Jan Bergström
S:t Eriksgatan 48
112 34 Stockholm
08-6505553
070-7559494 (GSM)
janbm70@gmail.com

2015-08-29

Näringsdepartementet

Remissvar eIDAS

Vad är direktivet/eIDAS? – en beskrivning av en teknisk maskin, en nationell PKI betroddhetsserver

Jag har tidigare utgått ifrån att det finns ett politiskt motstånd mot genomförandet av digitala signaturdirektivet 1999/93/EG de senaste 16 åren och nu digitala signaturförordningen 910/2014. Att varje gång de senaste åren jag klagat på att digitala signaturdirektivet inte är genomfört svarar departementet att det är genomfört i en lag. Ett svar som i allmänhet betraktats som ett skämtsamt sätt att vara undflyende svar på ett dåligt politiskt ställningstagande, genomförandet finns ju inte rent tekniskt att tillgå. ***Jag kan ju inte maila departementet med en digital signatur som verifierar ursprunget?***

I stort sett hela IT-marknaden har felaktigt betraktat situationen som korrupt. Sanningen är att departementet inte förstått direktivets och förordningens innehåll och inte följt en svenska konstitutionen. Detta till stort förtret för hela samhället som i 16 år inte haft tillgång till en nationell digital signaturinfrastruktur av stor ekonomisk och praktisk betydelse för såväl den enskilde, näringslivet som för myndigheterna.

Digitala signaturdirektivet 1999/93/EG de senaste 16 åren och nu digitala signaturförordningen 910/2014 handlar om en väldigt viktig allmän samhällsservice för den enskilde, näringslivet och statens myndighetsutövning för att kunna bygga säkra applikationer för användare av alla dess slag i samhället. För att kunna tillhandahålla tjänster som är omöjliga utan. Något som förnekats samhället i 16 år. Se ex ”digital signatur” på Wikipedia.se.

Digitala signaturdirektivet handlar om beskrivningen av en teknisk maskin, en nationell PKI digital signatur trustserver dit alla digitala signaturoperatörer frivilligt kan anslutna sig till.

Detta för att åstadkomma en nationell digital signaturenhet där vem som helst inom Sverige kan sända ett signerat dokument eller email och oberoende av vilken digital signaturoperatör parterna har kan dokumentet/emailets ursprung säkerställas. Att avsändarens PKI certifikat är genuina, att momsdirektivets artikel 233 om ursprungsmärkning av elektroniska fakturor tekniskt är genomförbart.

Det handlar om att skapa en nationell PKI digital signatur betroddhetsunion. Endast nivån för digital ursprungsmärkning är obligatorisk i digitala signaturdirektivet, anslutningen till nationella enheten är frivillig och så också alla andra mer avancerade tillämpningsformer. Endast staten kan driva en nationell central PKI betroddhetstrust.

Tekniskt sett finns inga problem eftersom standarder i IT-branschen är klara och fungerande sedan 1990-talet och finns tillgängligt för alla datortyper sedan dess för rutinmässig användning. ***Det enda som hindrar infrastrukturen att finnas är avsaknaden av regeringens utnämnande av en myndighet för direktivets genomförande.*** Vi talar om infrastruktur motsvarande betydelse som email, webben, telenät osv av stor betydelse för samhällets alla delar.

Digitala signaturförordningen ersätter digitala signatur-direktivet men har samma innehåll, där dock krav på anslutning till EUs internationella PKI digital signatur trustserver tillkommit. Dit de nationella PKI digital signatur trustservrarna (och inga andra) krävs anslutas till. Det finns ingen annan fungerande teknisk lösning.

Detta för att åstadkomma en tekniskt fungerande Europeisk enhetlig digital signatur betroddhetsunion. Dvs digitala signaturer skall fungera oberoende av digital signaturoperatör inom EU. Där sin dator skall ex kunna kontrollera genom att fråga sin operatör om en tysk avsändares certifikats genuinitet. Detta genom att operatörens maskin frågar den nationella trustservermaskinen som frågar den internationella som frågar den tyska nationella trustservern som frågar den lokala signaturoperatören om genuinitet, med svar tillbaka.

Ett av de huvudsakliga problemen med genomförande av digitala signaturförordningen i Sverige är att digitala signaturdirektivet inte är genomfört i Sverige. Man måste börja med att sätta upp den först. Det finns inget annat sätt att uppfylla digitala signaturförordningen.

Alla andra aspekter av direktivet/förordningen är underordnade frågor. Dock råder krav här på att det finns en nationell lösning för inloggning i myndigheternas web-informationssystems privata sidor även med certifikat från utlandet inom ramen för betroddhetsunionen. Något som man löser genom att sätta upp en särskild digital signatur-operatör för integration med myndigheternas inloggningssystem, bara den allmänna betroddhetsunionen inom EU existerar och fungerar.

Däremot läser man eIDAS-PMet inser man att departementet de senaste 16 åren inte förstått vad varken digitala signatur-direktivet 1999/93/EG eller nu digitala signaturförordningen 910/2014 handlar om. Departementet har uppfattningen att digitala signaturdirektivet 1999/93/EG de senaste 16 åren och nu digitala signaturförordningen 910/2014 handlar om krav på granskning av nationella digitala signaturoperatörer. Detta av någon slags allmän säkerhetsiver (som ingen kunna förklara) för att försörja myndigheter i sina problem med säker inloggning i sina publika web-informations-systems personliga sidor (som då inte skulle kunna ställas i upphandlingen, trots direktivet/förordningens existens).

- När lösningen på myndigheternas loginproblem till sina publika web-tjänsters personliga delar är till 90% avhängigt att digitala signaturdirektivet/förordningen genomförs genom att konstitutionsenligt en myndighet utnämns att genomföra dem.
  All aktivitet myndigheterna visat hittills, har handlat om att hitta alternativa vägar då det inte är accepterat inom myndigheterna att förklara att departementet inte förstått direktivets innehåll. Jag är inte myndighet och kan uttrycka det och jag kan klaga till EU-kommissionen om jag finner det nödvändigt.
- Resten löser myndigheterna genom att sätta upp en egen för ändamålet anpassad digital signaturoperatör vars system är kopplad till myndigheternas inloggningssystem enligt deras överenskommelse och ansluten till den nationella PKI-trusten.

Troligtvis är skälet till att departementet i 16 år inte förstått direktivets innehåll att:

- Man saknar intern teknisk komptens inom teknikområdet
- Varken departementet eller någon myndighet har deltagit i EU-arbetsgrupper för digitala signaturer och inhämtat kunskapen om vad digitala signaturer handlar om.

- Ingen myndighet är avdelad ansvarig att svara för statens intressen i digitala signaturfrågor, som informerar departementet om sakfrågorna och bevakar EU-kommittéerna.
- Vokabulären i EU-dokument är svårtydliga då de sällan beskriver direkt vad som avses utan runt omkring. Vad det handlar om anses givet av EU då man förutsätter deltagande i kommittéarbetet, men deltagande har inte fallet varit här.
- Vokabulären inom PKI ex begrepp som certifiering är snarlika juridiska begrepp som gör att man kan tro det handlar om juridiska texter om digitala signaturoperatörer och inte tekniska system där man kontrollerar betroddheten hos en avsändare.
- Man har inte följt konstitutionen och regeringen har försökt detaljstyra verkställigheten av direktivet själv, istället för att som konstitutionen kräver utnämna en myndighet med det ansvaret. Det är myndigheter som arbetar med verkställighetsfrågor av lagar och direktiv och skall regelverk skrivas skall de vara myndighetsföreskrifter och inte lagar.
- Departementet har haft väldigt svårt att få omgivningen att förstå sin tolkning av direktivet (som uppriktigt sagt är nonsens), få förankring för sin syn och kritik når/vågar inte fram, vilket gör det svårt att verka. Så allt fastnar i intet.

Jag hoppas att departementet följer konstitutionens rättelsekrav (RF1:9) och omgående genomför eIDAS på ett korrekt sätt. Utser en myndighet (SKV) att verkställa direktivet som är jämställt svensk lag. Säkerställa att myndigheten får regleringsbrev att deltaga i EUs digitala signatursamarbete i olika arbetsgrupper och sammankomster.

Verkställighet eller lagstiftningsuppdrag?

EU hävdar att dess direktiv och förordningar är jämställda med nationell lag och det lär redan finnas prejudikat i EU-domstolen på detta. Om inte annat måste den av mig i andra sammanhang kända EU-domen C-479-10 tolkas som att EU-kommissionens syn gäller. Det är alltså ingen situation som kräver någon ytterligare nationell lagstiftning för sin giltighet. ***Det är en ren verkställighetsfråga***.

I Sverige (och Finland) är regeringsmakten och staten (verkställighetsmakten) skilda vilket är unikt i Europa. I alla andra länder ansvarar departementet och ministern för direktiven och förordningarnas verkställighet (där det då inte heller handlar om lagstiftning). ***I Sverige och Finland är regeringen (departementet) förbjuden enligt konstitutionen att bedriva ministerstyre*** (RF 12:2 oh 12:3) och innehar enbart utnämningsmakten och skyldigheten att tillhandahålla resurser (regleringsbrev) för sakens verkställande.

Kort sagt det är en ren fråga om att utse en lämplig myndighet. Dessutom skall ev behov av förändringar av lagstiftningen initieras av den ansvariga myndigheten och inte departementet eftersom myndigheten besitter sakkunskapen och erfarenheten.

Departementet har ingen konstitutionell befogenhet att handlägga ärendet ytterligare. Möjligen i sin korrigeringsprocess lägga fram proposition om att Lag (2000:832) om kvalificerade elektroniska signaturer upphör omgående. Detta då om det krävs en sådan reglering vid sidan av EUs digitala signaturförordning skall det utfärdas som myndighetsdirektiv vilket är den normala gången i tillämpningsfrågor i Sverige.

Städarbete av lagstiftning är oberoende av verkställigheten. Primärt finns ett behov att alla uppgifter i lagtexter om underteckning/signatur uttrycks på ett tekniskt formoberoende sätt i all lagstiftning och liknade.

Vem som bör ansvara för arbetet?

Eftersom SKV handhar frågorna om identiteter i Sverige och ID-korten är SKV den absolut mest lämpliga myndigheten för uppdraget.

Man bör göra utnämnandet snarast och därför i uppdraget inkludera ansvaret för digitala signaturdirektivet som gäller till 2015-12-31.

Hur arbetet bör läggas upp

I utnämningen av myndigheten för ansvaret av digitala signaturförordningens genomförande och utfärdandet av regleringsbrevet kan regeringen utforma en uppdragsbeskrivning till myndigheten

1. Kostnaderna för genomförande digitala signaturdirektivet 1999/93/EG och nu digitala signaturförordningen 910/2014 bör av staten ses som en central komponent att rationalisera statens egen administration och därför ***finansieras direkt genom budgetanslag och inte genom avgifter***. Det är i statens intresse att detta tillämpas snarast.
2. ***2017-01-01 måste anses vara ett lämpligt krav om senaste driftstart*** av den grundläggande infrastrukturen. Upprättandet av en nationell PKI digital signaturserver.
    - En betroddhetsgemenskap som är frivillig för digitala signaturoperatörer att ansluta sig till och utöver frågan om kontroll av digitala dokuments utfärdares certifikats genuinitet, är funktionsnivån frivillig.
    - I uppdraget ingår att bevaka de legala omständigheterna av utgångspunkten av den nationella digitala signatur betroddhetsunionen och vilka myndighetsföreskrifter som måste komplettera EUs digitala signaturföreskrift. I uppdraget ingår att kommunicera med departementet och EUs arbetsgrupper i frågan.
3. ***Myndigheten ansvarig för ID-kort (SKV) bör i ett separat uppdrag*** bör anmodas att förse de nationella ID-kort som utfärdas med PKI digitala signatur-kompatibla chip för bärande av PKI certifikat.
    - Korten bör innehålla ett generellt PKI ID-certifikat utfärdat av staten
        - ***För detta certifikat måste man sätta upp en egen digital signaturoperatör*** och den bör enligt regeringsuppdraget vara ansluten till den nationella trustservern (2).
        - ***Inga avgifter för identifieringar av det generella ID-kortcertifikaten skall uttas*** av tredje part som önskar verifiering. Skall ses som statens generella tillhandahållande av säker infrastruktur och säkerställa överlägsenhet och stöd för legal beskattad handel och transparent skatte och ekonomiredovisning.
    - Korten skall medge (genom en betrodd procedur av tredje partsleverantörer) att kunna bära andra PKI certifikat för andra ändamål. Detta för att en PKI HW-infrastruktur skall tillhandahållas även för behoven för SME och privatpersoner, vilket är EU-krav.
    - Korten skall också kunna bära ytterligare data såsomför biometrisk kontroll som kan tillämpas även

på frivillig grund vid beställningar från olika organisationer/företag, ex för tjänstelegitimationer.

- Korten skall inte överdebiteras, utfärdas av staten till självkostandspris + gängse vinstmarginal 20% såsom en del av statens behov. De skall inte finansiera tjänstemannainfrastrukturen på myndigheten.

Regeringen bör också ge myndigheten i uppdrag att säkerställa att:

- Svenska ID-kort är säkert Schengen-kompatibla och säkra att använda för resa inom Schengenområdet
- Att Schengen-specifikationen för ID-kort uppdateras genom förhandlingar av myndigheten (det är alltid myndigheter som skall förhandla tillämpningsfrågor) med EU-kommissionen:
  - En rad krav idag saknar relevans eftersom Storbritannien som traditionellt saknat personnummer och ID-kort, är inte är med i Schengen. Endast nödvändiga uppgifter för identifiering i Schengen-registret behövs.
  - Kortens tillämpning i dagens tekniknivå bör utgå ifrån att det finns mobila kortläsare för läsning av korten, vid ex ID-kontroller av polis.
  - Nya data bör tillföras korten då det tekniskt är billigt att ex tillämpa fingeravtrycksläsning och det uppenbart är problem med ren bildidentifiering och bild-ID-bedrägerier förekommer.
  - Ökad layoutmässig samstämmighet inom EU för underlättande av läsning av utländska kort
- Körkortskravet bör avskaffas nationellt och ersättas med krav på id-kort (gammalt rationaliseringskrav). Staten skall utrusta varje polis med mobil ID-kortläsare som är ansluten till körkortsregistret.
  - Frågan om EU-gemenskapligt avskaffande av körkortskravet och ersättande med ID-kortkrav bör förhandlas fram av myndigheten.
- Körkorten bör framställas av staten på samma tekniska grund som ID-korten och ha samma status.

4. ***Utfärdande av nationella ID-kort skall kunna ske av tredje partleverantör*** enligt ett myndighetsföreskriftregelverk. Ex skall banker såsom i Norge ges möjligheten att förse bankernas bankkontokort med nationellt PKI digital signaturkompatibla ID-kort på kontokortets baksida.

   För reglering och kontroll av verksamheten bör en myndighet utses som ansvarig myndighet (förslagsvis PTS som reglerar liknade fall) med regleringsbrev för verksamheten.

   - Myndigheten bör också ansvara för att staten inklusive kommunerna genom offentlighetsprincipen tillhandahåller alla de digitala dokument som kan vara publikt tillgängliga och sökbara genom webben. (En del av regeringens IT-handlingsplan.) Den enskilde skall primärt klaga på bristande service hit.
   - Även körkort skall kunna utfärdas av myndigheten godkända tredjepart-leverantörer.

5. En myndighet, förslagsvis samma som (2) bör i ett separat ***uppdrag ges i uppdrag att ansvara för samordningen av svenska myndigheter, domstolars och kommuners behov av säkra gemensamma metoder för inloggning på web-platser med publik service för den enskilde***.

   Regeringen bör besluta att inloggningsmetoden bör vara gemensam för hela statens publika service via web-tjänster.

   - Projektet bör också få i uppdrag att utarbeta rutiner för säkerhetsnivåer för olika typer av personliga data där ingen överdriven säkerhet skall medföra att tillgängligheten på data försvåras.
   - Projektet bör också ansvara för hur staten säkerställer digitala identiteter i dokument och email som kommer in till staten (staten inkl kommuner och domstolar).
   - Projektet bör också ansvara för policy för hur staten själva tillämpar digitala signaturer för de dokument och email som man ger ut.

6. En myndighet, förslagsvis samma som (2) bör i ett separat ***uppdrag ges i uppdrag att ansvara för samordningen av svenska myndigheter, domstolars och kommuners behov av säkra gemensamma metoder för intern tjänstemannainloggning*** i standardmyndigheternas interna datornätverk, utbyte av information dem emellan och hur myndigheterna samarbete skall gå till (FL 4-7§§).

   - Tillämpningen skall vara frivillig för myndigheter och ses som en servicefunktion. Myndigheter med större säkerhetskrav (såsom ex militären) skall kunna ha egna lösningar/ varianter av denna lösning, men minst möta upp till de gemensamma kraven.

7. En myndighet förslagsvis SKV som har den omfattande arbetsgivare och momsredovisningsverksamheten bör ges i uppdrag att säkerställa att ***juridiska personers all myndighetsrapportering skall kunna ske i digital form*** med den juridiska personens digitala identitet (ex redovisningsbyråns ombudsrapporting). Att säkerställa att myndigheten ansvarande för (2) också skall säkerställa kravet att digitala identiteter för juridiska personer fungerar, enkelt kan tillämpas.

   - Att digitala signaturer fungerar ex email, elektroniska fakturor (artikel 233 i momsdirektivet), eSKD, INK, reviderade bokslut och försäkringskassan skall fungera.
   - Hur juridiska personer digitala signaturer skall tillämpas.
     - Hur skall ansvarig ägare av den juridiska identiteten kunna fördela och ta bort betroddhet att signera den juridiska identiteten, på fysiska individer ex anställda.

8. En myndighet förslagsvis SKV som redan idag ställer kraven på genuinitet på bokföringsverifikationer i skattekontrollfrågor ***bör ges ansvaret att med klarhet definiera en gemensam syn från staten vad en originalhandling är*** i en värld av digitala handläggningsstödsystem. Den enskilde har rätt att få originalhandlingen och är den digital skall den mailas av myndigheter digitalt till den enskilde.

   - Bokföringsnämnden har liknande men inte samma krav idag, andra är förvirrade, ett betydande problem

- Frågan har stor betydelse för elektroniska reskontror för alla företag och inte minst för staten och kommuner
- BFN, BV, E-legitimationsnämnden och SKV har till stora delar arbete med register med samma innehåll, formkrav på samma data och rapporteringskrav av samma data i olika form.
  - Myndigheterna bör slås samman
  - Gemensam registrering, formkrav och rapportering bör genomföras.

9. Med anledning av regeringens IT-handlingsplan, behovet av lokal kunskap och digitala signaturers väldigt stora rationaliseringspotential i myndighetsutövning, skall ***varje statlig myndighet, kommun och domstolsverket för domstolarna ha en metodstabsfunktion*** (och medges regleringsbrev för) som ansvarar för:
   - Öka tillämpbarheten och införande av digitala signaturer i verksamheten.
   - Arbetsstudier, arbetsutvecklingsarbete och tekniskt införande av datoriserade handläggningsstödsystem genomförs på myndigheten
     - Särskilt fokus på repetitiva arbeten, vilket är vanligt i myndighetsutövning
     - Särskilt fokus på korta ner handläggningstider och ärendebalanser, det klagas fn allmänt
     - Särskilt fokus på att alla ärenden registreras och alltid har en ansvarig handläggare, att de handläggs och handläggs säkert intill preskriptionstiden. Det slarvas ofta.
     - Ansvara för att rättelser av legala och andra fel omedelbart korrigeras även om ärendet överklagats. (Staten är felfri och begår inga fel, bara tjänstemän och de skall korrigeras utan fördröjning (RF1:9).) Fungerar riktigt dålig fn.
     - Framtagande av arbetsrutiner för olika vanliga ärendetyper till stöd för handläggarna
       - Säkerställa lika handläggning för motsvarande ärenden, klagas allmänt fn
   - Säkerställa att myndigheten offentligt tillhandahåller digitaliserad myndighetsinformation som är öppen enligt offentlighetsprincipen på sin web-informationsservice.
     - Säkerställa att enhetens offentlighet och sekretess är förenlig med gällande lag och direktiv. Det finns betydande brister fn.
   - Säkerställa att enheten samarbetar med andra myndigheter och utbyter information i handläggningen. Detta är för svårt för handläggare idag.
   - Deltar i statens gemensamma rationaliseringsarbete och digitala signatursamarbete.
   - Rapporterar och får uppdrag av enhetsledningen

Vänligen

Jan Bergström