikkel 37). Buypass har forstått det slik at kommisjonen ser for seg at dette skal være ekvivalent med Extended Validation (EV) SSL-sertifikater.

EV SSL-sertifikater er sertifikater som utstedes i hht EV Guidelines, etablert av CA/Browser forum for å sikre høyere tillit og aksept hos sluttbrukere som benytter tjenester på nett. Alle nettlesere presenterer nettsteder som autentiserer seg med EV SSL sertifikater med en visuell indikator (grønn adresselinje) som gjør det lett for sluttbrukere å identifisere slike ”sikre” nettsider. Dette er et resultat av samarbeidet i CA/Browser forum og nettleserleverandørene krever at sertifikatutstedere skal være sertifisert i hht WebTrust for CA og WebTrust for EV SSL eller ETSI 102 042 for å komme inn med sine rotsertifikater og derigjennom få den ettertraktede visuelle indikatoren for sine EV SSL sertifikater.

Buypass har, som medlem av CA/Browser forum, registrert en del usikkerhet når det gjelder forholdet mellom EU-kommisjonens kvalifiserte SSL-sertifikater og forumets EV SSL sertifikater. Dersom kvalifiserte SSL-sertifikater er ment å være ekvivalent med EV SSL sertifikater er det viktig at forordningen harmoniseres med CA/Browser forums retningslinjer på dette området. Det er også viktig at man baserer sluttbrukernes aksept og tillitt til slike sikre nettsteder på samme visuelle indikator. Et samarbeid mellom EU-kommisjonen og CA/Browser forum på dette området synes nødvendig for å unngå et fragmentert marked for SSL-sertifikater i og utenfor Europa. Dette er ingen tjent med.

Det er i denne sammenheng også verdt å nevne at artikkel 19 gjelder utstedelse av det kvalifiserte SSL-sertifikater. Det er pt ikke krav til personlig fremmøte ved utstedelse av EV SSL-sertifikater i hht CA/Brower Forums EV Guidelines og det bør ikke innføres andre regler for utstedelse av slike kvalifiserte SSL-sertifikater dersom hensikten er at disse skal være på samme nivå.

Buypass AS
Nydalsveien 30A, PO Box 4364 Nydalen
N-0402 Oslo, Norway
Tel.: +47 23 14 59 00
Fax: +47 23 14 59 01
E-mail: kundeservice@buypass.no
VAT: NO 983 163 327
www.buypass.no