Teknisk implementering av SAMSET:s Legala Användargränssnitt

Innehåll

1 Bakgrund

SAMSET har tagit fram ett regelverk (RSV M 2001:35) som i allt väsentligt har en *traditionell juridisk språkdräkt.*

Som ett nästa steg har SAMSET dessutom tagit fram ett dokument med s.k. legala gränssnitt. Dokumentet om gränssnitt är av vikt för att kunna införa juridiskt gångbara lösningar *så att användarna intuitivt kan* ***se och förstå*** vad de gör och därmed litar på funktioner och tjänster och använder dem rätt.

På motsvarande sätt har ett mycket stort antal tekniska standarder tagits fram på PKI-området och en rad lösningar har utvecklats på marknaden. Delvis med stöd av dessa standarder har gränssnitt och metoder skapats som på olika sätt påverkar möjligheten att realisera SAMSETs målsättningar.

1.1 Studien

Studiens målsättning har varit att på ett övergripande plan strukturera dessa frågor, ställa upp rimliga mål och visa på fungerande metoder för att införa SAMSETs legala gränssnitt. Studien skall även belysa viktiga vägval mellan vad som kan åstadkommas med hjälp av marknadens standardverktyg respektive med specialutvecklade stödfunktioner som medborgare kan ges tillgång till.

Frågorna sorteras enligt följande:

A. Föreslår SAMSET i gränssnittsriktlinjerna – i någon del – en lösning som är
   a) helt orealistisk,
   b) orealistisk idag men som bör drivas för genomförande inom två år,
   c) realistisk redan idag men behöver visst stöd, eller
   d) direkt användbar eftersom stöd redan finns?

B. För förslag som faller under b – d ovan är det viktigt att klarlägga vem som bör göra vad och i praktiken har möjlighet att påverka gränssnittet.
   a) Skall gränssnittsfrågan hanteras inom ramen för e-tjänsten eller ID-tjänsten?
   b) Är det en mjukvara som behövs eller är det bara ytterligare grafik och text?
   c) Hur kan *realistiska* steg tas framåt?
   d) Vilken långsiktig utveckling bör ske?

I studien har ingått att avstämma resultat och påverka utformningen av [Legala Användargränssnitt]. I de preliminära resultaten av denna studie fanns en rad invändningar som kunnat elimineras efter avstämningsprocessen. Det resultat som redovisas nedan avser utformningen av [Legala Användargränssnitt] efter avstämning mot denna studies resultat.

1.2 Bemanning

Studien har utförts av Stefan Santesson. Retrospekt AB.
stefan@retrospekt.com
Avstämning mot [Legala Användargränssnitt] har utförts av Stefan Santesson i samverkan med Per Furberg.

1.3 Terminologi

Denna studie har tagits fram främst för att belysa SAMSETs Legala Användargränssnitts praktiska realiserbarhet.

Denna studie använder delvis en något mer teknisk terminologi än den i SAMSETs riktlinjer. Läsaren förutsätts vara ytligt bekant med en rad begrepp som används i tekniska beskrivningar av PKI-relaterade tjänster.

Språkbruket har anpassats för att någorlunda effektivt redovisa studiens resultat för SAMSETs interna behandling.

I denna studie används omväxlande begreppet ”certifikat” och synonymen ”e-legitimation” som beskrivande koncept för intyg i elektronisk form av en utfärdare som kopplar ihop ett nyckelpar med en Innehavare och bekräftar vem Innehavaren är – jfr en vanlig ID-handling – som uppfyller kraven enligt riktlinjerna.

En användare av en e-tjänst, för vilken certifikat har utfärdats, benämns ”Innehavare”.

2 Sammanfattning

Studien har så långt det är möjligt försökt att översätta [Legala Användargränssnitt] till en enhetlig teknisk verklighet. Detta låter sig inte alltid göras, dels på grund av att den tekniska verkligheten inte är enhetlig i sig, dels för att den tekniska verkligheten är uppbyggd helt eller delvis enligt andra grundläggande principer.

Följande tabell är en grov beskrivning av realiserbarheten av [Legala Användargränssnitt].

	Realiserbarhet enligt [Legala Användargränssnitt]			
	Orealistiskt	Realistiskt inom 2 år	Realistiskt men behöver stöd	Direkt användbar
Legitimera			X	
Presentera e-legitimation		X		
Granska				X
Underteckna			X	
Skicka				X

Gränssnitt som bedöms som realistiska men i behov av stöd innebär att användargränssnittet realiseras i samverkan med lokala klientkomponenter som kan behöva anpassas för att uppnå fullständigt överensstämmelse med [Legala Användargränssnitt]. Dock bedöms gränssnittet som i huvudsak direkt realiserbart med användning av vanligt förekommande standardkomponenter.

Ett potentiellt problem, som är indirekt kopplat till gränssnitten, utgörs av den konceptuella sammankopplingen mellan gränssnitten ”Underteckna” och ”Skicka”. Många av dagens applikationer och webbformulär tillhandahåller inte dessa funktioner som separata steg. Vanligtvis aktiveras funktionen underteckna först när användaren väljer funktionen skicka. Jämför även med e-post där valet att signera resulterar i att signatur skapas först när meddelandet skickas.

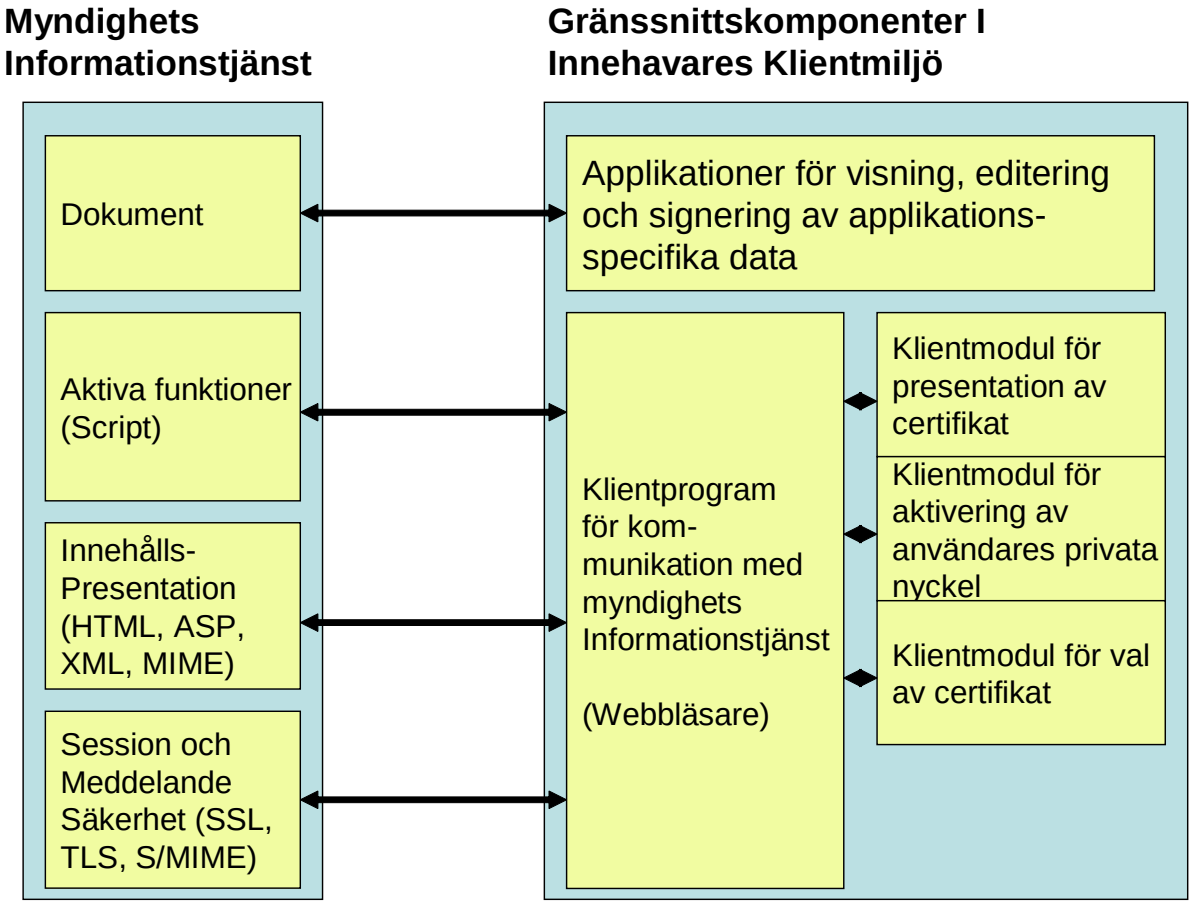
Bedömningen av gränssnittens realiserbarhet ovan avser endast när gränssnittet ”underteckna” är separerat från gränssnittet ”skicka”. Det bör dock påpekas att detta förfaringssätt, om än inte är tekniskt orealiserbart, förmodligen inte representerar det vanligaste förloppet i webbtjänster.

Denna studie visar på olika möjligheter och principer vid realisering av [Legala Användargränssnitt] men den utgör inte en komplett beskrivning av alla lösningar. Mycket bestäms även av marknadens parter och deras kreativitet. Denna studie föreslår därför att man uppdrar åt någon/några tillhandahållare av ID-tjänster (ex. Posten och Bankernas ID-tjänst), samt tillhandahållare av klientmiljöer (ex. Microsoft), att visa på hur och på vilket sätt man kan/vill stödja riktlinjerna.

3 Användargränssnittets uppbyggnad

3.1 Moduler

De gränssnitt som behandlas i SAMSETs Legala Användargränssnitt förverkligas i praktiken genom en rad gränssnittsmoduler i Innehavarens klientmiljö som på ett mer eller mindre enhetligt sätt översätter information och instruktioner i myndigheternas E-tjänster till information, grafiska element, förklarande texter och interaktiva komponenter i Innehavarens användargränssnitt.



I [Legala Användargränssnitt] definieras endast gränssnitt som rör utformningen av webbtjänster medan applikationer för läsning och bearbetning av dokument lämnats utanför riktlinjerna. Denna studie av möjligheterna att genomföra SAMSETs [Legala Användargränssnitt] tar därför sikte på utformningen av myndigheternas webbaserade e-tjänster.

Förklaringar av relevanta gränssnitskomponenter

1	Myndighets e-tjänst	Webbtjänst för aktiv interaktion med myndighet
2	Klientprogram för kommunikation med myndighets e-tjänst	I denna studie avses endast webbläsare. Denna modul styr vilken typ av lösning som tillämpas för 2a-2d
2a	Klientmodul för presentation av certifikat (e-legitimation)	Denna modul aktiveras av klientprogrammet (2) och av andra applikationer i klientmiljön, då ett certifikats informationsinnehåll skall presenteras för Innehavaren. Det kan finnas olika moduler för presentation av certifikat i samma dator. Det är här applikationen alternativt applikationens tillämpade säkerhetsbibliotek som styr val av denna modul i det fall flera moduler finns tillgängliga.
2b	Klientmodul för aktivering av Innehavares privata nyckel	Denna modul styrs av vilken lösning för lagring av privat nyckel som Innehavaren använder (t.ex. smart kort, USB-enhet eller mjukvara) I de flesta fall utgörs detta av en s.k. CSP. (Cryptographic Service Provider) men i vissa fall används även andra lösningar som t.ex. PKCS#12 modul i Netscape.
2c	Klientmodul för val av certifikat (e-legitimation)	Denna modul i Innehavarens klientmiljö aktiveras när något av Innehavarens certifikat skall användas, t.ex. vid säker inloggning på en webbtjänst, särskilt då Innehavaren har flera certifikat att välja mellan.
3	Applikationer för presentation, editering och signering av elektroniska handlingar och andra objekt [som är specifika för en applikation]	Typ Acrobat Reader, Microsoft Word, Excel etc. Vanligtvis signeras och krypteras data inte direkt i dessa applikationer men funktioner som möjliggör detta kan komma att användas i allt större utsträckning framöver.

3.2 Myndigheternas kontroll över Innehavarens gränssnitt

Myndigheternas möjligheter att påverka Innehavarens gränssnitt är primärt begränsade, till vad som kan styras genom utformningen av myndigheternas e-tjänster.

Fristående gränssnittsmoduler i Innehavarens klientmiljö, så som Innehavarens modul för presentation av certifikatinnehåll, kan inte påverkas från e-tjänsten eller från ID-tjänsten, annat än genom den mycket begränsade indirekta påverkan som utformningen av certifikaten medger.

Dock kan utformningen av dessa gränssnitt kontrolleras och förutses mer i detalj om man har möjlighet att styra Innehavarens val av modul genom att tvinga Innehavaren att installera och använda en speciellt utformad modul. Tillhandahållare av ID-tjänst kan här tvinga Innehavare av e-legitimation att installera särskilda gränssnittsmoduler i kombination med att e-legitimationen utfärdas till Innehavaren.

Det är särskilt vanligt med särskilda moduler för aktivering av Innehavarens privata nyckel i de fall Innehavaren försetts med s.k. ”hårda nycklar”, d.v.s. en lösning där Innehavarens privata nyckel lagra på en hårdvarumodul i form av t.ex. ett Smart kort eller en USB-enhet.

I vissa fall kan gränssnittsmoduler i Innehavaren klientmiljö ersättas med ett webbgränssnitt via aktivt utformade webbsidor. Exempel på detta är möjligheten att införa aktiva menyer (drop-down menyer) i Innehavarens gränssnitt för val av certifikat. Om detta utförs med lyckat resultat kan man undvika att standardmodulen för certifikatval aktiveras automatiskt. Detta medger i vissa fall ökade möjligheter att från e-tjänsten kontrollera utformningen av Innehavarens gränssnitt.

Generellt sett bör man dock ha i åtanke att en och samma myndighetstjänst – beroende på Innehavarens operativsystem och klientmjukvaror – kan generera mer eller mindre olika användargränssnittsresultat.

Myndigheternas möjligheter att påverka Innehavarens upplevelse av gränssnitten vid användning av olika komponenter sammanfattas i nedanstående tabell:

2	Klientprogram för kommunikation med myndighets e-tjänst	Här är påverkansmöjligheten störst och ganska självklar. Myndigheten utformar webbsidor, grafiska element och interaktiva komponenter som på ett relativt enhetligt sätt presenteras för Innehavare med olika klientmiljöer
2a	Klientmodul för presentation av certifikat (e-legitimation)	Här har myndigheten ringa eller ingen påverkansmöjlighet. Enda undantaget är en viss begränsad möjlighet att föra in grafiska ”sigill” på en webbsida som förflyttar Innehavaren till en webbsida som presenterar myndighetens webbservercerti-fikat och dess status (T.ex. VeriSign Secure Site). Studien indikerar att det i de vanligaste klientmiljöerna inte är görligt att byta ut denna modul genom s.k. plug-in moduler.
2b	Klientmodul för aktivering av Innehavares privata nyckel	Myndighet har endast indirekt inflytande över Innehavarens val av modul för aktivering av privat nyckel. Myndigheten kan dock indirekt påverka val av modul genom att kräva att certifikat (e-legitimationer) skall följa en certifikatpolicy som kräver användning av lämplig modul. Förutom val av modul har myndigheten ingen kontroll över modulens gränssnitt mot Innehavaren vad gäller förklarande texter vid användning av privat nyckel. Om myndigheten kan styra utformning och val av modul så kan dock moduler utformas som helt stödjer myndigheternas riktlinjer vad avser användargränssnitt.
2c	Klientmodul för val av certifikat vid legitimering	Denna modul aktiveras lokalt hos Innehavaren när bl.a. en skyddad session aktiveras. Myndigheten har ingen möjlighet att påverka utseendet på denna moduls gränssnitt men dock att ersätta användningen av denna modul, i de flesta klientmiljöer, genom kreativ utformning av webbtjänsten.
3	Applikationer för presentation, editering och signering av elektroniska handlingar och andra objekt [som är specifika för en applikation]	Gränssnittet styrs, med undantag för faktiskt innehåll i dokument, uteslutande av den applikation som tillämpas samt av de stödmoduler enligt ovan som applikationen använder sig av.

3.3 Rättighetsbaserad säkerhetsinfrastruktur

Traditionell säkerhetsinfrastruktur utgår from att Innehavare identifieras vid inloggning och sedan, beroende på rättigheter får tillgång till tjänster och information.

Ett alternativ till detta ligger i den metodik som utgår från s.k. ”Rights Management”, baserat på öppna standarders (XrML), där regler för tillgång till information kopplas till enskilda dokument i form av kryptografiskt skyddade licensvillkor.

Denna metodik, i fall den tillämpas av myndigheter, kan påverka möjligheten att skapa upplevelser av olika juridiskt relevanta användargränssnitt på ett sätt som inte är möjligt i traditionella webbgränssnitt.

Denna studie utgår främst från traditionella Webbtjänster och informationsflöden över e-post. Närmare kartläggning av de möjligheter som ges med framtida rights management tjänster, i den mån dessa bedöms som relevanta för SAMSET, bör belysas i separat studie.

Särskilt bör man då beakta den funktionalitet baserat på Rights Management som är standard i Microsoft Officeapplikationer från och med Office 2003.

4 SAMSET Legala Användargränssnitt

4.1 Legitimera

4.1.1 Realiserbarhet

4.1.1.1 Grundläggande målsättningar

I [Legala Användargränssnitt] definieras grafik och text som skall/bör presenteras för en Innehavare som identifieras i samband med *tillträde* till information och vid *uppgiftslämnande.*

Det scenario som identifieras för tillträdeskontroll och uppgiftslämnande i denna studie är förfarandet då Innehavaren får tillträde till en skyddad webbtjänst där information antingen kan hämtas eller lämnas. I det fall uppgiftslämnande säkras genom digital signatur, gäller gränssnittsfunktionen ”underteckna” istället för ”legitimera”.

Detta scenario realiseras huvudsakligen genom att kommunikationen med Innehavaren skyddas av en SSL/TLS session (https) där Innehavaren identifieras antingen;

1. som en del av etableringen av https sessionen (SSL-klientautenticering), eller;
2. genom separat inloggningsförfarande efter etablering av https sessionen.

Vid den enklaste tillämpningen av metod 1 och 2 ovan realiseras huvuddelen av Innehavarens inloggningsgränssnitt av gränssnittsmodulerna 2b och 2c.

4.1.1.2 Grafiska element, förklarande text och interaktiva komponenter

SAMSETs gränssnitt Legitimera kräver grafik och text som inte stöds direkt av gränssnittsmodulerna 2b och 2c. För att införa grafiska element enligt SAMSET krävs därför kreativa lösningar som dock i huvudsak förefaller möjliga att åstadkomma.

4.1.2 Genomförande

4.1.2.1 Implementeringsprinciper

Vid SSL-klientautenticering (Alternativ 1 ovan där Innehavaren begär tillträde till en (https) sida som kräver identifiering av klient med certifikat) aktiveras normalt identitetskontroll med hjälp av tillämpliga delar av Innehavarens lokala funktioner 2b och 2c. För att implementera SAMSET gränssnitt måste man därför införa en inloggningssida till vilken Innehavare hänvisas då legitimering skall ske. På denna webbsida kan man då dels visa lämpliga grafiska symboler och förklarande text och dels skapa webbaserade alternativ till modul 2c. Vid aktivering av privat nyckel är man dock hänvisad till användarens modul 2b.

Vid separat inloggningsförfarande (alternativ 2) byggs en separat funktion där klientens certifikat verifieras på annat sätt, t.ex. genom digital signatur av inloggningsdata. Även här aktiveras tillämpliga delar av innehavarens lokala gränssnittsmoduler 2b och 2c som standard. PÅ samma sätt som vid skapandet av inloggningssida för SSL-klientautenticering kan man här införa grafiska element och förklarande texter samt skapa webbaserade alternativ till modul 2c. Även här är man hänvisad till användarens modul 2b för aktivering av privat nyckel.

4.1.2.2 Tillämpning av speciell mjukvara

För fullständig implementering av SAMSET användargränssnitt krävs enligt ovan att man tvingar användare att använda en SAMSET-anpassad modul 2b (aktivering av privat nyckel). Detta krävs om man vill uppnå speciell text direkt i anslutning till aktivering av den privata nyckeln. Dock kan man i huvudsak uppfylla riktlinjerna även man marknadens standardmoduler.

4.1.2.3 Framtida målsättning

Den realistiska framtida målsättningen bör vara att försöka påverka utformningen av standardmoduler 2c så att de tillämpar ett lämpligt språkbruk som gör en alldaglig Innehavare medveten om innebörden av vad som sker.

4.1.2.4 Realistiska steg

Att följa och i viss mån påverka utformningen av standardkomponenter

4.2 Presentera e-legitimation

4.2.1 Realiserbarhet

4.2.1.1 Grundläggande målsättningar

I [Legala Användargränssnitt] föreslås grafiska principer för presentation av e-legitimation (certifikat), dels vid presentation av motparters certfikat vid validering av signerade handlingar samt validering av myndighetstjänster och dels vid presentation av egna certifikat då ett eget certifikat måste väljas utifrån ett antal tillgängliga certifikat.

Presentation av andras certifikat

Detaljerad presentation av certifikat i Innehavarens klientmiljö sker i allmänhet endast (med hjälp av modul 2a) efter det att Innehavaren aktivt begärt detta.

Som exempel i Microsoft Internet Explorer och Microsoft Outlook ges denna möjlighet:

- Genom att dubbelklicka på den låssymbol i webbläsarens nedre högra hörn som indikerar att säker kommunikation upprättats med en identifierad server. Därmed visas certifikatet på den server med vilken säker kommunikation upprättats.

- Genom att undersöka den signatur som tillfogats ett signerat e-postmeddelande. Därmed ges tillfälle att undersöka det certifikat som används för att verifiera meddelandets avsändare.

Presentation av egna certifikat

Presentation av en lista över Innehavarens egna certifikat vid t.ex. inloggning på säker webbsida, sker automatiskt vid behov, men till skillnad från exemplen ovan då certifikatens totala informationsmängd tillhandahålls, är det vanligt att endast presentera Innehavarens egna certifikat i listform med en enkel rad text för varje certifikat (med hjälp av modul 2b). Denna funktion har inget direkt gränssnitt definierat i SAMSET riktlinjer. Se även under avsnittet för ”Legitimera” ovan

4.2.1.2 Grafiska element, förklarande text och interaktiva komponenter

De grafiska element och presentationsprinciper som föreslås kan inte genomföras med de program och moduler som nu finns tillgängliga för Innehavare. Enligt nuvarande arkitekturprinciper så är det uteslutande Innehavarens modul(er) 2a som styr hur ett certifikat visas i sin helhet (egna och andras).

Det finns dock inga principiella hinder för att modulerna 2a helt eller delvis skulle kunna uppfylla riktlinjernas [Legala Användargränssnitt] målsättningar i framtiden.

Foto och grafisk bild på handskriven namnteckning kan redan idag knytas till certifikat genom standarden RFC 3039. Det finns emellertid inte någon utfärdare av e-legitimationer (Utfärdare, även kallad CA) eller någon tillverkare av modul 2a som har implementerat stöd för denna funktion.

Vidare ligger en ny standard för godkännande inom IETF som skall möjliggöra koppling av grafiska logotyper till certifikat. Denna standard, som kan användas även för att implementera foto och namnteckning enligt ovan, är utvecklad i samarbete med bl.a. Microsoft. Här finns goda möjligheter att framtida Utfärdare samt tillverkare av modul 2a kommer att stödja denna standard.

4.2.2 Genomförande

4.2.2.1 Implementeringsprinciper

Myndigheter är hänvisade till användarnas egen klientmiljö och deras funktioner för presentation av e-legitimation (certifikat). Myndigheterna kan påverka/påskynda införandet av en mera lättillgänglig grafisk presentation genom att:

- eftersträva att certifikat som utfärdas till Innehavare har stöd för grafiska element som utgör grundförutsättning för en bättre presentation,
- påverka Innehavare att uppdatera sin modul 2a i den mån detta är möjligt när bättre moduler finns att tillgå, och
- påverka tillverkare av 2a – moduler att understödja kommande standarder och därmed möjliggöra en mer lättillgänglig presentation av e-legitimationer i enlighet med SAMSETs riktlinjer.

4.2.2.2 Tillämpning av speciell mjukvara

I dagsläget är, enligt vad denna studie erfarit, möjligheten att ge Innehavare bättre funktionalitet genom specialutvecklade moduler mycket begränsade. I Windows baserade klientmiljöer tyder alla indikationer på att det kommer att krävas uppdatering till nytt operativsystem (efterföljare till XP) innan stöd för grafiska symboler i certifikat kan åstadkommas.

4.2.2.3 Framtida målsättning

Det är i allra högsta grad rimligt att på sikt ha målsättningen att certifikat, tjänster och klientmiljöer i samverkan skall uppfylla SAMSETs riktlinjer. Under förutsättning att certifikatutfärdare väljer att stödja grafiska symboler i certifikat så är det rimligt att anta att detta börjar få genomslag inom en tvåårsperiod.

4.2.2.4 Realistiska steg

[Legala Användargränssnitt] riktlinjerna är inte realistiska i dag men viss funktionalitet finns i dag och det är inte rimligt att åstadkomma mer i det korta perspektivet (inom ett år).
Det är trots detta rimligt att börja vidta åtgärder i enlighet med 4.2.2.1 för att på sikt skapa mera användarvänliga presentationsformer.

4.3 Granska

4.3.1 Realiserbarhet

4.3.1.1 Grundläggande målsättningar

[Legala Användargränssnitt] föreslår grafisk symbol och text att användas då en Innehavare skall uppmanas att granska information innan den undertecknas. Rent principiellt finns en skillnad mellan tillfällen då granskning avser ett bifogat dokument eller fil som måste öppnas separat, eller då granskning avser text som är en aktiv del i myndighetstjänstens interaktiva gränssnitt.

I samtliga fall är detta dock en del av användargränssnittet som till avgörande grad kan styras genom utformningen av myndighetens e-tjänst. Detta gäller särskilt för webbtjänster.

4.3.1.2 Grafiska element, förklarande text och interaktiva komponenter

De grafiska symboler och förklarande texter som föreslås i [Legala Användargränssnitt] kan införas med hjälp av befintlig teknik och programvara. Både vad avser servrar och klienter.

4.3.2 Genomförande

4.3.2.1 Implementeringsprinciper

Myndigheter kan sannolikt med hjälp av tillgänglig kompetens och befintliga verktyg införa föreslagna grafiska element och förklarande texter i sina Webbtjänster.

4.3.2.2 Tillämpning av speciell mjukvara

Behov saknas.

4.3.2.3 Framtida målsättning

Behov saknas.

4.3.2.4 Realistiska steg

Myndigheter utformar sina tjänster så att rekommenderade texter och grafiska element infogas i webbtjänster när ett färdigt utkast till en handling eller ett annat objekt skall granskas inför undertecknande.

4.4 Underteckna

4.4.1 Realiserbarhet

4.4.1.1 Grundläggande målsättningar

En rad olika funktioner och moduler bidrar till Innehavarens gränssnitt när elektroniska handlingar eller ett andra objekt undertecknas.

Några principiellt olika scenarier är:

1. Innehavaren undertecknar en text (ett formulär) som presenteras för Innehavaren som en del av en webbtjänst. Webbformuläret undertecknas med hjälp av lokala säkerhetsfunktioner där modul 2b styr interaktion med Innehavarens privata nyckel. Webbtjänsten kan presentera text och grafik innan signaturprocessen inleds men text och grafik som styr själva undertecknandet (aktivering av användarens privata nyckel) styrs uteslutande av Innehavarens modul 2b.
2. Innehavaren undertecknar handlingarna i en lokal applikation som överförs till myndighet genom e-post, FTP eller en lämplig webbaserad depositionstjänst. I detta fall signeras dokumentet uteslutande med hjälp av den lokala applikationens användargränssnitt för skapande av digital signatur:

SAMSET riktlinjer och denna studie fokuserar på fall 1 ovan.

Det finns en uppenbar risk att detta gränssnitt krockar i tillämpning och syfte med funktionen skicka. I många applikationer och tillämpningar finns ingen interaktiv funktion kopplad till undertecknande som föregår funktionen skicka. I dessa fall är det tvärtom funktionen skicka (alternativt genom instruktionen ”Godkänn” eller bara ”OK”) som initierar funktionen underteckna vilket sedan utförs då Innehavaren aktiverar sin privata signeringsnyckel genom modul 2b.

4.4.1.2 Grafiska element, förklarande text och interaktiva komponenter

Det föreslagna grafiska elementet och den förklarande texten kan införas i myndigheternas webbtjänster så som en gränssnittsfunktion som initierar signeringsprocessen. Själva undertecknandet, och därtill kopplade inmatning av signeringskod är dock underställd, Innehavarens modul 2b

4.4.2 Genomförande

4.4.2.1 Implementeringsprinciper

Det grafiska gränssnittet kopplat till bruk av användarens signeringsnyckel är i allt väsentligt underställt modul 2b. Principer för implementering av funktionella gränssnitt utgörs av att i rimlig mån påverka utformning av komponenter av typ 2b samt att i övrigt tillse att e-tjänsters övriga kommunikation med Innehavare förtydligar innebörden av att använda en viss privat nyckel enligt Innehavarens befintliga gränssnitt.

4.4.2.2 Behov av mjukvara, grafik och förklarande text

För fullständig implementering av SAMSET användargränssnitt krävs en SAMSET-anpassad modul 2b (CSP för aktivering av privat nyckel), om man vill uppnå speciell text direkt i anslutning till aktivering av den privata nyckeln. Man kan dock i huvudsak uppfylla riktlinjerna även med marknadens standardmoduler.

4.4.2.3 Framtida målsättning

En rimlig kortsiktig målsättning är att presentera föreslagna grafiska element, förklarande text och interaktiva komponenter som en del i webbtjänsternas aktivering av signaturprocesser och att sedan låta klienternas befintliga 2b moduler styra gränssnittet för PIN-inmatning eller motsvarande aktivitet som aktiverar signaturgenereringen.

4.4.2.4 Realistiska steg

Man kan överväga om det finns skäl att kräva av Innehavare att de anpassar sin användarmiljö med en uppdaterad modul 2b. Om detta sker så måste detta implementeras som en integrerad del i Innehavarens ID-tjänst (utfärdandet av Innehavarens certifikat) och därmed står detta under ID-tjänstens och inte e-tjänstens kontroll.

Myndighetens möjlighet att påverka detta är därmed knuten till godkännandet av de certifikat som uppfyller myndigheternas krav.

4.5 Skicka

4.5.1 Realiserbarhet

4.5.1.1 Grundläggande målsättningar

Funktionen för att skicka sammanfaller i hittillsvarande tillämpningar normalt med funktionen för att underteckna. Tudelningen av dessa gränssnitt i [Legala användargränssnitt] kan därför kräva kreativa lösningar, vilket i sin tur kan leda till olika tolkningar och implementeringar av [Legala Användargränssnitt]. Det kan därför vara lämpligt att komplettera [Legala användargränssnitt] även med en sådan logotype och förklarande text.

Bortsett från detta så är gränssnittet för skicka allra högsta grad realiserbart så som en funktion i E-tjänstens webbgränssnitt mot Innehavaren.

4.5.1.2 Grafiska element, förklarande text och interaktiva komponenter

Grafiska element, förklarande texter och interaktiva komponenter kan enkelt införas som en del i E-tjänstens webbgränssnitt.

4.5.2 Genomförande

4.5.2.1 Implementeringsprinciper

Gränssnittet realiseras i e-tjänstens webbgränssnitt och berör endast Innehavarens webbläsare.

4.5.2.2 Behov av mjukvara, grafik och förklarande text

Saknas

4.5.2.3 Framtida målsättning

Saknas

4.5.2.4 Realistiska steg

Saknas

4.6 Användargränssnitt för dokument

I [Legala Användargränssnitt] föreslås inte direkt några användargränssnitt för dokument i form av grafiska element, förklarande texter eller interaktiva komponenter. Dock är det värt att notera att flera av de aspekter som tas upp för e-tjänsten, kan komma att få allt större stöd i kommande applikationer. Härvid kommer rättighetsbaserade säkerhetslösningar typ rights management att erbjuda nya möjligheter (se avsnitt om rättighetsbaserad säkerhetsarkitektur (avsnitt 2.3).

5 Referenser

[Legala Användargränssnitt] Riktlinjer för användargränssnitt som från juridiska utgångspunkter stöder legitimationer, underskrifter och dokument i elektronisk form (legala användargränssnitt), (version 0.9.3 juristgruppen)

[Grundläggande Riktlinjer] Riksskatteverkets riktlinjer för myndigheternas användning av e-legitimationer och elektroniska underskrifter, (version 2.6, justerad efter sammanträde med juristgruppen 24.4)