



Sparebankforeningen
The Norwegian Savings Banks Association

Fornyings- og administrasjonsdepartementet
Postboks 8004 Dep
0030 OSLO

Kopi: Finansdepartementet

Deres ref:
200700605-KDB

Vår ref:
200700174 (FNH)
200700044 (Spafo)

Dato
Oslo, 14. mai 2007

Forslag til strategi for bruk av eID og e-signatur i offentlig sektor

Det vises til Fornyings- og administrasjonsdepartementets brev av 12. mars 2007 der et notat fra en arbeidsgruppe med forslag til strategi for eID og e-signatur i offentlig sektor ble oversendt til uttalelse. Sparebankforeningen og Finansnæringens Hovedorganisasjon (FNH) avgir med dette felles høringsuttalelse.

Økt bruk av eID og e-signatur i offentlig sektor vil gi samfunnsøkonomiske gevinster og bidra til at folk flest får bedre og enklere tilgang til det offentlige tjenestetilbud. Det er derfor positivt at FAD har et sterkt engasjement for å utvikle gode offentlige elektroniske tjenester. Målet med den strategien departementet nå skal utforme, må være at *flest mulig* i Norge får enkel, trygg og brukervennlig tilgang til offentlige elektroniske tjenester *så raskt og kostnadseffektivt som mulig*.

En bestemt teknisk løsning for eID må ikke bli et mål i seg selv. Det vil gå ut over muligheten til rask og kostnadseffektiv utrulling av offentlige tjenester på nett. Tekniske løsninger er virkemidler – også når det er snakk om eID.

FNH og Sparebankforeningen understreker at gevinstene for publikum og offentlig sektor enklest og billigst realiseres ved å bruke allerede etablerte løsninger for eID og e-signatur:

- Mange offentlige virksomheter bruker allerede, eller tilrettelegger nå for, eID og e-signatur. Flere kommuner og etater er i ferd med å høste gevinstene av investering og satsing på bruk av eID i sine tjenester. Andre har forventninger om å videreutvikle tilbudet allerede i år, fordi det er en sterk økning i utbredelsen av eID med høy kvalitet.
- Et stort antall borgere og næringslivsaktører ønsker og forventer å kunne bruke allerede anskaffet og hyppig brukt eID, også til offentlige tjenester.

For det offentlige vil det å velge verktøy som allerede er mye brukt som sikkerhetsløsning, være den raskeste og mest kostnadseffektive strategien for å gi trygg og enkel tilgang til offentlige nettjenester for alle brukere. Det er betydelig høyere terskel for brukerne til å ta i bruk nye verktøy eller verktøy man ikke bruker jevnlig.

Nye verktøy innebærer også betydelig mer "plunder og heft" for brukerne, og ikke minst risiko for svært høye kostnader til brukerstøtte og -administrasjon for offentlig sektor. Vi kan vanskelig se at det er realisme i de kostnadsanslag som er gitt i arbeidsgruppens rapport.

Noen synspunkter og innspill er ytterligere utdypet i vedlagt notat.

En rapport fra ECON peker klart i retning av at Norge bør satse på gjenbruk av løsninger som allerede er utviklet og rullet ut i befolkningen. Norge, Sverige og Danmark har basert seg på løsninger utviklet av private aktører, mens Finland har forsøkt å bygge opp en egen statlig infrastruktur. Den finske strategien ser ut til å ha vært langt mindre effektiv enn de andre landenes strategi på dette området. Finland startet utrulling av sitt borgerkort 1. desember 1999, men har ved inngangen til 2007 bare 123.000 brukere. Rapporten fra ECON er vedlagt.

Banknæringen har lang og bred erfaring med sikker elektronisk kommunikasjon både i forhold til enkeltpersoner, private virksomheter og offentlig sektor. Innen utgangen av 2008 vil flertallet av alle Norges 2,5 millioner nettbankkunder bruke banknæringens samordnede eID, BankID, som elektronisk ID og signatur. Våre brukerundersøkelser viser allerede i dag både høy bruksfrekvens og god brukervennlighet:

- BankID er nå tatt i bruk av 700.000 personer, og disse benytter i gjennomsnitt BankID to ganger hver uke
- BankID-brukerne oppgir en kundetilfredshetsscore på hele 5,2 (skala fra 1 til 6 der 6 angir høyest tilfredshet)
- 6 av 10 BankID-brukere sier at de gjerne vil benytte BankID i elektroniske tjenester fra offentlig sektor

Også andre utstedere har betydelige volumer av eID-er i det norske markedet.

BankID tilfredsstiller allerede det foreslåtte sikkerhetsnivå 4. Fellesmelding med deklarerer hos Post- og teletilsynet som Person-Høyt er levert, og den enkelte utsteder er registrert som utsteder av kvalifisert sertifikat.

Banknæringen ønsker å bidra aktivt til sikker elektronisk kommunikasjon gjennom økt bruk av eID og e-signatur. Dette gjelder også i forhold til offentlig sektors elektroniske tjenester. Det er riktig at det offentlige selv har et sterkt engasjement for å utvikle gode offentlige sikre elektroniske tjenester. Vi legger til grunn at FAD har som mål at *flest mulig* i Norge kan få enkel, trygg og brukervennlig tilgang til offentlige elektroniske tjenester *så raskt og kostnadseffektivt som mulig*. Vi mener at allerede etablerte eID-utstedere kan gi verdifulle bidrag for å kunne nå dette målet. Banknæringen ønsker å bidra positivt og ser frem til et videre samarbeid.

Med vennlig hilsen
for Finansnæringens Hovedorganisasjon

for Sparebankforeningen i Norge

Tor Johan Bjerkedal

Jan Digranes

Vedlegg:

1. Notat med enkelte utdypende kommentarer
2. Elektronisk legitimasjon i Norden, Rapport 2007-009, ECON
3. Resultater om BankID fra Sparebankforeningens nettbankundersøkelse 2007

Vedlegg 1: Noen utdypende kommentarer til forslag til strategi for eID og e-signatur i offentlig sektor

Krav til sikkerhet ivaretas gjennom e-signaturloven

I arbeidsgruppens forslag til strategi fremheves statlig behov for kontroll med sikkerheten for eID brukt i det offentlige.

Vi vil påpeke at det offentlige allerede i dag har god kontroll og styring over sikkerhetsbehovet på elektronisk kommunikasjon på sikkerhetsnivå 3 og 4. Det sikres gjennom de krav som stilles til kvalifiserte sertifikater og selvdeklarerer i forhold til Kravspesifikasjon for PKI i offentlig sektor, begge med hjemmel i e-signaturloven, gir allerede det offentlige god styring i forhold til sikkerhetsbehovet på elektronisk kommunikasjon på sikkerhetsnivå 3 og 4. At det offentlige har slik kontroll, har også vært Staten/FADs vurdering i arbeidet med kravspesifikasjonen, selvdeklarasjonsordningen, eforvaltningsforskriften og e-signaturloven. Banknæringen har forholdt seg til og tilpasset seg til dette regelverket.

Egen offentlig eID må likebehandles med likeverdige eIDer

Det er positivt at arbeidsgruppen ikke foreslår å gjeninnføre forretningsmodellen og organiseringen som ble brukt i forbindelse med den tidligere Sikkerhetsportalen. Dette vil gi større rom for det offentlige til å føre forhandlinger med tilbydere av eID med sikte på å oppnå løsninger, herunder forretningsmodeller (prismodeller), som ivaretar spesielle behov som offentlige myndigheter har.

Arbeidsgruppens forslag til strategi peker i retning av at det offentlige etablerer sin egen eID-løsning. Det er selvsagt ingenting prinsipielt i veien med dette, men som det fremgår av vår høringsuttalelse: Det vil være en meget lite heldig løsning å gjøre bruk av offentlige elektroniske tjenester på nett eksklusivt knyttet til en egen eID-løsning for bruk mot og i offentlig sektor, mens andre eIDer som er i daglig bruk av folk flest stenges ute. En slik "eksklusjonsstrategi" vil medføre så sterke begrensinger og forsinkelser i utrulling av offentlige elektroniske tjenester at vi tar det som en selvfølge at FAD ikke vil legge seg på denne linjen.

Spørsmålet blir da hvilke rammebetingelser det offentlige fastsetter for sin egen eID-løsning i forhold til myndighetenes rammebetingelser for de markedsbaserte løsninger. Vi legger til grunn at en offentlig løsning må forholde seg til det samme regelverk, konkurranse- og rammevilkår, som private eID-utstedere er underlagt, herunder at det offentlige i sin utstedelse følger e-signaturlovens regler og oppfyller Kravspesifikasjonen for PKI i offentlig sektor. Gitt at en offentlig løsning og andre aktørers løsninger skal operere under de samme rammebetingelser, og det finnes flere løsninger i markedet som for tiden er under rask utrulling til flertallet av norske nettbrukere, er det vanskelig å se gode grunner til at det offentlige skal påta seg de betydelige kostnader som etablering og drift av egen løsning vil representere.

Spesielt om det offentliges utstedelse av eID til virksomheter

Banknæringen opplever at det er relativt mange uavklarte forhold i forslaget til strategi på dette området.

For eksempel blir det i forslaget ikke klart kommunisert hvorvidt det er naturlig at det benyttes virksomhetssertifikater eller personsertifikater, alternativt rollesertifikater, for utveksling av elektronisk informasjon i risikoklasse 3 og 4 mellom virksomheter og offentlig forvaltning samt internt i offentlig forvaltning. I svært mange sammenhenger pålegger for eksempel lovgevingen at det er personer med en bestemt rolle i virksomheten som skal signere på rapporter, erklæringer og så videre. Eforvaltningsforskriften nevner riktignok bruk av virksomhetssertifikater i forbindelse med underretning om vedtak, samt at forskriften legger enkelte føringer for bruk av personlige sertifikater i forvaltningen.

Et annet eksempel er at det ikke nevnes i forslaget hvordan man har tenkt at Enhetsregisteret i Brønnøysund på en tilfredsstillende måte skal gjennomføre RA-oppgaven med legitimasjonskontroll av personer som mottar eID på vegne av de forskjellige virksomhetene.

Om samtrafikknivet

Etter banknæringens oppfatning er en viktig hensikt med et samtrafikkniv å legge til rette for at offentlige virksomheter enkelt kan benytte eIDer fra ulike utstedere. Dette omfatter også eIDer av høy kvalitet som er utstedt av private virksomheter, og som allerede tatt i bruk i stort omfang av privatpersoner og næringsliv.

Vi understreker at gevinstene for publikum og offentlig sektor enklest og billigst realiseres ved å bruke allerede etablerte løsninger for eID og e-signatur:

- Mange offentlige virksomheter bruker allerede, eller tilrettelegger nå for eID og e-signatur. Flere kommuner og etater er i ferd med å høste gevinstene av investering og satsing på bruk av eID i sine tjenester. Andre har forventninger om å videreutvikle tilbudet allerede i år, fordi det er en sterk økning i utbredelsen av eID med høy kvalitet.
- Et stort antall borgere og næringslivsaktører ønsker og forventer å kunne bruke allerede anskaffet og hyppig brukt eID, også til offentlige tjenester.

Dersom offentlig sektor skulle velge å utelukke bruk av høykvalitets eIDer utstedt av privat sektor, vil man dessuten antagelig oppleve komplikasjoner for tjenester som involverer flere verdikjeder. For eksempel er det i tinglysingen nødvendig at eID utstedt av private aktører også må kunne brukes i elektroniske tjenester som involverer det offentlige. Å skrive et skjøte, pantsette eller gi andre en rettighet i fast eiendom er i seg selv privatrettslige disposisjoner – altså en rettslig disposisjon mellom to private personer. For å gjennomføre denne disposisjonen burde det således ikke være nødvendig å trekke inn føringer fra arbeidsgruppens forlag til strategi for eID eller e-signatur som jo gjelder for samhandling med offentlig forvaltning. Ofte ønsker imidlertid partene at denne privatrettslige disposisjonen skal gis notoritet og publisitet gjennom tinglysingsordningen. En slik etterfølgende rettsvernhandling må imidlertid ikke formes slik at den signaturløsning som panthaver eller erverver av rettighet i eiendommen har stolt på, likevel ikke kan brukes.

Om forretningsmodell og kostnader

Banknæringen ser som nevnt positivt på at arbeidsgruppen ikke har videreført forretningsmodellen for den tidligere Sikkerhetsportalen.

Basert på banknæringens egne erfaringer, mener vi at arbeidsgruppen har undervurdert både kostnader og kompleksitet ved etablering og drift av eID-tjenester. Banknæringen og andre private eID-utstedere har erfart helt andre kostnadstall enn det man opererer med i strategiforslaget. Utbygging, vedlikehold og drift av nødvendig infrastruktur, apparat for utstedelse samt oppbygging av tilstrekkelig kapasitet for kundesupport og sperretjenester krever betydelige ressurser.

BankID er godt egnet som eID for offentlig sektor

Til slutt noen bemerkninger i forhold til bruk av bankenes eID – BankID – i offentlig sektor.

Det er en samlet banknæring i Norge som har lansert BankID som et kvalifisert elektronisk sertifikat for elektronisk autentisering og signatur ("uavviselighet"). Formålet var først og fremst bedre tilgjengelighet og mer anvendelige samordnede elektroniske finansrelaterte tjenester for kundene. For å oppnå virksam konkurranse er det avgjørende at tilgangen til finansielle tjenester blir uavhengig av de bankforbindelser respektive kunder har valgt. I BankID er det derfor samme høye grad av samordning som man vil kjenne igjen fra betalingsformidlingsområdet. Også en mer effektiv bankdrift har vært et viktig formål bak næringens satsing på BankID. Det har likevel hele tiden vært bankenes mål at kunder med BankID også skal kunne benytte denne i kommunikasjon med offentlig sektor. Banknæringen har derfor fortløpende tilpasset BankID til stadig nye myndighetskrav.

FNH og Sparebankforeningen har 12.03.07 sendt grunnlag til Post- og teletilsynet (PT) for deklarerer av PersonBankID som Person-Høyt i henhold til Kravspesifikasjon for PKI i offentlig sektor på grunnlag av forskrift om frivillig selvdeklarasjonsordninger for sertifikatutstedere, gitt med hjemmel i esignaturloven § 16a.

På bakgrunn av at bankene har felles regelverk og infrastruktur for PersonBankID, benyttes samme mal for selvdeklarerer som for melding om kvalifisert sertifikat. Det vil si at det som er felles for alle utstederne av PersonBankID er sendt av BankID Samarbeidet til PT, og så må den enkelte utsteder av PersonBankID i tillegg sende inn meldeskjema til PT.

BankID Samarbeidet vil gjennomføre tilsvarende prosess for AnsattBankID i løpet av kort tid.

Allerede nå sier 6 av 10 BankID-brukere at de gjerne vil bruke BankID i elektroniske tjenester fra offentlig sektor. 700 000 privatpersoner har pr mai 2007 BankID og alle hverdager gjennomføres det gjennomsnittlig 250 000 identifiseringer og signeringer. Omfanget og bruken vil øke betydelig når Nordea Bank Norge og DnB NOR Bank i år starter utrulling av BankID til sine personkunder. Sett på bakgrunn av at BankID blir påloggingsmekanismen for mer enn 2,3 millioner nettbankkunder, holder vi det for svært sannsynlig at det vil være nærmere 2 millioner BankID-er i aktiv bruk ved utgangen av 2008. Allerede nå sier 6 av 10 BankID-brukere at de gjerne vil bruke BankID i elektroniske tjenester fra offentlig sektor.

Banknæringen viderefører løpende arbeidet med sikkerhetsløsninger for eID, og søker til enhver tid å ligge i forkant av trusselbildet. Dette vil også det offentlige dra nytte av i sine tjenester.

Rapport 2007-009

**Elektronisk legitimasjon
i Norden**



Elektronisk legitimasjon i Norden

Utarbeidet for
BankID Samarbeidet

Innhold:

SAMMENDRAG OG KONKLUSJONER	1
1 OPPDRAGET	4
2 LEVERANDØRER AV ELEKTRONISK LEGITIMASJON.....	5
2.1 Norge.....	5
2.2 Sverige	6
2.3 Danmark.....	7
2.4 Finland	7
2.5 Samlet oversikt over bruken av elektroniske legitimasjoner	8
3 UTBREDELSE OG BRUKSOMRÅDER	10
3.1 Hvor mange har elektronisk legitimasjon?	10
3.2 Hva er bruksområdene – hvilke tjenester er tilknyttet elektronisk legitimasjon?	11
3.2.1 Brukersteder i Norge.....	11
3.2.2 Brukersteder i Sverige.....	13
3.2.3 Brukersteder i Danmark.....	14
3.2.4 Brukersteder i Finland.....	16
3.2.5 Flest brukersteder for elektronisk legitimasjon i Norge og Danmark.....	17
4 VALG AV STRATEGI FOR UTVIKLING AV ELEKTRONISK LEGITIMASJON DE ULIKE LANDENE	18
4.1 Norge.....	18
4.2 Sverige	21
4.3 Danmark.....	23
4.4 Finland	24
4.5 Forholdet mellom det offentliges strategi og utbredelsen av elektronisk legitimasjon.....	25
VEDLEGG 1: ELEKTRONISK SIGNATUR, ELEKTRONISK LEGITIMASJON OG SERTIFIKATER	27

Sammendrag og konklusjoner

Resymé

Elektronisk ID – elektronisk identitet er en elektronisk form for legitimasjon og signatur. Denne kan særlig benyttes i åpne nett (som Internett) for å bevise at man er den man gir seg ut for å være.

Det finnes ingen oppdatert sammenligning av utbredelse og bruk av PKI-basert¹ elektronisk legitimasjon i de fire nordiske landene Norge, Sverige, Danmark og Finland. BankID Samarbeidet har derfor bedt ECON om å kartlegge utbredelse og bruk samt hvilken strategi myndighetene i de ulike landene har valgt i forhold til bruk av PKI-basert elektronisk legitimasjon.

Utviklingen av elektronisk legitimasjon i de nordiske landene startet allerede på slutten av 1990-tallet. Myndighetene i hvert land har vært sentrale aktører i utviklingen, både for å fastsette krav og retningslinjer, og som etterspørrere av legitimasjoner for bruk i forvaltningen. En viktig forutsetning for at elektronisk legitimasjon skal gi merverdi for brukere og brukersteder, er at det for brukerstedenes er tilstrekkelig mange brukere og for brukerne at det er tilstrekkelig mange brukersteder som aksepterer elektronisk legitimasjon.² Utbredelsen av elektronisk legitimasjon er betydelig større i Norge, Sverige og Danmark enn i Finland. Av brukersteder er det fremdeles offentlig forvaltning og banker som dominerer i alle landene. Få andre private aktører har implementert systemer for elektronisk legitimasjon.

Myndighetene har valgt ulike strategier for å implementere elektronisk legitimasjon. Mens finske myndigheter har forsøkt å bygge opp en egen statlig infrastruktur, har Sverige, Danmark og Norge i større grad basert seg på å utnytte infrastrukturløsninger som er utviklet av andre aktører.

Oppdraget

BankID Samarbeidet i Norge har bedt ECON om å kartlegge status over utbredelse og bruk av PKI-basert (Public Key Infrastructure)³ elektronisk legitimasjon i de nordiske landene (Norge, Sverige, Danmark og Finland) samt hvilken strategi landenes myndigheter har valgt i forhold til bruk av slik elektronisk legitimasjon i offentlig forvaltning.

Følgende hovedpunkter er dekket i rapporten:

- Hovedleverandører av elektronisk legitimasjon i de ulike landene
- Utbredelse og bruksområder for elektronisk legitimasjon i de ulike landene

¹ Public Key Infrastructure. Navnet på infrastrukturen henspiller på den teknologien som ligger til grunn, nemlig offentlignøkkel-kryptografi. Denne teknologien gir muligheter for å vite hvem avsenderen av en elektronisk meddelelse er (*autentisering*), muligheter for å sikre meddelelsen slik at alle forsøk på endringer blir oppdaget (*integritet*), muligheter for å forvrenge innholdet (*kryptere*) slik at det blir uleselig for andre enn mottakeren (*konfidensialitet*) og muligheter for å knytte innholdet til avsenderen slik at hun ikke kan nekte for å stå bak det (*ikke-benektning*). Jf. vedlegg 1.

² Dette kalles ofte nettverkseffekter. Nettverkseffekter eksisterer når en kundes nytte ved å være tilknyttet et nettverk avhenger av hvor mange andre som er tilknyttet nettverket.

³ Jf. fotnote 1 og vedlegg.

- Myndighetenes strategier i forhold til bruk av PKI-basert elektronisk legitimasjon og hvem som har vært pådrivere i de enkelte landene. Basert på funnene har vi kort kommentert forholdet mellom strategi og resultater i form av utbredelse og bruk for de fire utvalgte landene.

Konklusjoner

Utviklingen av elektronisk legitimasjon startet omtrent samtidig i de fire nordiske landene, og i 1999 ble det av EU etablert et rammeverk for elektronisk signatur som de nordiske landene har implementert i sine nasjonale lovverk. Myndighetene i de ulike landene har lagt opp ulike strategier for bruk av elektronisk legitimasjon i samfunnet.

Det er i dag betydelige forskjeller mellom landene når det gjelder hvor langt implementeringen av elektronisk legitimasjon har kommet. I Norge er det i dag i hovedsak to PKI-baserte elektroniske legitimasjoner, BuyPass som eies av Posten og Norsk Tipping og BankID som eies av bankene. I Sverige er det tre PKI-baserte legitimasjoner: BankID, som eies av noen av bankene, Nordeas elektroniske legitimasjon og Telia Sonera/SEBs elektroniske legitimasjon. I Danmark er det bare én, TDC, som har fått i oppdrag i levere PKI-basert elektronisk legitimasjon til det danske folk på den såkalte OCES-standarden. I Finland har myndighetene utviklet det såkalte Borgerkortet som utstedes av Befolkningsregistersentralen (PKI-basert). Gjennom et samarbeid med OKO Bank, TeliaSonera og Elisa, kan den elektroniske legitimasjonen også utstedes på enkelte bankkort og simkort.

Utbredelsen av elektronisk legitimasjon er betydelig større i Norge, Sverige og Danmark enn i Finland. I Norge er det til sammen utstedt og aktivert om lag 2,6 millioner PKI-baserte elektroniske legitimasjoner. 2 millioner av disse er levert av BuyPass⁴ til 1,8 millioner brukere og 630.000 BankID-legitimasjoner er levert av bankene. Norge er samtidig det landet med flest internettbaserte brukersteder for elektronisk legitimasjon. Brukerstedene er i stor grad banker og offentlige myndigheter. I Sverige er det utstedt 1,3 millioner elektroniske legitimasjoner, i Danmark 750.000 og i Finland 100.000. Brukerstedene i Sverige er tilsvarende som Norge i stor grad banker og offentlig forvaltning. I Danmark kan den PKI-baserte OCES-løsningen nesten utelukkende benyttes i det offentlige, og det samme gjelder for Borgerkortet i Finland.

Når det gjelder den faktiske bruken av elektronisk legitimasjon er det vanskelig å finne tall for dette, fordi leverandørene av elektronisk legitimasjon ofte enten ser på dette som forretningshemmeligheter eller ikke fører statistikk for bruken. Det gjennomføres hver dag rundt 200.000 transaksjoner på internett med norske BankID-legitimasjoner, 130.000 med BuyPass-legitimasjoner og 70.000 med svenske BankID-legitimasjoner.⁵

I tabellen nedenfor er navn på legitimasjoner, leverandører, antall brukere og gjennomsnittlig bruk i Norge, Sverige, Danmark og Finland oppsummert.

⁴ Vi har ikke tall for hvor mange av BuyPass-legitimasjonene som faktisk brukes på Internett, fordi slik bruk krever at det i tillegg er installert kortleser på maskinen. BuyPass har av forretningshensyn ikke ønsket å gi ECON opplysninger om antall installerte kortlesere.

⁵ Tall for de øvrige elektroniske legitimasjonene er ikke oppgitt.

Tabell A Oppsummering PKI-baserte elektroniske legitimasjoner, leverandører, antall brukere og gjennomsnittlig daglig bruk i Norge, Sverige, Danmark og Finland

Land	Legitimasjon	Leverandør	Antall brukere	Daglig bruk
Norge	BankID (kvalifisert)*	Bankene i Norge	630.000	200.000
	BuyPass (kvalifisert)*	BuyPass (som eies av Norsk Tipping og Posten)	**	130.000
Sverige	BankID	Swedbank, Handelsbanken, Ikanobanken, Danske Bank i Sverige, Länsförsäkringar bank, Skandiabanken, Sparbanken Finn og Sparbanken Gripen	700.000	70.000
	Nordeas legitimasjon	Nordea	260.000 40.000 smartkort	ikke oppgitt
	TeliaSonera/SEBs legitimasjon	TeliaSonera/SEB	200.000, 50.000 smartkort	ikke oppgitt
Danmark	OCES	IT- og Telestyrelsen (outsourcet til TDC)	750.000	ikke oppgitt
Finland	Borgerkortet (kvalifisert)*	Befolkningsregistersentralen	123.000 smartkort	ikke oppgitt

Note: *=Med kvalifisert mener vi kvalifisert i henhold til e-signaturlovgivningen.

**=Det er i følge BuyPass utstedt 2 millioner BuyPass-legitimasjoner til 1,8 millioner brukere, men det er ikke kjent for oss hvor mange som faktiske benyttes på Internett. Tall for BuyPass er derfor ikke oppgitt i tabellen.

Finske myndigheter ser ut til å ha valgt en strategi som har vært mindre effektiv enn de andre landene for å oppnå kritiske masser av brukere og brukersteder for elektronisk legitimasjon. Myndighetene har valgt å etablere en ny infrastruktur fremfor å utnytte en allerede eksisterende. Dette har medført en betydelig ekstrakostnad for å få utstedt elektronisk legitimasjon i form av tidsbruk til fysisk oppmøte hos opp til flere instanser, samt kostnader knyttet til å få installert smartkortleser på brukernes datamaskiner. Når i tillegg antall tjenester som elektronisk legitimasjon kan benyttes på er begrenset, har trolig kostnaden for mange finske borgere vært større enn nytten ved å ha en elektronisk legitimasjon.

I Norge, Sverige og Danmark har myndighetene i større grad basert seg på å bruke eksisterende infrastruktur utviklet i markedet. Landene har likevel valgt litt ulike strategier når det gjelder å utnytte infrastrukturen. Mens svenske myndigheter har inngått rammeavtale med alle leverandørene av elektronisk legitimasjon som har tilfredsstilt en ikke spesielt detaljert kravspesifikasjon, har danske myndigheter utformet en mer detaljert kravspesifikasjon og valgt kun én leverandør av elektronisk legitimasjon. I Norge er det for tiden ingen sentral rammeavtale for PKI-basert elektronisk legitimasjon.

1 Oppdraget

Allerede i 1999 etablerte EU et rammeverk for elektronisk signatur.⁶ En rekke land i Europa, herunder Norge⁷, Sverige⁸ og Finland⁹ har implementert dette EU-direktivet i det nasjonale lovverket.

Det finnes ingen oppdatert kartlegging av utbredelse og bruk av PKI-basert (Public Key Infrastructure) elektronisk legitimasjon i et sammenlignende perspektiv for de fire nordiske landene Norge, Sverige, Danmark og Finland. BankID Samarbeidet har derfor bedt ECON om å kartlegge utbredelse og bruk samt hvilken strategi myndighetene i de ulike landene har valgt i forhold til bruk av PKI-basert elektronisk legitimasjon.

Vi har i prosjektet samlet tilgjengelig informasjon på Internett og gjennomført en rekke intervjuer. Vi har snakket med representanter fra relevante myndigheter i de fire landene om det offentlige strategi for utbredelse av elektronisk legitimasjon, i tillegg til de største leverandørene av elektronisk legitimasjon. Dokumentasjonen i denne rapporten er basert på de innhentede opplysningene.

For Danmark og Sverige har vi også kort beskrevet to elektroniske legitimasjoner som ikke er PKI-baserte. Disse legitimasjonene er imidlertid ikke inkludert i samstillingen av informasjon om PKI-baserte elektroniske legitimasjoner på tvers av landegrensene.

⁶ Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf

⁷ LOV 2001-06-15 nr 81: Lov om elektronisk signatur (esignaturloven)
<http://www.lovdata.no/all/hl-20010615-081.html>

⁸ Lag (2000:832) om kvalificerade elektroniska signaturer
http://rixlex.riksdagen.se/htbin/thw?%24%7BOOHTML%7D=SFST_DOK&%24%7BSNHTML%7D=SFSTR_ERR&%24%7BBASE%7D=SFST&BET=2000%3A832&%24%7BTRIPSHOW%7D=format%3DTHW

⁹ Laki sähköisistä allekirjoituksista 24.1.2003/14 (Lov om elektroniske signaturer 24.1.2003/14)
<http://www.finlex.fi/fi/laki/ajantasa/2003/20030014>

2 **Leverandører av elektronisk legitimasjon**

Leverandører av elektronisk legitimasjon i Norge, Sverige, Danmark og Finland er først og fremst banker og teleselskaper. Noen av disse leverer legitimasjoner som er kvalifiserte i henhold til e-signaturlovgivningen, mens andre leverer legitimasjoner som ikke er det.

I det følgende skal vi se nærmere på de ulike elektroniske legitimasjonene i de nordiske landene.

2.1 **Norge**

I Norge er det i hovedsak to PKI-baserte elektronisk legitimasjoner, BankID og BuyPass.¹⁰ Begge disse er registrert hos Post- og teletilsynet som kvalifiserte sertifikater i henhold til e-signaturloven.

Det er per 1. januar 2007 utstedt BankID til 630.000 bankkunder i Norge, og ifølge BankID Samarbeidet vil de fleste nettbankkunder ha fått tilbud om elektronisk legitimasjon i løpet av 2007. BuyPass oppgir at de har utstedt 2 millioner aktiverte elektroniske legitimasjoner i smartkort og mobil.¹¹ For at smartkortene kan benyttes på Internett, må det imidlertid også installeres en kortleser på datamaskinen som benyttes. En oversikt over antallet kortlesere vil kunne indikere hvor mange som kan være direkte brukere av kortet fra egen datamaskin. Vi har ikke hatt tilgang på antallet installerte kortlesere.

Det pågår dessuten en diskusjon hos myndighetene om en elektronisk legitimasjon som fungerer som et nasjonalt elektronisk identitetskort/Schengen-pass.

BankID

Banknæringen har utviklet BankID til bruk på Internett, både for sikker identifisering og signering. Legitimasjonen kan brukes for å bevise brukerens identitet og til personlig elektronisk signatur i nettbank, ved nettbetaling, ved handel, bruk av offentlige tjenester eller inngåelse av avtaler på nett.

Det finnes tre varianter: PersonBankID er en personlig elektronisk legitimasjon som banken utsteder til personkunder, AnsattBankID er en personlig elektronisk legitimasjon som i tillegg knytter den fysiske personen til en privat eller offentlig virksomhet, samt BrukerstedsBankID som er en virksomhetslegitimasjon.

Det gjennomføres rundt 200.000 BankID-identifiseringer og -signeringer på internett hver dag.

¹⁰ En fullstendig oversikt over registrerte tilbydere av kvalifiserte elektroniske legitimasjoner finnes på www.npt.no.

¹¹ Administrerende direktør Gunnar Lindstøl i BuyPass oppgir til ECON 4. januar 2007 at selskapet per 31. desember 2006 har utstedt ca 2 millioner legitimasjoner på smartkort og mobil fordelt på ca 1,8 millioner personer. Alle disse legitimasjoner oppgis å være aktiverte for bruk på Internett.

BuyPass

BuyPass tilbyr både ID-tjenester, betalingstjenester og såkalte bedriftstjenester. ID-tjenestene i BuyPass Nett benytter elektronisk legitimasjon for identifisering, elektronisk signering og informasjonsutveksling. Den elektroniske legitimasjonen ligger lagret på et smartkort eller i en mobiltelefon.

Betalingstjenestene i BuyPass Nett brukes til betaling over Internett og mobil, og sikres gjennom bruk av elektronisk legitimasjon. Betaling gjennomføres med BuyPasskonto som er basert på bruk av elektronisk penger (elektroniske kontanter). Brukerne kan via internett og mobil overføre elektroniske penger til og fra BuyPasskontoen. Til bedrifter tilbyr BuyPass personalisert smartkort hvor elektronisk legitimasjon kan installeres.

BuyPass-smartkortet kan også benyttes til spill hos Norsk Tippings kommisjonærer, gjerne butikker og kiosker.

2.2 Sverige

I Sverige utstedes elektronisk legitimasjon av banker og Telia. Disse tilbyr til sammen tre forskjellige legitimasjoner, *BankID*, *Nordeas elektroniske legitimasjon* og *Telias elektroniske legitimasjon*. I tillegg til disse har også Steria rammeavtale med det offentlige, men Sterias tjeneste er ikke i bruk.¹² Ingen av legitimasjonene i Sverige er kvalifiserte i henhold til e-signaturlovgivningen.

Per oktober 2006 er det utstedt til sammen 2 millioner elektroniske legitimasjoner og antall legitimasjoner som er aktivert for bruk i e-handel er til sammen 1,2 millioner.¹³ Det er registrert rundt 700.000 aktive BankID-brukere i Sverige.¹⁴

I tillegg til *BankID*, *Nordeas legitimasjon* og *Telias legitimasjon* finnes det et nasjonalt elektronisk identitetskort/Schengen-pass i Sverige. Dette blir utstedt av politiet, og 25.000 svensker hadde skaffet seg et slikt pass etter ett år i produksjon. Dette identitetskortet kan imidlertid foreløpig ikke brukes i forbindelse med e-handel.

Det er kun tre banker i Sverige (Sparbanken Finn, Ikanobanken og Sparbanken Gripen) som har tatt i bruk BankID i egen nettbank, men Handelsbanken har planer om å ta det i bruk i 2007. Derimot har statlige, offentlige nettsider og aktører som Handelsbanken Finans tatt BankID i bruk. Det er fullt mulig for en bedrift/organisasjon å godta alle de forskjellige elektroniske legitimasjonene. De fleste offentlige etater godtar både BankID, Nordeas og Telias legitimasjon.

På månedsbasis er det i snitt 2 millioner BankID-transaksjoner i Sverige. Det betyr i underkant av 70.000 pr dag.¹⁵

¹² Steria er nevnt som leverandør i Sverige i statusrapporten fra det 10. møte i Porvoo-gruppen, 2-3 november 2006. [http://www.vaestorekisterikeskus.fi/vrk/files.nsf/files/4036B970E0CAA61BC2257219004E5639/\\$file/Summary_of_the_country_updates.doc](http://www.vaestorekisterikeskus.fi/vrk/files.nsf/files/4036B970E0CAA61BC2257219004E5639/$file/Summary_of_the_country_updates.doc)

¹³ Kilde: Statusrapport fra det 10. møte i Porvoo-gruppen, 2-3 november 2006. [http://www.vaestorekisterikeskus.fi/vrk/files.nsf/files/4036B970E0CAA61BC2257219004E5639/\\$file/Summary_of_the_country_updates.doc](http://www.vaestorekisterikeskus.fi/vrk/files.nsf/files/4036B970E0CAA61BC2257219004E5639/$file/Summary_of_the_country_updates.doc)

¹⁴ Kilde: Johan Eriksson, VD i Finansiell ID-Teknik BID AB i Sverige, som har samme oppgave som BankID Samarbeidet i Norge.

Nordea i Sverige har utstedt i underkant av 260.000 softwarebaserte elektroniske legitimasjoner og i underkant av 40.000 på kort.¹⁶ TeliaSonera har utstedt rundt 200.000 softwarebaserte elektroniske legitimasjoner og rundt 50.000 på kort.¹⁷

2.3 Danmark

I Danmark er det to elektroniske legitimasjoner. Den ene er utviklet i regi av danske myndigheter (IT- og Telestyrelsen) og kalles OCES (Offentlige Certifikater til Elektronisk Service). Dette er en PKI-basert legitimasjon som eies og forvaltes av staten, men er outsourcet til TDC (teleselskap). Den andre er utviklet av bankene og kalles NetID. NetID er ikke PKI-basert sett fra brukernes side, men bankene signerer på vegne av kunden. Det er PBS (Payment Business Services) i Danmark som selger NetID til brukerstedsmarkedet. Begge legitimasjonene er softwarebaserte. Ingen av legitimasjonene i Danmark er kvalifiserte i henhold til e-signaturlovgivningen.

Per november 2006 er det utstedt 750.000 elektroniske legitimasjoner på OCES-standard.¹⁸ OCES kan benyttes på en lang rekke offentlige nettsteder, mens NetID bare kan brukes i enkelte banker og noen få offentlige nettsteder. Offentlige nettsteder som aksepterer NetID, aksepterer også OCES.

2.4 Finland

I Finland er det to elektronisk legitimasjoner, et smartkort som Befolkningsregistersentralen utsteder og en som bankene står bak, Tupas. Den siste legitimasjonen er imidlertid ikke PKI-basert.

Borgerkortet

Den elektroniske legitimasjonen som Befolkningsregistersentralen i Finland utsteder, kalles "borgerkortet". Denne legitimasjonen kan utstedes som et rent identitetskort, ligge i et bankkort eller i sim-kortet på mobiltelefonen.

Hele statsforvaltningen i Finland skal ta i bruk borgerkortet som identitetskort med elektronisk legitimasjon, og i dag er det rundt 22.000 kort i bruk. I tillegg til rene ID-kort kan borgerkortet utstedes på Visa Electron kort fra OP Bank Group/OKO Bank og på simkort fra TeliaSonera Finland Oyj og Elisa Corporation.

OKO Bank har inngått avtale med Befolkningsregistersentralen om å utstede legitimasjonen på bankkort. Kunden kan dermed få bankkort med elektronisk legitimasjon ved å møte fysisk opp i banken og identifisere seg med pass eller andre identifikasjonspapirer. For å få legitimasjonen på et simkort må imidlertid kunden først møte fysisk hos et av teleselskapenes utsalgssteder. Deretter må kunden gå til den lokale politistasjonen med identifikasjonspapirer for å få aktivert legitimasjonen, fordi teleselskapene ikke har noen avtale med Befolkningsregistersentralen om å utstede selve legitimasjonen.

¹⁵ Kilde: Johan Eriksson, VD i Finansiell ID-Teknik BID AB i Sverige, som har samme oppgave som BankID Samarbeidet i Norge.

¹⁶ Kilde: Nordea Sverige, Niclas Westen.

¹⁷ Kilde: TeliaSonera, Cristine Karlsson.

¹⁸ Kilde: www.digitalsignatur.dk

Befolkningsregistersentralens borgerkort er PKI-basert, og den eneste elektroniske legitimasjonen i Finland som oppfyller kravene til kvalifisert sertifikat i loven om elektroniske signaturer. Kortene er også godkjent som identitetskort i Europa. Totalt er det per oktober 2006 utstedt 123.000 elektroniske ID-kort i Finland, og 104.000 av disse er aktiverte.

Det er nesten hundre forskjellige tjenester tilgjengelige for bruk av PKI-baserte elektroniske legitimasjoner i Finland, både innenfor bank, e-handel og offentlige tjenester. Tjenestene er i stor grad knyttet til innlevering av søknader og til å hente ut informasjon om pensjonsrettigheter. Nylig ble det besluttet at PKI-legitimasjon skal kunne benyttes som en prøveordning ved kommunevalget i 2008.¹⁹

Det relativt begrensede antallet borgerkort som til nå er utstedt i Finland, begrenser interessen fra bedrifter av å implementere systemer for å håndtere elektronisk legitimasjon. Dette gjør det igjen mindre interessant for brukerne å skaffe seg borgerkortet. Mulighetene for å subsidiere borgerkortet fra myndighetenes side har blitt debattert i Finland, og det er foreslått at borgerkortet skal utstedes gratis i 2008.

Tupas

Tupas kan både benyttes i banker for å utføre banktjenester, og for å signere dokumenter hos bedrifter som har inngått en avtale med Tupas om dette. Tupas er imidlertid, som nevnt, tilsvarende som NetID i Danmark ikke en kvalifisert, PKI-basert legitimasjon.

Banker som er med i Tupas-samarbeidet er Handelsbanken, Nordea Bank Finland, OP Bank Group (OKO Bank), Sampo Bank, sparebanker og lokale andelsbanker, Tapiola Bank og Bank of Åland.²⁰

2.5 Samlet oversikt over bruken av elektroniske legitimasjoner

I Tabell 2.1 nedenfor har vi laget en oversikt over de PKI-baserte elektroniske legitimasjonene som er i bruk i Norge, Sverige, Danmark og Finland, med tilhørende leverandører, antall brukere og gjennomsnittlig bruk.

¹⁹ Kilde: Statusrapport fra det 10. møte i Porvoo-gruppen, 2-3 november 2006.
[http://www.vaestorekisterikeskus.fi/vrk/files.nsf/files/4036B970E0CAA61BC2257219004E5639/\\$file/Summary_of_the_country_updates.doc](http://www.vaestorekisterikeskus.fi/vrk/files.nsf/files/4036B970E0CAA61BC2257219004E5639/$file/Summary_of_the_country_updates.doc)

²⁰ Kilde: Bankforeningen i Finland: Banks' Tupas Certification Service for Service Providers,
<http://www.pankkiyhdistys.fi/sisalto/upload/pdf/tupasV21eng.pdf>

Tabell 2.1 Oppsummering PKI-baserte elektroniske legitimasjoner, leverandører, antall brukere og gjennomsnittlig bruk per dag i Norge, Sverige, Danmark og Finland

Land	Legitimasjon	Leverandør	Antall brukere	Daglig bruk
Norge	BankID (kvalifisert)*	Bankene i Norge	630.000	200.000
	BuyPass (kvalifisert)*	BuyPass (som eies av Norsk Tipping og Posten)	**	130.000
Sverige	BankID	Swedbank, Handelsbanken, Ikanobanken, Danske Bank i Sverige, Länsförsäkringar bank, Skandiabanken, Sparbanken Finn og Sparbanken Gripen	700.000	70.000
	Nordeas legitimasjon	Nordea	260.000 40.000 smartkort	ikke oppgitt
	TeliaSonera/SEBs legitimasjon	TeliaSonera/SEB	200.000, 50.000 smartkort	ikke oppgitt
Danmark	OCES	IT- og Telestyrelsen (outsourcet til TDC)	750.000	ikke oppgitt
Finland	Borgerkortet (kvalifisert)*	Befolkningsregistersentralen	123.000 smartkort	ikke oppgitt

Note: *=Med kvalifisert mener vi kvalifisert i henhold til e-signaturlovgivningen.

**=Det er i følge BuyPass utstedt 2 millioner BuyPass-legitimasjoner til 1,8 millioner brukere, men det er ikke kjent for oss hvor mange som faktiske benyttes på Internett. Tall for BuyPass er derfor ikke oppgitt i tabellen.

Kilde: Statusrapport fra det 10. møte i Porvoo-gruppen, 2-3 november 2006.

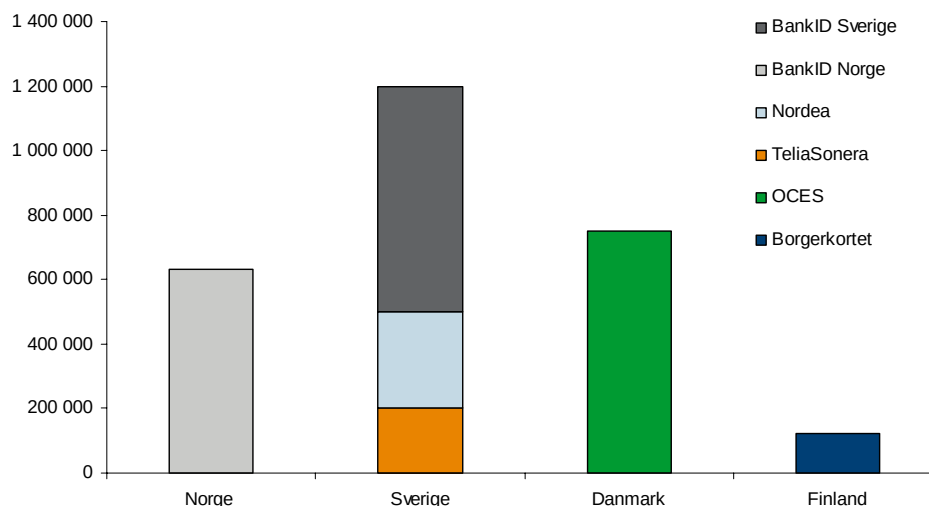
[http://www.vaestorekisterikeskus.fi/vrk/files.nsf/files/4036B970E0CAA61BC2257219004E5639/\\$file/Summary_of_the_country_updates.doc](http://www.vaestorekisterikeskus.fi/vrk/files.nsf/files/4036B970E0CAA61BC2257219004E5639/$file/Summary_of_the_country_updates.doc), BankID i Sverige, Nordea Sverige (Nicklas Westen, desember 2006), TeliaSonera (Cristine Karlsson, desember 2006), Buypass (Gunnar Lindstøl, januar 2007), www.bankid.no, www.digitalsignatur.dk, www.fineid.fi, www.fba.fi, www.buypass.no, www.e-legitimation.se, Peter Fjelbye i PBS i Danmark

3 Utbredelse og bruksområder

3.1 Hvor mange har elektronisk legitimasjon?

Antall utstedte og aktiverte PKI-baserte elektroniske legitimasjoner varierer mellom landene. I Figur 3.1 har vi laget en oversikt over dette.

Figur 3.1 *Antall utstedte PKI-baserte elektroniske legitimasjoner*²¹



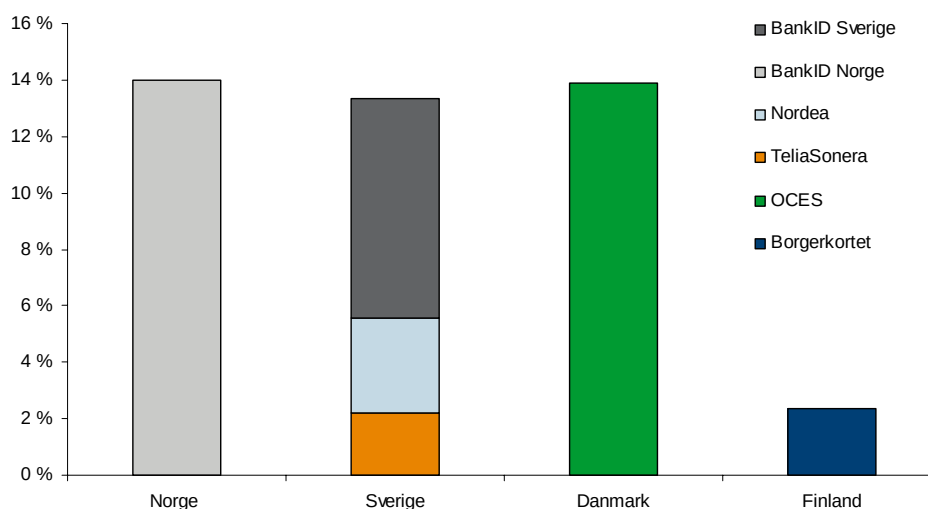
Kilde: De respektive leverandørene

Når det gjelder BuyPass i Norge vet vi som sagt ikke hvor mange av legitimasjonene som er i bruk på Internett, og vi har derfor ikke inkludert dette i figuren. Hvis vi ser bort fra BuyPass, er Sverige det landet med flest brukere av PKI-basert elektronisk legitimasjon, foran Danmark. Finland med sitt Borgerkort er det landet som har færrest brukere av PKI-basert elektronisk legitimasjon.

Hvis vi ser på antallet elektronisk legitimasjoner som andel av befolkningen, ligger Norge, Sverige og Danmark relativt likt med 13-14 prosent, mens Finland bare har utstedt legitimasjoner tilsvarende 2 prosent av befolkningen. I Figur 3.2 nedenfor har vi illustrert dette.

²¹ Tall for BuyPass-legitimasjoner er ikke med fordi vi ikke vet hvor mange av BuyPass 2 millioner utstedte smartkort som er i bruk på Internett, jf. avsnitt 2.1.

Figur 3.2 *Antall utstedte elektroniske legitimasjoner i andel av befolkningen*



Kilde: De respektive leverandørene og SSB

3.2 **Hva er bruksområdene – hvilke tjenester er tilknyttet elektronisk legitimasjon?**

I de følgende avsnittene har vi laget oversikter over brukerstedene for de ulike løsningene for elektronisk legitimasjon i Norge, Sverige, Danmark og Finland. Omtalen viser kun informasjon om de PKI-baserte elektroniske legitimasjonene.

3.2.1 **Brukersteder i Norge**

I Norge er det som nevnt to ulike PKI-baserte elektroniske legitimasjoner, BankID og BuyPass.

BankID kan benyttes i de fleste nettbankene i Norge i tillegg til enkelte kommuner og nettbutikker. I Tabell 3.1 er en oversikt over brukerstedene for BankID.

Tabell 3.1 Brukersteder BankID i Norge

Andebu Sparebank	Indre Sogn Sparebank	SpareBank 1 Lom og Skjåk
Ankenes Sparebank	Jernbanepersonalets Sparebank	SpareBank 1 Midt-Norge
Arendal og Omegns Sparekasse	Klepp Sparebank	SpareBank 1 Nord-Norge
Askim kommune	KLP	Sparebank 1 Nordvest
Askim Sparebank	Klæbu Sparebank	SpareBank 1 Ringerike
Aurland Sparebank	Komplett.no	SpareBank 1 SR-Bank
Aurskog Sparebank	Kolumbus	SpareBank 1 Vestfold
Bamble og Langesund Sparebank	Kragerø Sparebank	SpareBank 1 Volda Ørsta
Bank2	Kvinesdal Sparebank	Sparebanken Bien
BankID Samarbeidet (begrenset brukergruppe)	Larvikbanken Brunlanes Spb.	Sparebanken Grenland
BankID-verktøy	Leksvik kommune	Sparebanken Hedmark
Berg Sparebank	Lillestrøm Sparebank	Sparebanken Hemne
Birkenes Sparebank	Lofoten Sparebank	Sparebanken Telespar
Bjugn kommune	Marker Sparebank	Spareskillingsbanken
Bjugn Sparebank	Meldal Sparebank	Spydeberg kommune
Blaker Sparebank	Melhus Sparebank	Spydeberg Sparebank
Boing-klubben	Modum SpareBank 1	Stadsbygd Sparebank
Bud Fræna og Hustad Sparebank	Mosvik kommune	Stavanger kommune
Bø Sparebank	Narvik Sparebank	Strømmen Sparebank
Deal.no	Nes Prestegjelds Sparebank	Sunnadal Sparebank
DnB NOR (pilotbrukere)	Nesset Sparebank	Surnadal Sparebank
Drangedal og Tørdal Sparebank	Nore og Uvdal kommune	Time Sparebank
Eidsberg Sparebank	Nøtterø SpareBank 1	Tinn Sparebank
eServicetorget i Numedal	Odal Sparebank	Tjeldsund Sparebank
Etmedal Sparebank	Ofoten Sparebank	TL-klubben
Evje og Hornnes Sparebank	Oppdalsbanken	Tolga- Os Sparebank
Fana Sparebank	Orkdal Sparebank	Totens Sparebank
Fjaler Sparebank	Osen kommune	Transportstøttetjenesten (Innovasjon Norge)
Flesberg kommune	Pennyklubben	Trøgstad Sparebank
Fokus Bank	Pensjonsrett.no	Tysnes Sparebank
Fosenportalen	Rindal Sparebank	Valle Sparebank
GE Money Bank	Rissa kommune	Vang Sparebank
Gjerpen og Solum Sparebank	Roan kommune	Vegårshei Sparebank
Gjerstad Sparebank	Rollag kommune	Verran Sparebank
Grong Sparebank	Rygge-Vaaler Sparebank	Vestre Slidre Sparebank
Grue Sparebank	Rørosbanken Røros Sparebank	Vik Sparebank
Halden SpareBank 1	Selbu Sparebank	Voss Sparebank
Haltdalen Sparebank	Seljord Sparebank	yA Bank og Forsikring
Harstad Sparebank	Setskog Sparebank	Ørland kommune
Hjartdal og Gransherad Spb.	Soknedal Sparebank	Ørland Sparebank
Hjelmeland Sparebank	SpareBank 1 Gran	Ørskog Sparebank
Hobøl kommune	SpareBank 1 Gudbrandsdal	Øystre Slidre Sparebank
Hol Sparebank	SpareBank 1 Hallingdal	Åfjord kommune
Holla og Lunde Sparebank	SpareBank 1 Jevnaker	Åfjord Sparebank
Høland Sparebank	SpareBank 1 Jevnaker	Aasen Sparebank
Hønefoss Sparebank	SpareBank 1 Kongsberg	

Kilde: www.bankid.no februar 2007

BuyPass kan ikke benyttes i banker, men på brukerstedene listet opp i Tabell 3.2.

Tabell 3.2 Brukersteder BuyPass

Komplett.no
Norsk Tipping
KLP Forsikring
Oppdal kommune
Stavanger kommune
Advokatoppgjør as
Lånekassen
Skatteetaten
Statistisk sentralbyrå
Brønnøysundregistrene
Konkurransetilsynet
Kredittilsynet
Fiskeri- og Kystdepartementet
Norges Bank
Økokrim
Produktregisteret
Statens Innkrevingssentral
Statens Landbruksforvaltning

Note: Gunnar Lindstøl i BuyPass oppgir i januar 2007 at antall tjenestesteder på internett er flere enn det som kommer frem på Buypass.no. Han sier at BuyPass kan benyttes på 47 brukersteder. Vi har imidlertid ikke noen oversikt over disse brukerstedene.

Kilde: www.buypass.no november 2006

3.2.2 Brukersteder i Sverige

De fleste offentlige etatene i Sverige som godtar elektronisk legitimasjon, godtar både BankID, Nordeas elektroniske legitimasjon og TeliaSonera/SEBs. I Tabell 3.3 er en oversikt over alle brukerstedene i Sverige.

Tabell 3.3 Oversikt over alle brukersteder i Sverige

Apoteket AB	LIC och Sparbanken Finn
Bolagsverket	Länsstyrelsen Stockholm
CSN	Nacka kommun
Energimyndigheten	Pensionsbolag/staten
Finansinspektionen	SBAB
Försäkringskassan	Skatteverket
GE Money Bank	Sparbanken Finn
Handelsbanken Finans	Sparbanken Gripen
Ikanobanken	Stockholms läns landsting
Itella	Svensk Adressändring AB
Jordbruksverket	Umeå kommun
Komplett.se	Vaggeryds kommun
Lantmännen	Vägverket

Kilde: www.e-legitimation.se november 2006.

3.2.3 Brukersteder i Danmark

I Danmark er det én PKI-basert elektronisk legitimasjon, nemlig det offentliges OCES som er outsourcet til TDC.

I Tabell 3.4 er en oversikt over brukerstedene for OCES.

Tabell 3.4 Brukersteder OCES

3F	Handelshøjskolen i Århus	Optagelse.dk
Alm. Brand	Hashøj kommune	PensionDanmark
Arbejdsformidlingen i Danmark - Jobnet	Helsinge Kommune	PensionsInfo
Arbejdsskadestylens og Arbejdstilsynets Elektroniske Anmeldesystem	Helsingør kommune	PKA
ATP	Herlev kommune	Purhus kommune
Ballerup kommune	Herning Kommune	Randers kommune
Billund Kommune	Hobro Kommune	Ringsted kommune
BorgerWeb	Holbæk kommune	Rosenholm kommune
BRF Kredit	Hvalsø kommune	Roskilde kommune
Brønderslev Kommune	Hvidovre kommune	Rougsø kommune
Danmarks Tekniske Universitet - CampusNet	Hørsholm Kommune	Rødby kommune
Den Kgl. Veterinær- og Landbohøjskole	IAK	Salon Hair
Den offentlige informationsserver	Industriens pension	Skandiabanken
Det centrale personregister, CPR-kontoret	Ingeniørhøjskolen i København	Skat
Det kongelige bibliotek	Ingeniørhøjskolen i Odense Teknikum	Sorø kommune
digte.dk	Ingeniørhøjskolen i Århus	Studielaan.dk
Domæneadministration DynDNS Pro	InterResearch A/S	SU
Dragsholm kommune	JØP Pension	Sundhed.dk
Dronninglund kommune	Kerteminde Kommune	Sundhedsstyrelsen
Ebeltoft kommune	Klasselotteriet	Sygeforsikring danmark
eBoks	Kolding kommune	Sæby kommune
ePosthuset	Kristelig Fagbevægelse	Søllerød kommune
Esbjerg kommune	Københavns kommune	Sønderhald kommune
FerieKonto	Lemvig kommune	TDC online
Fredericia kommune	Lunderskov Kommune	Telmore
Frederiksberg kommune	Lyngby Taarbæk Kommune	Trundholm kommune
Frederikshavn kommune	Lønmodtagernes Dyrtidsfond	Tårnby kommune
Frederiksværk kommune	Medicinprofilen	Vejle Kommunes Musikskole
Fuglebjerg kommune	NemKonto	Viborg amt
Gentofte Kommune	Netborger.dk	Aabybro Kommune
Gladsaxe kommune	Nibe Kommune	Aalborg kommune
Glostrup Kommune	Odder kommune	Aarhus kommune
Hammel kommune	Odense kommune	Århus Kommunes Biblioteker

Note: Oversikten viser de brukerstedene som tilbyr selvbetjening ved bruk av digital signatur. En lang rekke brukersteder som ikke er med i oversikten tilbyr "sikker e-post", men ikke selvbetjening.

Kilde: www.digitalsignatur.dk november 2006

3.2.4 Brukersteder i Finland

I Finland er det én PKI-basert elektronisk legitimasjon, Borgerkortet. I Tabell 3.5 er en oversikt over brukersteder i Finland for Borgerkortet.

Tabell 3.5 *Brukersteder for Borgerkortet*

Nettsted	Tjeneste
http://patent.prh.fi	Patentsøknader
http://www.aina.fi/	Diverse tjenester
http://www.fennia.fi/	Forsikringstjenester
http://www.lappeenranta.fi/	Søknadshjelp
http://www.mela.fi/	Pensjon landbruk
http://www.milnet.fi/	Forsvaret
http://www.muuttoilmoitus.fi/	Flyttemelding
http://www.op.fi/	Banktjenester
http://www.plussa.com/	Transaksjoner Plussa-kort
http://www.tyvi.org/	Rapportering til offentlige myndigheter
https://www.palkka.fi/	Beregning av lønnskostnader mv.
https://www.verkkoposti.com/e3/Identification	Posttjenester
Loki Service	Pensjon sjømenn
Varma's Elakearvio service	Beregning av pensjon
www.etu-klubi.fi	Informasjon om tjenester knyttet til borgerkortet
www.fennia.fi/fennia/index.html	Pensjonsrettigheter
www.fineid.fi	e-legitimasjon
www.kela.fi	Studentinformasjon og velferdstjenester
www.keva.fi	Pensjon kommuneansatte
www.lomake.fi	Utfylling av offentlige skjemaer
www.mol.fi	Jobbsøkertjenester og søknad voksenopplæring
www.sahkoinenreissuvihko.fi	Kontakt hjem-skole/barnehage
www.tampere.fi	Innsending av forslag til kommunen
www.tekes.fi/rahoitus	Søknad om støtte til forskning og produktutvikling
www.tyoelake.fi	Pensjonsrettigheter
www.vaestorekisterikeskus.fi	Befolkningsregistret
www.vantaa.fi	Søknad om sosialstøtte
www.verkkomummo.fi	Elektronisk møteplass for barn

Kilde: www.fineid.fi

3.2.5 Flest brukersteder for elektronisk legitimasjon i Norge og Danmark

Når vi summerer antall internettbaserte brukersteder for elektronisk legitimasjon i de fire landene, ser vi at Norge er på topp med nesten 130 brukersteder for BankID og i underkant av 20 brukersteder for BuyPass.²² Danmark er nummer 2 med i overkant av 100 brukersteder for OCES.

Det er forskjeller i type brukersteder i Norge og Danmark. Mens legitimasjonen med flest brukersteder i Norge, nemlig BankID, per i dag hovedsaklig kan benyttes i banker, kan OCES i Danmark nesten utelukkende benyttes i forhold til offentlige tjenester. I Sverige kan både Telias, Nordeas og BankIDs løsninger benyttes på de samme brukerstedene, og dette er stort sett i det offentlige.

I Finland kan borgerkortet i all hovedsak benyttes for å legitimere seg på det offentliges brukersteder. Det er imidlertid én bank, OKO Bank, som aksepterer borgerkortet.

I neste kapittel beskriver vi nærmere de ulike strategiene myndighetene har valgt for utviklingen av elektronisk legitimasjon i de ulike landene.

²² Gunnar Lindstøl i BuyPass oppgir i januar 2007 at antall tjenestesteder på internett er flere enn det som kommer frem på Buypass.no. Han sier at BuyPass kan benyttes på 47 brukersteder. Vi har imidlertid ikke noen oversikt over disse brukerstedene, jf. Tabell 3.2.

4 Valg av strategi for utvikling av elektronisk legitimasjon de ulike landene

Vi har gjennomført intervjuer med sentrale myndighetspersoner i Norge, Sverige, Danmark og Finland. Intervjuene er gjennomført per telefon i perioden november 2006-januar 2007. Målet med intervjuene har vært å kartlegge hvilken strategi som er valgt i forhold til bruk av elektronisk legitimasjon i de ulike landene i Norden.

Spørsmålene vi tok utgangspunkt i var følgende:

1. Hvilken strategi myndighetene i de ulike landene har valgt for utvikling av elektronisk legitimasjon:
 - a. Hvordan har prosessen vært i de ulike landene i forhold til utviklingen av elektronisk legitimasjon?
 - b. Hvilke føringer har myndighetene lagt i forhold til utviklingen av elektronisk legitimasjon?
 - i. Grad og type av offentlig styring, det offentliges rolle?
 - ii. Grad av offentlig utvikling, offentlig-privat samarbeid, bruk av markedsløsninger, konkurranseperspektiver
 - iii. Eventuelt motivasjon eller begrunnelse for de veivalgene som er gjort
2. Hvem som har vært pådrivere i utviklingen i de enkelte landene:
 - a. Er det offentlige eller private aktører som har ledet an i utviklingen?

I det følgende er informasjonen fra disse intervjuene referert.

4.1 Norge

I Norge har man i det offentlige jobbet med utviklingen av digital legitimasjon helt siden 1996.²³ Utgangspunktet for dette arbeidet var å effektivisere saksbehandlingen internt i det offentlige. På slutten av 90-tallet ble det inngått avtaler med Merkantildata, Telenor og Posten om å utvikle tjenester. Merkantildata falt etter hvert bort som leverandør, mens Telenor og Posten gikk sammen og etablerte det felles eide ZebSign. Problemet på slutten av 90-tallet var imidlertid at forvaltningen ennå ikke var moden for å ta slike tredjepartstjenester i bruk, blant annet fordi innføringen av elektronisk saksbehandling ikke hadde kommet skikkelig i gang ennå.

I 2000 ble det satt ned et offentlig utvalg som skulle utrede innholdet i en policy for offentlig forvaltning når det gjaldt bruk av digital signatur, dokumentkryptering for konfidensialitetsformål og tilhørende infrastruktur. Utredningen skulle presisere og avgrense hvilke spørsmål man mener en offentlig PKI-politikk skal berøre, foreslå innhold i policyen på enkelte punkter og eventuelt videre utredningsarbeid på andre, uttale seg om hva slags status en slik policy bør ha i forvaltningen og anbefale tiltak. Blant hovedspørsmålene som skulle utredes var hvilke typer digitale legitimasjoner man

²³ Kilder til dette avsnittet: Telefonsamtale med Katarina De Brisis i Fornyingsdepartementet 7. desember 2006, notatet "Utbredelse av PKI-anvendelser i offentlig sektor – Strategivalg" datert 17. februar 2005 (<http://odin.dep.no/fad/norsk/tema/ITpolitikk/pkiorgan/strategi/bn.html>) og NOU 2001: 10 "Uten penn og blekk".

skulle ha, hva slags digitale legitimasjoner forvaltningen skulle godta fra andre og om det var behov for felles policy for elektroniske legitimasjoner i forvaltningen.

Utvalget leverte sin rapport, NOU 2001: 10 "Uten penn og blekk" i mars 2001. I rapporten anbefalte utvalget blant annet bruk av en felles kravspesifikasjon for hele forvaltningen og ga anbefalinger i forhold til hvordan hele folket kan forsynes med elektronisk legitimasjon og hvordan forvaltningen kunne koordinere seg internt.

I 2002 arbeidet en arbeidsgruppe under AAD (Arbeids- og administrasjonsdepartementet) med en ny rammeavtale under Forvaltningsnettsamarbeidet. Avtalen skulle dekke forsyning av personer og virksomheter med elektronisk legitimasjon. Dette arbeidet ble lagt ned da statsråd Victor Norman la ned Forvaltningsnettsamarbeidet. Istedenfor ble det arbeidet med en "IKT-strategi i offentlig sektor" som Norman la frem i februar 2003. Denne strategien anbefalte etablering av et Koordineringsutvalg for PKI i offentlig sektor. Utvalget ble etablert i 2003, med sekretariat i AAD.

Da Morten Meyer tok over som statsråd etter Victor Norman, ble det satt ned en egen arbeidsgruppe for å utarbeide felles Kravspesifikasjon for PKI i offentlig sektor. Arbeidsgruppen rapporterte til Koordineringsutvalget for PKI. Dette Koordineringsutvalget ble imidlertid nedlagt i november 2004 og erstattet av et bredere utvalg, KoeF (Koordineringsutvalget for elektronisk Forvaltning). Dette utvalget anbefalte bruk av Kravspesifikasjon for PKI som en forvaltningsstandard for både staten og kommunene, og la i februar 2005 frem notatet "Utbredelse av PKI-anvendelser i offentlig sektor – strategivalg"²⁴ for Regjeringen.

Regjeringen ga i februar 2005 sin tilslutning til strategien. I notatet fremkommer det at Staten, ved Brønnøysundregistrene, skulle inngå en rammeavtale om tjenester fra en sikkerhetsportal, med funksjoner knyttet til autentisering og signering, tiltrodd arkivering samt tjenester for felles pålogging i tjenesteportaler. Det ble forutsatt at portalen skulle integrere løsninger fra flere PKI-leverandører som oppfylte den felles kravspesifikasjonen for offentlig sektor.

Rammeavtalen skulle inngås med én leverandør, som skulle innestå for at de PKI-løsningene som blir integrert i portalen oppfylte nødvendige krav. Det ble stilt krav om at minst 3 ulike, godkjente leverandører av PKI skal kunne brukes gjennom sikkerhetsportalene.²⁵

Godkjenning skulle skje gjennom at PKI-leverandøren frivillig sertifiserer seg i en offentlig godkjenningsordning, dersom slik finnes, eller ved at portalleverandøren, gjennom en uavhengig evaluering, inngikk en avtale med PKI-leverandørene om å innestå for deres PKI-løsninger. Portalleverandøren skulle ikke kunne nekte å godta en offentlig sertifisert PKI-leverandør som underleverandør.

Rammeavtalen for portaltjenester skulle gjøres obligatorisk for alle nye brukere av PKI (dvs. de som ikke benytter allerede eksisterende avtaler) i staten.

²⁴ Se <http://odin.dep.no/fad/norsk/tema/ITpolitikk/pkiorgan/strategi/bn.html>

²⁵ Årsaken til at man ønsket å inngå avtale med bare én sikkerhetsportalleverandør var en anskaffelsesforskrift som forbyr parallelle rammeavtaler. Et nytt EU-direktiv på området åpner imidlertid nå for at parallelle avtaler kan inngås. Dette direktivet er i Norge implementert i "Forskrift om offentlige anskaffelser" 2006-04-07 nr 402 som nå er revidert i samsvar med direktivet.

Ifølge strategiplanen skulle Staten/Brønnøysundregistrene på mellomlang sikt, ultimo 2005-2006, inngå en rammeavtale om virksomhetssertifikater og personsertifikater til bruk internt i offentlige virksomheter, for både ”Høyt” og ”Standard” sikkerhetsnivå. Avtalen skulle forutsette full samtrafikk mellom aktuelle PKI-leverandører. Det skulle også etableres én eller flere frivillig(e), offentlig(e) godkjenningss/sertifiserings-ordning(er).

Både rammeavtalen om en sikkerhetsportal og rammeavtaler om elektronisk legitimasjon/elektronisk signatur til bruk internt i offentlig sektor skulle inngås også på vegne av kommunesektoren og skal således gjelde for hele offentlig sektor.

Våren 2005 ble det inngått en rammeavtale med BBS om å levere denne sikkerhetsportalen til offentlig sektor. Det viste seg imidlertid at forretningsmodellen som lå til grunn for denne løsningen ikke fikk tilslutning fra leverandørene av elektronisk legitimasjon. Avtalen med BBS ble dermed avvirket i juni 2006.

Minside, som er en felles inngangsport for offentlige tjenester på nett, ble etablert som et samarbeidsprosjekt mellom Fornyings- og administrasjonsdepartementet (daværende Moderniseringsdepartementet) og de etatene som leverte tjenester. Minside ble lansert i desember 2006 med en autentisering basert på PIN-koder. Denne autentiseringen er i følge Fornyings- og administrasjonsdepartementet kun en midlertidig løsning inntil ny sikkerhetsportal for offentlig sektor blir etablert.²⁶

Det jobbes nå med en ny strategi for elektronisk legitimasjon og elektronisk signatur i offentlig sektor.²⁷ Den nye strategien baseres på de erfaringer som offentlig sektor har gjort i forbindelse med den gjeldende strategien. Det er ennå ikke foretatt endelig valg av ny strategi, men strategidokumentet forventes ferdigstilt i løpet av januar 2007 og skal da sendes ut på høring.

Strategidokumentet skal blant annet redegjøre for strategiske valg av forretningsmodeller for bruk av fellesløsninger som virker som insentiver for aktuelle aktører til å bidra til spredning og bred bruk av løsningene. Modellene skal sikre økonomisk forutsigbarhet for de ulike aktører. Løsningene som etableres bør ifølge arbeidsgruppen også kunne benyttes ved avtaleinngåelser mellom private parter.

I Norge er det ifølge De Brisis i like stor grad private aktører som det offentlige som har ledet an i utviklingen av elektronisk legitimasjon. Private aktører har stått for den tekniske utviklingen, mens det offentlige har fungert som en slags katalysator og rådgiver i prosessene. Det offentlige har også agert som ”krevende kunde” og derved bidratt til leverandørutviklingen gjennom det.

I Norge er det for tiden ingen sentral rammeavtale for PKI-basert elektronisk legitimasjon.

²⁶ Se http://www.norge.no/minside/om_miniside.asp

²⁷ Kilde: Mandatet for arbeidsgruppen som jobber med strategiarbeid for elektronisk legitimasjon og elektronisk signatur i offentlig sektor. Arbeidsgruppen er sammensatt av representanter fra NAV, SKD, Brønnøysundregistrene, Sosial- og helsedirektoratet, KS og FAD. Katarina de Brisis fra FAD leder arbeidsgruppen.

4.2 Sverige

I 2000 ga Regjeringen i oppdrag til Riksskatteverket (nåværende Skatteverket) sammen med Riksförsäkringsverket (nåværende Försäkringskassan), Patent og registreringsverket (nåværende Bolagsverket) og Statskontoret (nåværende Verva²⁸) å utrede og komme med forslag til hvordan ansvaret for å utvikle elektronisk legitimasjoner burde organiseres innenfor statsforvaltningen.²⁹ Bakgrunnen for oppdraget var Regjeringens visjon om å etablere såkalte ”24-timers myndigheter”.

Oppdraget ble utført i form av et prosjekt, SAMSET-prosjektet, som høsten 2000 overleverte rapporten ”RSV Rapport 2000:15, Hantering av certifikat och elektroniska signaturer inom statsförvaltningen”.³⁰ I rapporten ble det foreslått følgende:

- Myndighetene skal anvende tre sikkerhetsnivåer: *høy*, som skulle tilfredsstillе kravene til kvalifiserte signaturer, *middels*, som skulle tilfredsstillе kravet til avanserte signaturer, og *lav*, som skulle være andre typer løsninger som PIN-kode og tilsvarende. Rapporten vurderte det slik at middels nivå ville tilfredsstillе behovet til en stor del av virksomhetene innenfor statsforvaltningen, og dagens elektroniske legitimasjoner i Sverige er på dette nivået.
- Riksskatteverket skal ha i ansvar å være lede statens arbeid med utviklingen av elektroniske legitimasjoner.
- Det skal legges til rette for at også kommuner og landsting kan bli med i samarbeidet gjennom å benytte de rammeavtaler som inngås.

Etter at rapporten var levert ga Regjeringen i desember 2000 et nytt oppdrag til Riksskatteverket. Verket fikk i oppdrag å samordne alle spørsmål knyttet til elektronisk legitimasjon innen statsforvaltningen og på bakgrunn av dette utforme myndighetenes kravspesifikasjon til elektronisk legitimasjon i offentlig sektor. Det ble gjort klart fra Regjeringens side at samarbeid med private aktører skulle utnyttes så langt som mulig. Dette var basert på at det allerede fantes en stor gruppe av befolkningen hadde et system for å identifisere seg i nettbank, og at det offentlige ønsket å utnytte dette systemet. Dette arbeidet ble også gjort innenfor SAMSET-prosjektet og ble rapportert våren 2003.

I 2001 ble BankID i Sverige etablert og samme året hentet Statskontoret i nært samarbeid med SAMSET-prosjektet inn tilbud på elektronisk legitimasjon, med en kravspesifikasjon som ikke var spesielt detaljert. Anbudsprosessen endte med at fire aktører fikk rammeavtale:

- BankID med IBM CBT (Java Applet) med støtte for softwarebaserte legitimasjoner
- Nordea med SmartTrust Personal med støtte både for softwarebaserte legitimasjoner og smartkort

²⁸ Verket för förvaltningsutveckling, etablert januar 2006.

²⁹ Kilder til dette avsnittet: Telefonsamtaler med Jose Guevara 27. november 2006 og Jonas Øholm 29. november 2006. Begge er ansatte i Skatteverket. Jonas Øholm sitter også i arbeidsgruppene som jobber med utviklingen av Elektronisk legitimasjon i Sverige. Vi har også fått innspill fra Dag Osterman som store deler av tiden har ledet prosjektet med utvikling av Elektronisk legitimasjon.

³⁰ Se <http://www.skatteverket.se/skatteverketsrapporter/rapport20001123/samsetrapport0927.4.584dfe11039cdb62698000770.html>

- Posten med SmartTrust Personal med støtte både for softwarebserte legitimasjoner og smartkort
- Telia med SmartTrust Personal med støtte for smartkort, og Telia med Verisign PTA (ActiveX) med støtte for softwarebaserte legitimasjoner

Utgangspunktet fra myndighetenes side var at disse aktørene skulle operere med en prismodell som innebærer at tjenesten er gratis for sluttbrukerne og at det ikke skulle være noen engangskostnader for brukersteden ved implementering av systemet. Inn-tjeningen skulle komme fra bruken, og da var det brukersteden som skulle betale.

Enkelte offentlige myndigheter med små budsjetter har uttrykt skepsis til å ta i bruk elektronisk legitimasjon, fordi det er uklart hvor mange som vil benytte seg av elektronisk legitimasjon og at det dermed er usikkert hva dette til syvende og sist vil koste den enkelte etat. Forretningsmodellen tar imidlertid ikke endelig stilling til prismodellen. Det er derfor ikke noe hinder for at en etat eller en gruppe av etat forhandler frem en annen prismodell. Dette skjedde i november 2005 da de tre største statlige etatene, de tre største landstingene og de tre største kommunene i fellesskap tegnet en avtale om en fast pris i tre år med bankene og TeliaSonera. Det sentrale virkemiddelet for Verva i forhold til små myndigheter som ønsker å komme i gang med e-tjenester er å trekke disse inn i denne avtalen.

I 2004 var det en ny anbudsrunde med de tre aktørene BankID, Nordea og Telia på banen. Posten hadde på dette tidspunktet solgt sin virksomhet innenfor elektronisk legitimasjon til Telia. I tillegg kom Steria med som en aktør, men ingen brukersteder aksepterer Sterias løsning i dag. Steria er dermed i realiteten ikke en tilbyder av elektronisk legitimasjon, selv om de har en rammeavtale.

Et problem ifølge våre kilder er imidlertid at myndighetene ikke har vært mer detaljerte i kravspesifikasjonen. Dette har blant annet resultert i at systemene ikke kan "snakke sammen".

De aller fleste offentlige myndigheter i Sverige har implementert alle de tre systemene. Alle svensker med elektronisk legitimasjon kan derfor benytte sin elektroniske legitimasjon for de fleste tjenestene som er tilgjengelige. Selv om de direkte engangskostnadene ikke er noe større for myndighetene ved å implementere tre systemer, påløper det større interne implementerings- og driftskostnader med tre systemer fremfor ett. Det finnes eksempler på etater som ikke har implementert alle tre løsningene, hvilket kan resultere i at en borger som for eksempel har fått utstedt elektronisk legitimasjon hos Nordea ikke kan søke om sosiale goder i sin kommune på nettet. Dette problemet kan imidlertid løses forholdsvis enkelt ved hjelp av en "mellommann".

Videre har det kommet kritikk fra myndighetene i Sverige for at næringslivet ikke i større grad har kommet på banen og lagt til rette for bruk av elektronisk legitimasjon på sine nettsider. Jo flere tjenester brukerne kan benytte elektronisk legitimasjon på, jo større verdi vil legitimasjonen ha for den enkelte bruker.

Elektronisk legitimasjon utstedes i dag fra alle de tre leverandørene både i en chip på et bankkort eller lignende, og som software til å installere på PCen. BankID og TeliaSonera samarbeider for tiden om å knytte elektronisk legitimasjon til sim-kortet på mobilen. Dette vil gjøre elektronisk legitimasjonen enda mer anvendelig enn i dag for svenske borgere.

Fra januar 2007 kommer virksomheten i SAMSET-prosjektet til å legges til Verva. For perioden 2006 til og med 2008 disponerer Verva 12 millioner SEK i året for å støtte mindre myndigheters startkostnader i forbindelse med innføring av elektronisk legitimasjon.

4.3 Danmark

På initiativ fra Regjeringen i Danmark, ble det på begynnelsen av 1999-2000 satt i gang flere pilotprosjekter om digital signatur.³¹ Målet for prosjektene var å se om det var mulig å etablere et marked for digital signatur. Pilotprosjektene konkluderte med at dette ikke var mulig. Borgerne var ikke villige til å betale for en digital signatur som de ikke visste hva kunne brukes til, og bedriftene var ikke villige til å bruke penger på å utvikle et system for digital signatur, så lenge det ikke var noen brukere.

Konsekvensen av arbeidet i pilotprosjektene ble derfor at Vitenskapsministeriet og IT- og Telestyrelsen utarbeidet en felles offentlig standard for digital signatur. Denne standarden ble kalt OCES (Offentlige Certifikater til Elektronisk Service). IT- og Telestyrelsen administrerer den felles offentlige standarden i form av tre legitimasjons-politikker.

I 2002 utlyste Vitenskapsministeriet et oppdrag om å utvikle en digital signatur på OCES-standard. TDC vant dette oppdraget i konkurranse blant annet med finansnæringen. TDC tegnet så en kontrakt på 4 år, med opsjon på et femte år, med Vitenskapsministeriet.

Utviklingskostnadene til dette prosjektet blir delvis finansiert av det offentlige. Forretningsmodellen er basert på at brukerstedene betaler for bruken av infrastrukturen. Offentlig sektor er gjennom en sentralt finansiert avtale fritatt for å betale for å motta signaturer. Digital signatur er gratis for danske borgere og signaturen kan fritt benyttes til å kryptere og dekryptere e-post, og til de rundt 100 offentlige selvbetjeningsstedene hos myndigheter i Danmark. Tilsvarende kan private virksomheter gratis bruke medarbeidersignaturer til offentlige myndigheter. Private virksomheter som ønsker å bruke infrastrukturen og motta signaturer, må inngå en egen avtale med TDC. Rundt 30 private virksomheter i Danmark har inngått slike avtaler og tilbyr tjenester med digital signatur.³²

Banknæringen i Danmark har etter at TDC fikk oppdraget for IT- og Telestyrelsen, utviklet NetID. Denne legitimasjonen er ikke PKI-basert sett fra brukernes side. Legitimasjonen er slik at bankene gis fullmakt til å signere på vegne av kunden, men kunden er ikke utstyrt med noen "public key" som kan benyttes hos forskjellige tjenesteleverandører.

IT- og Telestyrelsen skal i nær fremtid ha en ny anbudsrunde om å utvikle og drifte OCES i Danmark de neste årene. Både TDC og andre aktører kan gi tilbud på dette.

En av hovedutfordringene fremover blir ifølge IT- og Telestyrelsen å få etablert strukturer som gjør det mulig å benytte elektronisk legitimasjon på tvers av lande-

³¹ Kilde: Telefonsamtale med Charlotte Jacoby i IT og Telestyrelsen 28. november 2006. Sjefskonsulent Palle H. Sørensen som sitter i IT-sikkerhedskontoret i styrelsen er ansvarlig for prosjektet Elektronisk signatur i Danmark.

³² Se oversikt over virksomhetene i Tabell 3.4.

grensene. Det er også en viktig utfordring å få utbredt den digitale signaturen ytterligere, for eksempel til den finanssektoren, slik at danske borgere kan bruke den samme digitale signaturen både for å få utført banktjenester og for tjenester i offentlig forvaltning.

4.4 Finland

Finske myndigheter tok i 1997/1998 initiativ til å utvikle elektronisk legitimasjon i Finland.³³ Det var Finansdepartementet og Innenriksdepartementet som var sentrale fra myndighetenes side, og i 1999 kom det en ny lov om elektronisk kommunikasjon i Finland som la føringer i forhold til utviklingen av elektronisk legitimasjon.

I 1999/2000 etablerte banker og telecom-selskaper i Finland et felles selskap for å utvikle elektronisk legitimasjon. Tanken var å lage en felles legitimasjon. I 2002 gikk imidlertid selskapet konkurs, og bankene og telecombransjen skilte lag. Telecom gikk inn i samarbeidet med myndighetene og utviklet det som i dag er borgerkortet. Bankene på sin side fortsatte å utvikle sin egen løsning, Tupas. Tupas er tilsvarende som NetID i Danmark som nevnt tidligere foreløpig ikke en PKI-basert løsning.

Myndighetene har stått for utviklingen av borgerkortet. Myndighetene har imidlertid ikke finansiert utviklingen på egen hånd. Utviklingskostnadene har vært et spleiselag mellom myndighetene og private aktører, i den forstand at alle som har vært med har bidratt gratis.

Borgerkortet, eller Citizen Certificate, kan utstedes enten på et rent ID-kort, på simkortet i mobilen, eller på et bankkort. Befolkningsregistersentralen har som nevnt et samarbeid med OKO Bank om å utstede legitimasjonen på bankkort og med Telia Sonera og teleselskapet Elisa i Finland om å utstede legitimasjonen på sim-kort. Det er bare én bank i Finland, OKO Bank, som aksepterer borgerkortet.

Utfordringene fremover er fremdeles ”høna og egget”-problematikken innenlands for å få opp kritisk masse både av brukere og tjenesteleverandører, i tillegg til harmonisering mellom landene. Det vil også være viktig for å øke nytteverdien av borgerkortet i større grad å kunne koble personlig informasjon fra ulike registre sammen.

Høsten 2006 ble det lagt frem en strategi for e-Government i Finland, *Finnish Information Society Strategy for 2007–2015*. Dette er i hovedsak en strategi for hvordan man i større og større grad kan flytte kommunale og statlige tjenester over på nett. I forbindelse med fremleggelsen av strategien har det kommet forslag om å gjøre borgerkortet gratis tilgjengelig for alle som ønsker det i 2008.

Når det gjelder hvorfor såpass få av innbyggerne i Finland foreløpig er utstyrt med elektronisk legitimasjon, og at utviklingen på den måten har gått relativt langsomt, mener Jelekäinen at det har sammenheng med de svært høye kostnadene forbundet med utvikling av en helt ny infrastruktur. Kostnaden per bruker i Finland er spesielt stor,

³³ Informasjonen i dette avsnittet er hentet fra intervjuer med Tapio Aaltonen 29. november 2006 og Pekka Jelekäinen 4. januar 2007. De har begge vært sentrale i utviklingen av elektronisk legitimasjon fra myndighetenes side i Finland. Tapio Aaltonen ledet inntil nylig administrasjonen av Porvoo-gruppen. Han jobbet tidligere i Befolkningsregistersentralen, som utsteder borgerkortet i Finland, men har nå en annen posisjon i innenriksdepartementet i Finland. Pekka Jelekäinen er i dag direktør for Certificate Service Department i Befolkningsregistersentralen.

både når det gjelder implementering og drifting, fordi det er så få brukere. Jelekäinen har oversikt over hvor store de samlede kostnadene har vært, men dette tallet ønsker han ikke å offentliggjøre.

I neste kapittel skal vi se nærmere på forskjeller mellom de fire landene i Norden når det gjelder implementering av elektronisk legitimasjon.

4.5 Forholdet mellom det offentlige strategi og utbredelsen av elektronisk legitimasjon

Det er mange forhold som kan påvirke utbredelse og bruk av elektronisk legitimasjon. Vi kan ikke trekke noen entydig konklusjon om sammenhenger basert på den begrensede kartleggingen som er gjennomført i forbindelse med denne rapporten.

Likevel ser vi at enkelte strategier tilsynelatende har vært mer vellykkede enn andre når det gjelder å få tilstrekkelig antall brukere til at elektronisk legitimasjon skal være interessant for brukerstedene og motsatt. Finland ser ut til å ha valgt en strategi som har vært mindre effektiv enn de andre landene på dette området. For det første har myndighetene valgt å etablere en helt ny infrastruktur fremfor å utnytte en allerede eksisterende. Dette har medført en ekstrakostnad for å få utstedt elektronisk legitimasjon i form av tidsbruk til fysisk oppmøte hos utstederen av elektronisk legitimasjon. Når i tillegg antall tjenester som elektronisk legitimasjon kan benyttes på er begrenset, har trolig kostnaden for finske borgere vært større enn nytten ved å ha en elektronisk legitimasjon.

Generelt har Norge, Sverige og Danmark en høyere utbredelse av elektronisk legitimasjon enn Finland. I motsetning til Finland har Norge, Sverige og Danmark valgt strategier som baserer seg på å utnytte allerede eksisterende infrastruktur. Disse tre landene har likevel litt ulik tilnærming. Svenske myndigheter har inngått rammeavtale med alle tre leverandører av elektronisk legitimasjon som har tilfredsstilt en ikke spesielt detaljert kravspesifikasjon. Dette har gitt utfordringer knyttet til at systemene ikke har kommunisert med hverandre og at brukerstedene dermed har måttet implementere alle tre systemene for å være tilgjengelige for alle med elektronisk legitimasjon. Danske myndigheter har utformet en mer detaljert kravspesifikasjon og valgt kun én leverandør av elektronisk legitimasjon for bruk i offentlige tjenester. Bankenes infrastruktur i Danmark er dermed ikke utnyttet av myndighetene. I Norge har man i dag ikke sentralisert anskaffelsen av elektronisk legitimasjon. Det er opp til de ulike offentlige etatene hvordan de løser dette. På samme måte som i Danmark har man i Norge i liten grad benyttet seg av den infrastrukturen som er etablert innenfor bank.

Utbredelse av elektronisk legitimasjon kan vurderes i lys av teorier om nettverks-effekter. Nettverkseffekter eksisterer når en kundes nytte ved å være tilknyttet et nettverk avhenger av hvor mange andre som er tilknyttet nettverket. En viktig forutsetning for at elektronisk legitimasjon skal være attraktivt for brukere og brukersteder, er at det for brukerstedene er tilstrekkelig mange brukere og for brukerne at det er tilstrekkelig mange brukersteder som aksepterer elektronisk legitimasjon. Tilstedeværelsen av nettverkseffekter kan gjøre at det eksisterer en kritisk masse for at gevinstene skal hentes ut. Én utfordring ligger dermed i å få opp volumet på utbredelsen av elektronisk legitimasjon. Ut i fra dette vil omfanget av nettverket også øke dersom de ulike systemene kommuniserer med hverandre. Samsnalking er mulig gjennom

tekniske løsninger, men det er store utfordringer knyttet til ulike sikkerhetsnivåer og ansvarsproblematikk, særlig for kvalifiserte sertifikater.

Fra et myndighetsståsted vil det sannsynligvis være et ønske om størst mulig utbredelse av elektronisk legitimasjon når dette først skal være en tilgjengelig tjeneste i forvaltningen. Slik sett virker det som en mer effektiv strategi fra myndighetenes side å basere seg på eksisterende infrastruktur heller enn å utvikle nye systemer, gitt at markedsløsningene tilfredsstiller kravene som settes. På den måten kobler man seg på en etablert brukermasse. Forskjellen mellom Finland og de andre nordiske landene kan sannsynligvis benyttes til å illustrere dette poenget.

Mange ulike forhold påvirker utviklingen og implementeringen av elektronisk legitimasjon, for eksempel den lange tradisjonen med infrastrukturensamarbeid mellom alle bankene i Norge.

Vi har ikke nok informasjon til å vurdere den potensielle sammenhengen mellom myndighetenes strategivalg og effekt i form av utbredelse.

VEDLEGG 1: Elektronisk signatur, elektronisk legitimasjon og sertifikater

Elektronisk signatur er en generell betegnelse på teknikker som kan benyttes til å "signere" digital informasjon på tilsvarende måte som en håndskrevet signatur benyttes til å undertegne et papirdokument. Elektronisk signatur er en av flere mulige teknikker som kan brukes til slik signering.³⁴

En elektronisk signatur kan også benyttes til å bekrefte hvem man kommuniserer med, og kan da for eksempel benyttes til å erstatte passord ved pålogging til datasystemer og tjenester på Internett. Brukt slik fungerer den elektroniske signaturen som en elektronisk legitimasjon.

For at mottakeren skal kunne godta en elektronisk signatur må han kunne stole på at undertegneren er den han utgir seg for å være. Til dette brukes ofte et sertifikat og valideringstjenester. Sertifikatets funksjon er å gi mottakeren de opplysningene han trenger for å kunne ta stilling til hvorvidt han kan stole på den elektroniske signaturen som mottas. Utstederen av sertifikatet er dermed en tredjepart i forholdet mellom undertegneren og mottakeren av signaturen. Sertifikatutstederen bekrefter ved å utstede sertifikatet at undertegner er den han gir seg ut for å være.

Post- og teletilsynet er tilsynsmyndighet ovenfor utstedere av kvalifiserte sertifikater, og de ulike sertifikattyper er beskrevet i "Kravspesifikasjon for PKI i offentlig sektor" (Person-Høyt, Person-Standard og Virksomhet).³⁵

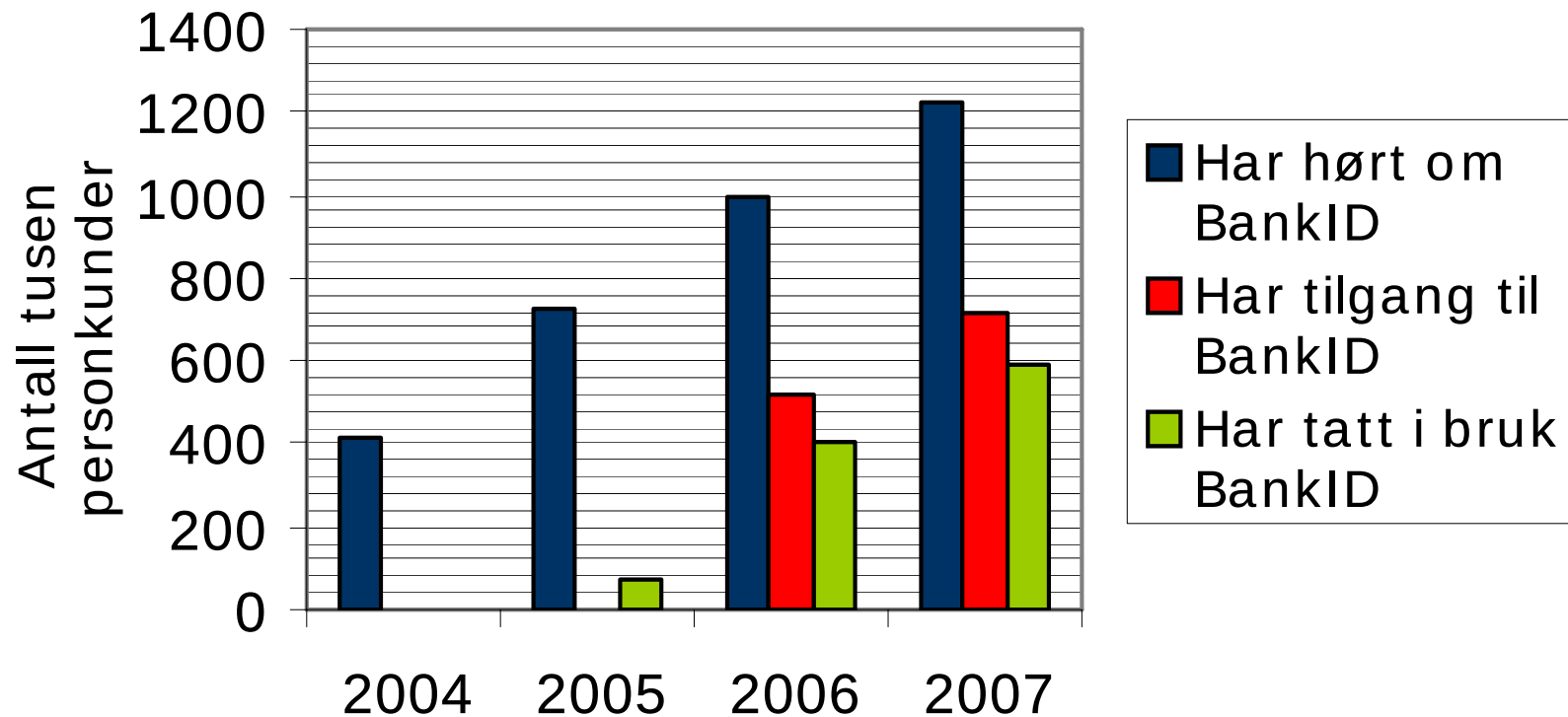
PKI-basert elektronisk signatur

Den som vil bruke en PKI-basert elektronisk signatur får tildelt et (eller flere) elektronisk "nøkkelpar" som består av en offentlig og en privat nøkkel samt et sertifikat som knytter undertegners identitet til den offentlige nøkkelen. Den offentlige nøkkelen kan distribueres til mottakerne av de signerte meldingene like åpent som man for eksempel gjør med telefonnumre. Den private nøkkelen er strengt personlig og må holdes hemmelig, som koden til bankkortet. Det er altså kun én person som kan signere meldingen ved hjelp av den private nøkkelen, mens det er mange som kan verifisere denne signaturen ved hjelp av den offentlige nøkkelen.

³⁴ Innholdet i dette avsnittet er hentet fra www.npt.no

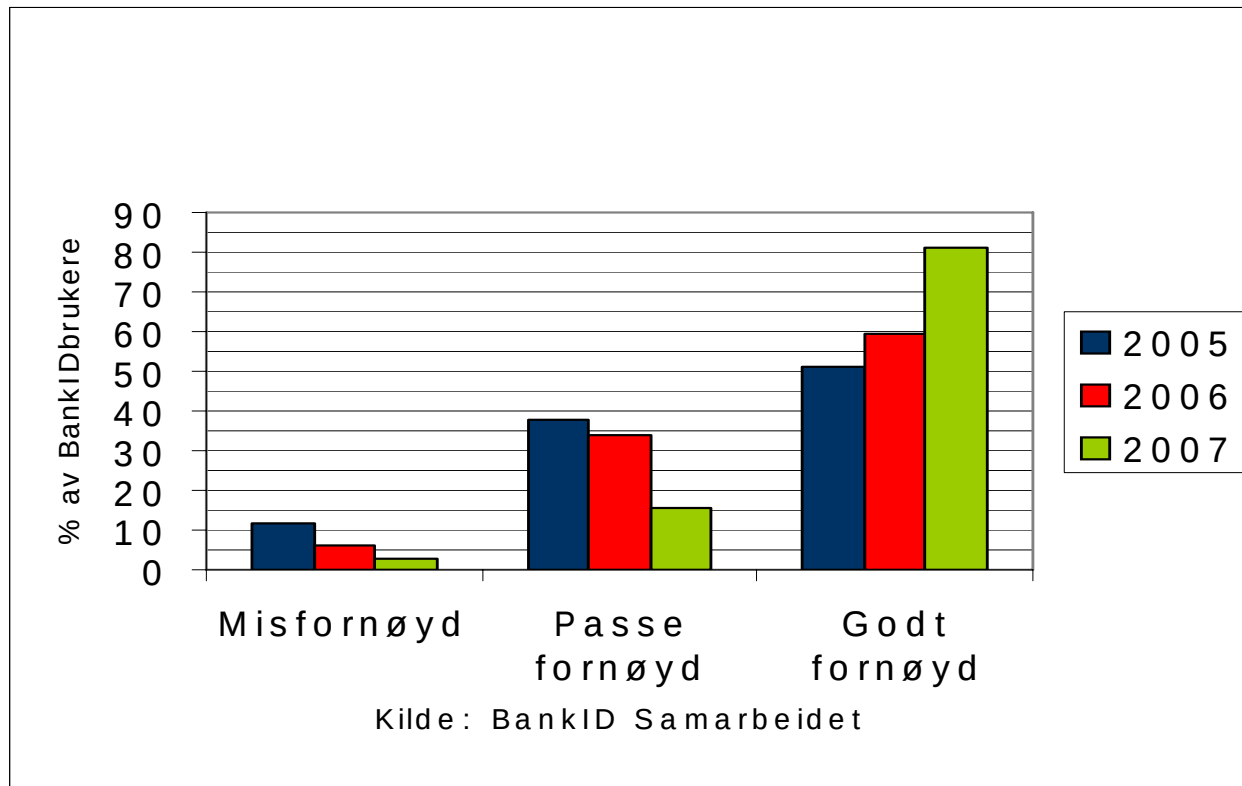
³⁵ Se http://odin.dep.no/filarkiv/234033/Kravspek_PKI_v102.pdf

Stigende kjennskap til og bruk av BankID



Kilde: BankID Samarbeidet

Stigende tilfredshet blant BankID-brukerne



På en skala fra 1-6 ligger gjennomsnittet på 5,2