Rättssäkerhet för medborgare vid digitala signaturer i offentlig sektor

Håkan Söderström
Stockholm, Sweden
hs@soderstrom.se

Abstrakt. Digitala underskrifter har varit giltiga i EU sedan ett första direktiv 1999. Direktivet breddades radikalt i en förordning 2014 (eIDAS) som kräver att e-tjänster i offentlig sektor ska kunna användas över landsgränser i EU. Lagen förutsätter teknik som inte finns. För att ändå åstadkomma e-tjänster över landsgränser har alternativ teknik utvecklats som inte använder medborgarens egna digitala signatur. Lagen har därmed satt krokben för sig själv. Rapporten visar att den teknik som nu används möter myndigheternas behov på bekostnad av medborgarens rättssäkerhet och föreslår möjliga förbättringar.

Innehåll

1. Bakgrund och inriktning....2
2. Terminologi....2
3. Vad innebär en signatur?....2
   3.1 Hur fungerar digitala signaturer?....3
   3.2 Standardisering....3
   3.3 Tradition av bristande transparens....4
4. Identifiering jämfört med signering....4
   4.1 Federerad identifiering....4
   4.2 Federerad signering?....5
5. Att signera över landsgränser....5
   5.1 Lösning: fristående underskriftstjänst....5
   5.2 Begreppet överlämningspunkt....5
   5.3 Traditionell ärendehantering....5
   5.4 Ärendehantering med indirekt signering....6
   5.5 Myndighetens perspektiv....7
   5.6 Medborgarens perspektiv....7
   5.7 När man faktiskt signerar något....8
6. Analys....8
   6.1 Antagande om ofelbarhet....9
   6.2 Varför det ändå fungerar....9
   6.3 Sammanfattning....9
7. Slutsatser, möjliga åtgärder....10
   7.1 Var är juristerna?....10
   7.2 Springande punkten....10
   7.3 Signera enbart original....11
   7.4 Aspekter av säkerhet....12
   7.5 Kalkylerad risk....13
Appendix A: Digital eller elektronisk?....14
Appendix B: Digital signatur som datamängd....14
Appendix C: Bakgrund till ”wysiwys”....14
Appendix D: Erfarenhet är inget bevis....15
Appendix E: Ny funktion i BankID....15

1. Bakgrund och inriktning

Digitala underskrifter har varit giltiga i EU sedan ett första direktiv från 1999 [1] blev lag i medlemsländerna. År 2014 kom en reviderad och kraftigt utvidgad EU-förordning [2] [3] som gäller när detta skrivs. Den kallas ofta *eIDAS*.

En digital signatur, om den görs rätt, är inte mindre giltig än en traditionell med bläck på papper. Det är den springande punkten i lagen sedan allra första början.

Den starka ställning som personnummer har i Sverige passade utmärkt för digitala signaturer. BankID lanserades 2003. Användningen av digitala signaturer har sedan dess ökat exponentiellt och blivit vardagsmat för svenskar. Ytterligare leverantörer av e-id har tillkommit.

I och med eIDAS infördes ett radikalt breddat perspektiv. Digitala tjänster i offentlig sektor ska kunna användas av medborgare i andra EU-länder. Denna rapport tar upp konsekvenser av breddningen, bland annat sådana som påverkar medborgarens rättssäkerhet.

2. Terminologi

I lagtexten används konsekvent termen *elektronisk* identifiering och *elektronisk* signatur. Lagstiftaren såg inte skillnaden mellan budskap och bärare. En signatur är ett digitalt budskap, elektronik en möjlig bärare.

Den korrekta termen är *digital* identifiering och *digital* signatur. Se även Appendix A: Digital eller elektronisk?, sid 14.

Lagtexten skiljer på *kvalificerade* och *avancerade* digitala signaturer. Det har visat sig svårt att hålla reda på skillnaden. I denna rapport använder vi termen *certifikatbaserade* signaturer för en signatur som uppfyller lagkraven för en giltig, digital underskrift. En person som signerar kallar vi *signatär*. Mottagaren, som begär signatur, kallas *förlitande part*.

Att *validera* en digital signatur betyder att kontrollera dess giltighet.

Ett *certifikat* är en digital id-handling som entydigt pekar ut en innehavare. Innehavaren kan vara en fysisk person, men är inte begränsad till personer[1].

En *prompt* är i it-sammanhang något som visas för att en användare ska förstå att it-systemet väntar på användarens respons.

3. Vad innebär en signatur?

Lagtexten, eIDAS, lanserar ingen ny teori för begreppet signatur. Därmed förutsätter den att det vi vet om signaturer fortfarande gäller, även om den digitala kostymen är ny. Konventioner som gäller traditionella signaturer med bläck på papper borde följaktligen gå att överföra och praktisera för digitala signaturer i många fall.

1 Miljontals webbtjänster identifierar sig med certifikat.

3.1 Hur fungerar digitala signaturer?

Spårbarhet är den faktor som gör en signatur giltig. En handskriven namnteckning anses vara tillräckligt spårbar för att knyta ett dokument till en person. För att säkra spårbarheten kan man kräva vittnen.

I en digital signatur som uppfyller lagens krav på giltighet är det ett certifikat som ger spårbarhet. Villkoret är att certifikatet har en utfärdare (ofta kallad CA, Certificate Authority), som uppfyller lagens krav. En CA är en oberoende tredje part, ungefär som ett vittne, vars enda uppgift är att vara slutpunkten i en kedja av tillit. Därför är den tjänsten också reglerad i eIDAS.

Signaturen är krypterad med signatärens privata nyckel, en nyckel som ingen annan har tillgång till, inte ens certifikatets utfärdare. Krypteringen kan ”låsas upp” med signatärens publika nyckel – och enbart den.

Sammanlagt ger det en digital signatur *autenticitet* (att det är rätt person som skrivit under), *integritet* (kan inte ändras utan att göra signaturen ogiltig) och *icke-förnekbarhet* (inte trovärdigt för signatären att förneka signaturen).

Nedanstående tabell jämför en traditionell signatur och en digital.

	Traditionell	Digital
Dokument före sign.	Papper	Digital datamängd (fil)
Spårbarhet genom	Namnteckning med bläck	Certifikat: tillitskedja som slutar med betrodd CA
Knytning till dokument	Bläck förenas med pappers-fibrer	Kryptering med signatärens privata nyckel
Dokument efter sign.	Fysiskt papper	Digital datamängd (fil)
Kopiering	Kopia bryter giltigheten	Giltig efter kopiering

I en traditionell signatur är bläcket i handskriften oupplösligt förenat med ett papper. I en digital signatur är personens certifikat oupplösligt förenat med ett digitalt dokument. Det finns en parallell.

Den stora skillnaden mellan traditionell och digital signatur gäller kopiering. I den digitala världen finns inte begreppen original och kopia. Därför är en digital kopia av ett digitalt signerat dokument lika giltig som originalet.

3.2 Standardisering

Digitala signaturer är föremål för internationell standard. De innehåller inga affärshemligheter. Detta är i högsta grad avsiktligt för att varje signatur ska kunna valideras av en oberoende tredje part, någon som inte är inblandad i det ärende som signaturen gäller.

Det är en tillgång att giltigheten kan prövas opartiskt vid en eventuell tvist. Även en signatär med små resurser kan få rätt mot en stor organisation med många jurister. Det förutsätter dock att signatären har tillgång till sin egen signatur.

3.3 Tradition av bristande transparens

Konventionen för traditionella underskrifter är att man framställer flera likalydande exemplar av en handling. Varje signatär får ett exemplar med alla underskrifter i original.

Digitala underskrifter borde lätt kunna följa denna konvention, men så är det inte i offentlig sektor[2]. Ingen medborgare har någonsin erbjudits en kopia av sin egen digitala underskrift. Med tiden har denna bristande transparens cementerats till en dålig vana som tas för given. Man kan inte säga att den bidrar positivt till medborgarens rättssäkerhet.[3]

4. Identifiering jämfört med signering

E-tjänster måste veta vem som loggar in. Certifikatbaserad *identifiering* säkerställer identiteten hos användare med hög tillförlitlighet.

En certifikatbaserad identifiering resulterar i en datamängd. Den består framför allt av medborgarens certifikat med bland annat personnummer. Dessutom bär den en tidstämpel och information om den teknik (exempelvis mobiltelefon) medborgaren använt vid identifieringen.

Utåt, mot medborgaren, använder man ofta ordet *legitimering* snarare än identifiering eftersom det stämmer med vardagligt språkbruk. Det användaren ser är en standardtext, exempelvis ”Jag legitimerar mig hos [*förlitande part*]”, där *förlitande part* ersätts av namnet på den som tar emot identifieringen, exempelvis ”Bolagsverket”.

En *signering* har, till skillnad från identifiering, alltid ett *föremål*, något man signerar. Detta något kan vara en godtycklig datamängd. Vi kallar det *dokumentet*. Utöver dokumentet innehåller en typisk signatur samma information som en identifiering.

4.1 Federerad identifiering

I och med eIDAS behöver it-system i olika EU-länder kunna hantera och lita på personliga identiteter som inte är landets egna. Tekniken för detta kallas *federerad identifiering*, ett omfattande teknikområde.

Här konstaterar vi bara att eIDAS, som gemensam EU-lagstiftning, är nödvändig för federerad identifiering eftersom tekniken förutsätter ömsesidig tillit och samordning mellan ländernas system.

I Sverige tillhandahåller Myndigheten för digital förvaltning (DIGG) en tjänst för federerad identifiering som både offentliga och privata aktörer kan ansluta sina e-tjänster till [4].

2 Eller i bankvärlden.

3 Se även Appendix B: Digital signatur som datamängd, sid 14.

4.2 Federerad signering?

Man skulle kunna tänka sig federerad signering, att man kunde göra digitala underskrifter över landsgränser. Den tekniken finns inte för närvarande.

5. Att signera över landsgränser

Lagen föreskriver att medborgare i EU-länder ska kunna använda andra EU-länders digitala tjänster i offentlig sektor. En svårighet är att alla EU-länder har olika system och olika regler för personlig identitet.

Det första steget i en e-tjänst är inloggning, det vill säga identifiering. Det går numera att ordna med federerad identifiering, som nämns i avsnitt 4.1. Värre är det med digital underskrift. En underskrift är slutklämmen i nästan alla e-tjänster. Man lämnar exempelvis in en ansökan som ska signeras.

Lagen påbjuder att detta ska kunna göras över landsgränser, men teknik saknas. Någon ”federerad signering” existerar inte. Lagen kräver alltså en funktion som inte går att realisera i dagsläget. Det kan man kalla en utmaning.

5.1 Lösning: fristående underskriftstjänst

It-människor har som yrke att lösa problem och därför har även signerings-problemet fått en lösning. Den kallas *indirekt signering.* Det innebär att signeringen ersätts av en extra identifiering.

DIGG förespråkar att svenska myndigheter gör detta på ett visst sätt, nämligen i en *fristående underskriftstjänst*. Funktionen hos en fristående underskrifts-tjänst specificeras i detalj i [5]. I princip fungerar den som en underskrifts-robot, ett mekaniskt ombud som producerar underskrifter.

För medborgaren ser en indirekt signering ut exakt som en identifiering vilken som helst. Det beror på att den *är* en identifiering vilken som helst, det finns inga andra.[4]

5.2 Begreppet överlämningspunkt

Vi definierar här termen *överlämningspunkt* som markerar tillfället när en medborgare lämnar över (eller lämnar in) sina uppgifter till en myndighet och därmed startar ett ärende hos myndigheten. Överlämningen kan vara digital eller traditionell med pappersblankett.

5.3 Traditionell ärendehantering

Vi gör en kort tillbakablick på ärendehantering med pappersblankett.

4 Se dock Appendix E: Ny funktion i BankID, sid 15

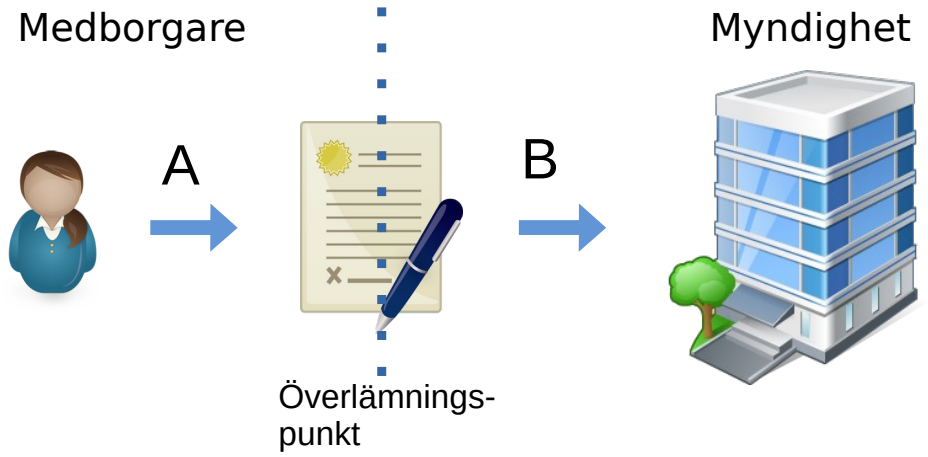

Fig 1: Traditionell ärendehantering med överlämningspunkt

Medborgaren startar ett ärende hos myndigheten genom att överlämna en undertecknad pappersblankett.

Bokstaven A betecknar ”utdata” från medborgaren. B är ”indata” till myndigheten. Den prickade linjen är överlämningspunkten, ansvarsgränsen mellan medborgare och myndighet. A och B är identiska, ingenting händer när data passerar överlämningspunkten. Medborgaren vet exakt vad som är inlämnat, nämligen identiskt samma blankett som myndigheten har tagit emot.

5.4 Ärendehantering med indirekt signering

Nästa illustration visar ett ärende som startas digitalt med indirekt signering. Skatteverket är exempel på en myndighet som arbetar på detta sätt.

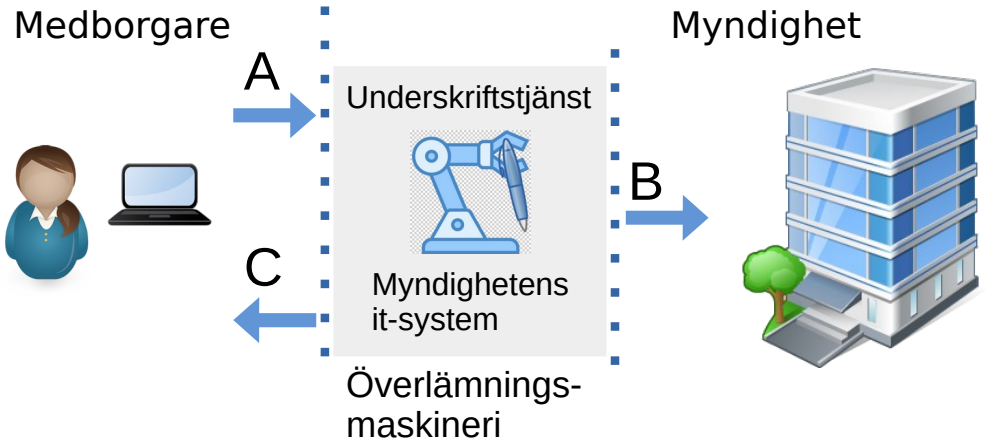

Fig 2: Aktuell digital ärendehantering

Den stora skillnaden mot traditionell hantering är att det finns ett avstånd mellan A, det som medborgaren lämnar in och B, det som myndigheten tar emot.

I stället för att passera en överlämningspunkt där ingenting händer passerar data från medborgaren ett överlämningsmaskineri. Vi går igenom processen ur myndighetens respektive medborgarens perspektiv.

5.5 Myndighetens perspektiv

Lösningen med indirekt signering i en underskriftstjänst uppfyller myndighetens krav eftersom dessa har drivit utvecklingen av lösningen. Kreativitet och yrkeskunskap är nerplöjda i överlämningsmaskineriet så att myndigheten kan lita på att indata (B ovan) i ett ärende är autentiska och indirekt signerade av rätt person. Myndighetens krav är därmed uppfyllda.

5.6 Medborgarens perspektiv

Medborgaren skapar ärendet i en interaktiv dialog som kan omfatta flera skärmbilder. Det medborgaren uppfattar som utdata till myndigheten (A ovan) är synintrycket från en eller flera skärmbilder.

När det blir dags för signering uppmanas medborgaren att identifiera sig en extra gång. Den prompt som visas för medborgaren är den vanliga för identifieringar, till exempel: *Jag legitimerar mig hos Skatteverkets Underskrifttjänst* (om det nu gäller Skatteverket).

Vem kan ana att identifiering i en underskriftstjänst har helt andra konsekvenser än andra identifieringar? Den anses nämligen ge underskriftstjänsten fullmakt att signera å medborgarens vägnar. Underskriftstjänsten kan ses som en robot och symboliseras därför av en robotarm med penna i figuren.

Roboten signerar indata till myndigheten (B), en XML-fil[5] som skapas av överlämningsmaskineriet och som aldrig visas för medborgaren.

Från överlämningsmaskineriet får medborgaren ett kvitto (C) som innehåller information om ärendet som just har startats.

Några iakttagelser:

- Indata till myndigheten (B) är något annat än vad medborgaren tror sig ha lämnat in (A). Det är signerat av roboten, inte medborgaren.
- Kvittot (C) är också något annat än medborgarens utdata (A) och även något annat än myndighetens indata (B).

Inte så att (A) och (B) nödvändigtvis motsäger varandra, inte heller (A) och (C). Det är ändå ett problem att **inte vid någon punkt har medborgaren och myndigheten *identisk* information i ärendet**.

Även utan att veta vad som händer bakom kulisserna borde den indirekta signeringen väcka förvåning.

- En tänkande medborgare borde undra hur man kan underteckna något utan att göra en signering. De flesta känner ju till hur man signerar ärenden hos banker och kan skilja mellan identifiering och signering.
- Under identifieringen ser man inte vad som anses bli signerat. Sambandet mellan signering och dess föremål är underförstått. Innebörden är ”du skriver under det där du såg nyss”.

Man skulle kunna tro att den extra identifieringen innehåller en osynlig referens till ärendet. Så är dock inte fallet. Om medborgaren fick en kopia av

5 XML är ett textformat som är olämpligt för mänsklig kommunikation.

sin identifiering (vilket aldrig har hänt) skulle man se att den, liksom identifieringar i allmänhet, saknar information om sitt sammanhang. En identifiering är en identifiering[6].

5.7 När man faktiskt signerar något

Ibland förekommer en verklig signering. Här är ett autentiskt exempel som handlar om att signera sin inkomstdeklaration med BankID hos Skatteverket.

I BankID-appen visas rubriken *Jag skriver under hos Skatteverkets Underskrifttjänst*. Dokumentet som ska skrivas under lyder *Jag legitimerar mig mot Skatteverkets underskrifttjänst*. Den foglige medborgaren skriver alltså under ett dokument vars text i sin helhet är: *Jag legitimerar mig mot Skatteverkets underskrifttjänst*. Även bortsett från det tvetydiga budskapet (skriver jag under eller legitimerar jag mig?) har dokumentets innehåll inte minsta relevans för det ärende som behandlas.

En tänkande medborgare borde undra varför man ska signera ett dokument vars innehåll är nonsens. Svaret är att denna signering anses ge fullmakt åt underskriftsroboten att signera i medborgarens namn det som verkligen är relevant för ärendet.

6. Analys

För signaturer, traditionella eller digitala, finns en principen ”what you see is what you sign”, *wysiwys*, ”det du ser är det du skriver under”[7]. Den kan konkretiseras i **tre kriterier**.

1. För att kunna signera något måste man se det
2. Det man binder sig till när man signerar är begränsat till det man ser
3. För att en signatur ska vara meningsfull måste det gå att i efterhand återge det man såg och signerade

Kriterierna är självklarheter eller rentav naturlagar som omöjligt kunde åsidosättas innan signaturer blev digitala.

Överlämningsmaskineriet åsidosätter alla tre.

Medborgaren anses ha (indirekt) signerat myndighetens indata (B), ofta en XML-fil, men har aldrig sett den (wysiwys kriterium 1).

När man gör den extra identifiering som anses vara en signering ser man inte vad man signerar (kriterium 2).

Medborgaren får ett kvitto på startat ärende (C). Det är ändå inte samma data som medborgaren tror sig ha signerat (kriterium 3) utan ett härlett dokument skapat av överlämningsmaskineriet.

Den digitala signatur som skapas för myndighetens indata (B) görs av en underskriftsrobot. Den extra identifieringen innebär att medborgaren ger

6 Se dock Appendix E: Ny funktion i BankID, sid 15.

7 För ytterligare bakgrund: se Appendix C: Bakgrund till ”wysiwys”, sid 14

fullmakt åt roboten att som ombud skriva under ett underförstått dokument i medborgarens ställe.

6.1 Antagande om ofelbarhet

Myndighetens maskineri för att ta emot ärenden digitalt är tämligen komplicerat, vilket om inte annat framgår av den omfattande tjänstespecifikationen [5]. Trots det vilar maskineriet på ett antagande om ofelbarhet och kräver obegränsad tillit av medborgaren.

Misstag från myndigheten när ett ärende väl har startat kan överklagas på vanligt sätt. Att något skulle hända i själva överlämningsmaskineriet är så att säga omöjligt och går därmed inte att överklaga[8].

Vi talar nu om pålitliga myndigheter med goda avsikter. I en sämre värld är överlämningsmaskineriet en säkerhetsmässig kortslutning.

6.2 Varför det ändå fungerar

Om det är så mycket fel kan man undra: varför fungerar det alls?

Digitala tjänster är uppskattade. Svenskar litar på sina myndigheter. Myndigheterna har, som exempelvis Skatteverket, byggt upp förtroende hos medborgarna genom att visa sig pålitliga år efter år.

6.3 Sammanfattning

Ett av EU:s viktigaste mål är fria flöden mellan EU-länder. Lagen (eIDAS) föreskriver följdriktigt att digitala tjänster i offentlig sektor ska kunna användas över landsgränser i EU-länder.

Eftersom teknik för detta saknas används indirekt signering. En extra identifiering ersätter en regelrätt digital signatur. I processen uppstår flera anomalier:

- Medborgaren signerar aldrig något med sin egna digitala signatur
- Om en verklig signering ändå utförs av medborgaren avser den ett dokument vars innehåll är nonsens för ärendet ifråga
- När medborgaren utför den identifiering som anses motsvara signering går det inte att se dokumentets innehåll. Medborgaren gör alltså den indirekta signeringen med förbundna ögon.
- Medborgaren har i många fall aldrig sett det indirekt signerade dokumentet (det genereras av överlämnginsmaskineriet) men anses ändå ha signerat det
- Till skillnad från en regelrätt digital signatur kan indirekt signering inte prövas av oberoende tredje part (jämför 3.2, sid 3).

Indirekt signering är utformad så att myndigheten kan lita på att det som produceras på detta sätt är autentiskt. Det som blir lidande är rättssäkerhet för medborgaren.

8 Se även Appendix D: Erfarenhet är inget bevis, sid 15.

7. Slutsatser, möjliga åtgärder

Det finns enkel, öppen och tillförlitlig teknik för digital underskrift, det vi kallar certifikatbaserade signaturer. Sådana signaturer har varit juridiskt bindande i EU sedan början av 2000-talet.

Den breddade lagen, eIDAS, som kom 2014, utvidgade tillämpningen till e-tjänster över landsgränser i EU. Grunden för certifikatbaserade signaturer är oförändrad. Däremot har breddningen i praktiken och efter avsevärda investeringar *avskaffat* digitala signaturer i offentlig sektor. I detta avseende är eIDAS ett grandiost självmål som inte kan undgå att skapa frågetecken kring själva lagstiftningsprocessen.

Oavsett lagens brister måste svenska myndigheter och i första hand DIGG anpassa sig till eIDAS – naturligtvis. Något annat är inte tänkbart. Även med de bästa avsikter har syftet med eIDAS bara kunnat nås på omvägar, nämligen med *indirekt* signering där medborgaren enbart *legitimerar* sig i en underskriftstjänst och aldrig *signerar* något.

Kapitel 6, Analys, sid 8, visar hur medborgarens rättssäkerhet äventyras genom att det finns ett överlämningsmaskineri mellan medborgaren och myndigheten som åsidosätter självklarheter för signering.

Det är omöjligt att nå en lika tillförlitlig lösning med indirekt signering som med en regelrätt certifikatbaserad signatur. På några punkter finns dock möjliga förbättringar inom ramen för bibehållen indirekt signering.

7.1 Var är juristerna?

Digitala underskrifter är juridik i praktisk tillämpning. Frånvaron av jurister inom området är slående. Kan det vara så att digitala underskrifter har kommit att hanteras som en it-fråga? Det skulle i så fall delvis förklara att de juridiska problem som nämns i denna rapport fått så lite uppmärksamhet.

Kanske problemen börjar redan i eIDAS [2]? I de inledande skälen (nr 9) nämns ”elektroniska hinder” för gränsöverskridande e-handel. Detta trots att gränsöverskridande e-handel var vardagsmat för medborgare i EU-länder redan innan eIDAS och utan någon EU-gemensam infrastruktur. Det som däremot stötte på hinder var att använda andra länders tjänster i offentlig sektor. Att kategorisera hindret som ”elektroniskt” antyder att lösningen också är ”elektronisk” och kan förverkligas av it-konsulter – ett önsketänkande.

7.2 Springande punkten

Den springande punkten i indirekt signering är att det inte går att se vad man skriver under i själva underskriftsmomentet. Det finns för närvarande ingen teknisk lösning för det. I pappersvärlden skulle det motsvara att man signerar ett universaldokument vars text i sin helhet är ”Jag undertecknar härmed det där andra jag såg nyss”. Föremålet för underskriften är långt ifrån väldefinierat.

Processen vilar på ett förtroende, att förlitande part (den som tar emot underskriften) hanterar underskriften på ett ansvarsfullt sätt.

I många fall saknas även en väldefinierad överlämningspunkt där myndighet och medborgare har identisk information i ärendet. Det är då svårt att ens teoretiskt definiera vad underskriften gäller.

7.3 Signera enbart original

Överlämningsmaskineriet är den funktion som tar emot indata från medborgaren och startar ett ärende. Det består nu av två sammanslagna funktioner (se även 5.4, sid 6).

1. Bearbetning av indata till en form som är lämpad för myndighetens hantering
2. Indirekt signering

I dagsläget anses medborgaren signera resultatet av (1), data som de aldrig har sett eller kommer att får se. Medborgaren borde inte behöva signera något annat än sin egen information i original.

Bearbetningen (1) anses ofelbar och är oåtkomlig för medborgaren. Den görs ju innan det finns något ärende och kan inte överklagas.

Exempel: En medborgare gör en momsdeklaration på nätet och uppger momsbelagd försäljning till 10.000:-. En bug i överlämningsmaskineriet[9] medför att Skatteverket ser försäljningssumman 10.000.000:- och kräver därför medborgaren på 2,5 miljoner kronor i utgående moms. Den förbryllade medborgaren lämnar då in en ”korrigerad” momsdeklaration, men buggen är kvar, och därmed även momskravet som ett potentiellt konkurshot.

Medborgaren löser till slut problemet genom att lämna momsdeklarationen på pappersblankett. Pappersblanketter har en väldefinierad överlämningspunkt vilket utesluter denna typ av problem.

Lösning: Det enda rimliga är att ta bort funktionen (1) från överlämnings-maskineriet. Kvar blir bara den indirekta signeringen. Signering ska inte göras på något annat än original som medborgaren har full tillgång till.

Figur 3 visar en möjlig realisering i skissform.

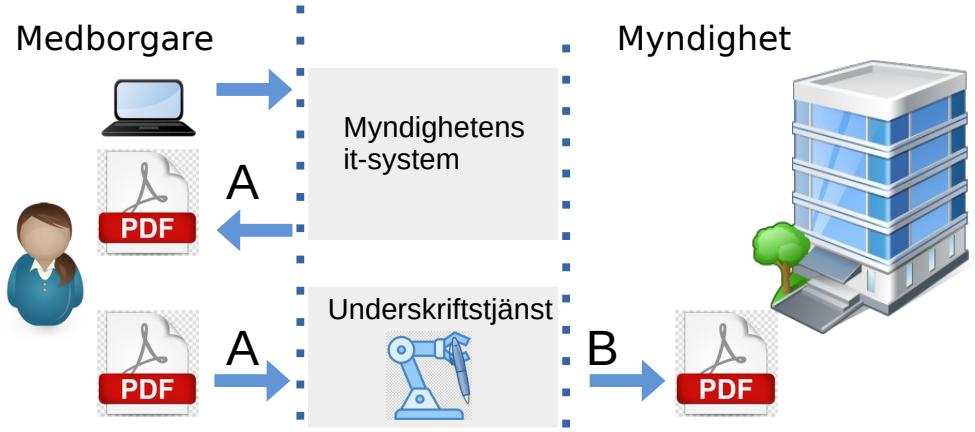

Fig 3: Digital ärendehantering med överlämningspunkt

De två funktionerna i överlämningsmaskineriet är nu separerade.

9 Se även Appendix D: Erfarenhet är inget bevis, sid 15

Medborgaren förbereder underlag för ett nytt ärende i en interaktiv dialog med myndighetens it-system, precis som tidigare. Det nya är att resultatet blir **ett konkret dokument** (A). (Vi förutsätter här PDF-format [6].) Medborgaren har full tillgång till dokumentet och kan till exempel spara det på sin egen enhet.

Vid lämplig tidpunkt lämnar medborgaren in dokumentet till myndigheten. Det passerar då underskriftstjänsten och förses med indirekt robotsignatur. Någon annan förändring görs inte. Vi har uppnått att det finns en överlämningspunkt där medborgaren vet exakt vad som är inlämnat (A). Det är exakt samma information, signerad, som myndigheten tar emot (B). (Se även 5.3, sid 5.) Säkerligen behöver myndigheten bearbeta informationen ytterligare. Det är fritt fram, det påverkar inte vad som anses vara indata till ärendet. Någon ofelbarhetsdoktrin behövs inte. Eventuella buggar blir ett internt problem för myndigheten.

För full transparens bör medborgaren erbjudas ladda ner kopia av B, det vill säga identiskt samma information som myndigheten fått.

I termer av kriterierna för wysiwys (se sid 8) uppfylls kriterium 1 på så vis att medborgaren vet exakt vad som är inlämnat. Kriterium 3 är uppfyllt eftersom medborgaren har möjlighet att spara underlaget på sin egen enhet. Med indirekt signering kan aldrig kriterium 2 uppfyllas eftersom man inte kan se vad man signerar under själva signeringsoperationen.

7.4 Aspekter av säkerhet

Säkerhet i it-sammanhang baseras på kryptografiska metoder. Säkerheten i en regelrätt certifikatbaserad digital signatur ligger i krypteringen.

Det som inte är kryptografiskt är ad hoc, alltså ”vi gör så gott vi kan”. Det må vara aldrig så intrikata lösningar – men utan kryptografisk styrka är de inte säkra.

Underskriftsroboten i indirekt signering producerar faktiskt en giltig digital signatur, men den ingår i en kedja med en betydligt svagare länk. Den svaga länken är sambandet mellan att medborgaren legitimerar sig i underskrifts-tjänsten och att roboten aktiveras. Det sambandet är ad hoc.

Har man en gång bestämt sig för att avstå från kryptografisk säkerhet (genom att avstå från regelrätta signaturer) går det inte att uppnå samma säkerhet på annat sätt. Det är slutgiltigt, av teoretiska skäl.

En annan aspekt av säkerhet går däremot att åtgärda: *begriplighet*. Varje obegriplighet i ett it-system är ett potentiellt säkerhetshål.

Något borde göras åt de moment i indirekt signering som är obegripliga för medborgaren eller som är ”felskyltade”. Det är inte bra att vänja en hel befolkning att klicka ”OK” efter ”OK” genom obegripliga processer.

Startpunkten för indirekt signering illustrerar detta. Medborgaren ser en prompt som liknar följande. Myndighetens namn varierar naturligtvis.

- Jag legitimerar mig hos Skatteverkets Underskrifttjänst

Att man legitimerar sig betyder i normalt språkbruk att man blir passivt insläppt genom en dörr, bokstavligen eller i överförd bemärkelse i ett it-system.

Att legitimera sig mot en underskrifttjänst är däremot en aktiv åtgärd som får konsekvenser. Legitimeringen ger fullmakt åt underskriftsroboten att underteckna en handling för medborgarens räkning och lämna in den till myndigheten. (Se även avsnitt 5.6, sid 7.)

BankID har meddelat att det ska bli möjligt att ange avsikten med en identifiering[10]. Detta kan bli ett sätt att informera svenska medborgare om innebörden av en indirekt signering. Annars är det obegripligt för medborgaren att ”legitimera sig” skulle innebära att man anses underteckna och lämna in en handling.

Själva prompten ”Jag legitimerar mig hos…”, definieras av det e-id-system medborgaren använder, inte av myndigheten.

Liknande gäller fallet när medborgaren faktiskt signerar något vars innehåll saknar relevans för ärendet. Resultatet är även då att man ger fullmakt åt underskriftsroboten att underteckna och lämna in en handling i medborgarens namn. Medborgaren bör informeras om detta.

7.5 Kalkylerad risk

Trots betänkligheterna som radas upp i tidigare avsnitt fortsätter digitala tjänster i offentlig sektor att rulla på med framgång. Det som gör att tjänsterna fungerar och används av många medborgare är att medborgarna litar på myndigheterna. Med rätta, för svenska myndigheter är pålitliga.

Det är ändå en viss skillnad mellan att vara pålitlig och att vara ofelbar. Medborgaren förväntas nu ha obegränsad tillit till myndigheten men erbjuds inte mycket till transparens i överlämningsmaskineriet. Det finns ingen oberoende tredje part som kan vara ”vittne”.

Skulle något inträffa som kastar tvivel över exempelvis Skatteverkets pålitlighet finns en uppenbar risk att medborgare raskt återgår till det som har en tydlig överlämningspunkt, nämligen pappersblanketter. Förtroende kan förloras på ett ögonblick. Många års digitalisering kan plötsligt ersättas av floder av papper.

10 Se Appendix E: Ny funktion i BankID, sid 15

Appendix A: Digital eller elektronisk?

Lagstiftaren har tyvärr inte sett skillnaden mellan budskap och bärare. En signatur är ett *digitalt* budskap. Det kan bäras av olika medier, bland annat elektronik, men även till exempel papper i form av en utskriven QR-kod.

Att kalla digitala signaturer ”elektroniska” är ett sakfel som upprepas flera hundra gånger i lagtexten och smittar av sig på relaterad dokumentation. Att upprepa ett sakfel med så hög frekvens kan inte undgå att skapa frågetecken för lagstiftarens kompetens.

Appendix B: Digital signatur som datamängd

En digital signatur är en datamängd som på flera sätt kan jämföras med ett Word-dokument. Båda kan lagras som en fil på en dator, i en mobil eller på en minnespinne. Filstorleken kan variera, men som ett Word-dokument på ett tiotal sidor är vanligt.

Precis som det krävs ett program (Word) för att återge ett Word-dokument på skärmen krävs det ett program för att återge innehållet i en digital signatur.

En digital signatur kan kopieras och spridas obegränsat utan att förlora sin giltighet. Inget hindrar därför att en signatär får en kopia av sin signatur.

Det är ändå ovanligt att medborgare har behov av en kopia av sin digitala underskrift i offentlig sektor. I händelse av tvist bör medborgaren medges skälig insyn i sitt eget ärende. En kopia av ens egen underskrift måste anses skäligt och erbjudas för nedladdning.

Appendix C: Bakgrund till ”wysiwys”

Termen *what you see is what you sign* myntades redan före det första EU-direktivet om digitala signaturer, alltså [1]. Digitala signaturer var då ett aktivt forskningsområde. En viktig fråga gällde att ett digitalt dokument strängt taget är en följd av binära bitar som inte kan tolkas av människan. Ett program krävs för att omvandla bitföljden till något begripligt på en skärm eller en skrivare.

Det man ser är alltså en kraftig bearbetning av det som *är* dokumentet. Det man signerar är dock bitföljden. Hur kan man veta att det man ser motsvarar bitföljden?

Resonemangen landade i självklarheten att man inte kan anses signera något annat än det man ser, alltså ”wysiwys”.

Som en påminnelse om diskussionerna i början på 2000-talet finns följande kod i varje signatur från BankID:

```
<usrVisibleData ... visible="wysiwys">
```

Denna kod markerar början på det som visas för signatären vid signering.

Appendix D: Erfarenhet är inget bevis

Detta appendix handlar om testning av it-system. Det it-system vi har kallat överlämningsmaskineriet är givetvis väl testat.

För test av it-system gäller ändå regeln: erfarenhet kan aldrig bevisa, bara motbevisa. Tusen vita vitsippor bevisar inte att alla vitsippor är vita. Däremot räcker en enda röd vitsippa för att motbevisa att alla vitsippor är vita.

På samma sätt kan test av it-system bara påvisa fel, aldrig bevisa korrekthet. Att ett it-system passerar en testsvit utan fel betyder bara att det saknas testfall som detekterar de återstående felen.

Ett aktuellt exempel på oupptäckt fel är Skatteverkets utskick av förifyllda digitala deklarationsunderlag mars 2022.

Dessvärre är det lika svårt att testa perfekt som att skapa ett perfekt it-system.

Appendix E: Ny funktion i BankID

BankID annonserar 2022-02-09 en ny funktion vid identifiering. Ett extra textfält ska göra det möjligt att ange en avsikt vid identifieringen. Därmed finns teknik för att stödja förbättringar som skissas i avsnitt 7.4, sid 12 – för svenska medborgare.

Referenser

[1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[2] EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG

[3] Lag (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

[4] DIGG, Myndigheten för digital förvaltning, ”Sweden Connect”. Utförlig dokumentation finns på www.swedenconnect.se

[5] DIGG, Myndigheten för digital förvaltning, ”Tjänstespecifikation för fristående underskriftstjänst”, version 1.40, 2020-04-22. Länk: https://www.digg.se/dokument/diid/normativ-specifikation/tjanstespecifikation. Läst 2021-11-26.

[6] Adobe Systems: ”Document management – Portable document format – Part 1: PDF 1.7”. http://wwwimages.adobe.com/www.adobe.com/content/dam/acom/en/devnet/pdf/pdfs/PDF32000_2008.pdf (Länken går till Adobe eftersom ISO tar betalt för standardpublikationer.)