Digital Signering

En kokbok i digitala signering

Version 1.0

SUNET Inkubator
Digital Signering
Kokbok i digital signering
Mats Törnblom

Innehåll:

Sammanfattning

Detta dokument ger en översikt av området digital signering samt förklara tekniska begrepp och lösningsmönster. Dokumentet innehåller ett antal exempel på för lärosäten relevanta use case och diskuterar slutligen möjligheten att inrätta en lärosätesgemensam lösning i SUNETS regi.

Bakgrund

Digital signering är ett område som det råder mycket förvirring runt. ATI föreslog därför att Inkubator skulle göra ett mindre initiativ runt detta för att producera ett kortfattat material som reder ut begreppen så att det är rimligt begripligt även för en lekman på området.

Syfte

När det gäller digital signering finns oändliga möjligheter att gå vilse i juridiska detaljer, kryptografiska algoritmer och luddig nomenklatur. Ett genomgående problem i området är att det är alltför vanligt att tekniker försöker förklara juridiken, jurister försöker förklara tekniken och folk som är varken eller försöker tolka vad teknikerna och juristerna säger.

I det här dokumentet försöker vi göra digitala signaturer och digital signering begripligt för IT-generalister, främst IT-arkitekter, utan att gå inte på alltför mycket detaljer.

Tanken är att denna ”kokbok” ska vara något att hålla i handen för arkitekter när man hade behov av att diskutera och/eller implementera digital signering.

Vidare är syftet att konkretisera några vanliga use case och lösningar som kan fungera som referens för lösningsarkitekter som ställs inför kravbilder runt digital signering.

Slutligen ställs frågan om det vore önskvärt att SUNET levererar en lärosätesgemensam lösning för digital signering.

Nomenklatur

Nomenklaturen, eller avsaknad därav, är en anledning till varför det här området är så svårt att få grepp om. I stort sett varje nytt initiativ och leverantör tycks ha hittat på sina egna begrepp.

I det här dokumentet försöker vi använda oss av de begrepp som vi arkitekter normalt använder när vi diskuterar IT lösningar. Därför använder vi till exempel begreppet ”autentisering” för att beskriva processen att identifiera en användare istället för ”identifiering” som ofta används i just detta område.

Vidare använder vi uttrycket ”digital signering” istället för ”elektronisk signatur”, eftersom det är det begreppet som normalt används av lösningsarkitekter. Detta är inte okontroversiellt eftersom ”elektronisk signatur” är det som används av e-legitimationsnämnden. Vi ser ”digital signering” som ett vidare och mindre exakt begrepp än ”elektronisk signatur”.

I övrigt försöker vi dock hålla oss till e-legitimationsnämnden nomenklatur, beskriven här:
https://www.elegnamnden.se/vanligafragor/ordlista.4.4498694515fe27cdbcfba.html

Digital signering – lite grunder

Syfte

Uttryckt väldigt förenklat, en lösning för digital signering har två syften:

- att dokumentera att en eller flera fysiska och/eller juridiska personer godkänt ett ”dokument” vid en viss tidpunkt.
- att säkra att det signerade dokumentet inte ändrats.

Det här är som sagt väldigt förenklat, bland annat behöver en signering inte handla om ett ”dokument”, det kan vara ett antal olika saker.

Digital signering vs. digitalt signerat dokument

Det är skillnad på ”digital signering” och ett ”digitalt signerat dokument”.

Med ”digitalt signerat dokument” menas oftast:

- ett helt fristående signerat digital dokument som inte kan ändras,
- där en autentisering av parterna har skett i samband med signeringen och
- där information om parterna är inkluderat i dokumentet.

Det är ju det här som kommer närmast den fysiska världens signerade dokument.

”Digital signering” däremot är aktiviteten att verifiera en avsikt, överenskommelse, förbindelse, intyg etc. Vi säger ofta ”digitalt signerat dokument”, för så var det ju alltid i den analoga världen, men i den digitala världen behöver inte en signering resultera i ett fristående dokument. Vi ”signerar” till exempel våra betalningar i internetbanken, det är ju en verifiering av att vi ger banken i uppdrag att utför dessa betalningar. Det är en överenskommelse mellan oss och banken som ju är avsedd att binda oss vid avsikten i en domstol, men det resulterar ju aldrig i ett fristående dokument, i alla fall inte ett som vi som kund kan ta del av eller visa för andra parter.

Grundläggande mönster för ”digitala signaturer”

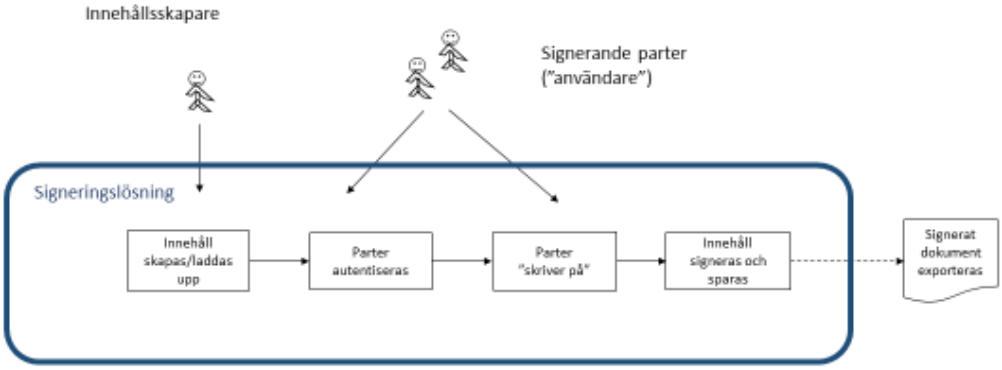
En digital signering initieras alltid i ett IT system av något slag.

I IT-systemet upprättas någon typ av innehåll som avser en avsikt, överenskommelse, förbindelse, intyg etc. Det kan vara ett avtal, ett betyg, ett uppdrag osv.

Till detta innehåll vill vi knyta en eller flera parter. Det kan vara enskilda personer eller organisationer. Vi vill också hålla reda på vid vilken tidpunkt detta gjorts. Detta gör vi via en signering.

Via signaturen skapar och dokumenterar vi länken mellan parterna, innehållet och tidpunkten. Den svåraste delen i signeringen handlar om att autentisera de signerande parterna på ett tillförlitligt sätt.

Systemet kan sedan *eventuellt* och om så önskas producera innehållet som ett fristående förändringsskyddat dokument i form av en fil (.pdf, .docx etc) med information om de signerade parterna och tidpunkt inkluderat.



Vad är en ”digital signering”?

Om vi använder begreppet ”digital signering” i vid bemärkelse finns ett stort spann i vad det är.

I ena ändan av det spannet finns situationer där man som användare tydligt informeras om att man gör en ”signering”, där en explicit signeringsmetod användas (tex baserat på Mobilt Bankid) och där ett externt dokument produceras som resultat.

I andra ändan av spannet finner man enkla avsiktsverifieringar som en ”vill du verkligen gör det här?”-ruta eller en ”jag accepterar villkoren”-knapp.

Här är åter en nomenklaturförbistring. Somliga skulle med emfas hävda att endast det första fallet är ”digital signering”. Samtidigt skulle i de flesta fall de senare metoderna hålla i en domstol och därmed fylla syftet med en digital signatur. Gör det att de är att betrakta som ”digital signering”? Det beror på hur man definierar ”digital signering”.

”Signerat dokument” vs ”signerat data”

Som indikerats ovan så behöver ju inte en signering (om man använder ordet i vid bemärkelse) avse ett fristående dokument.

Många lösningar där vi gör ”digitala signering” lagrar bara data som den signerandes avsikt som data i en databas. Databasen kan innehålla en ”har signerat”-kolumn där namnet på de som ”signerat” ligger – inget fristående dokument har producerats, inga certifikat är involverade osv.

Olika hybridvarianter finns också, tex lösningar där ett faktiskt dokument finns lagrat i systemet, men där kopplingen mellan en användare som har gjort en signering och dokumentet finns lagrat i systemets databas.

I dessa lösningar står alltså ”signeringen” i direkt relation till systemets integritet, vilket kontrasterar mot ett fristående signerat dokument. I det förra fallet kan existerar inte ”signaturen” utanför systemet, i det senare fallet finns inget beroende till system i vilket signeringen har gjorts, endast till det certifikat som använts.

Betrodda tjänster

Betrodda tjänster är tjänster (lösningar/”produkter”) som levereras av företag (i huvudsak) och som följer ett EU regelverk för ”elektroniska signaturer”. Post och Telestyrelsen (PTS) är tillsynsmyndighet för betrodda tjänster i Sverige.

Använder man en ”Betrodd tjänst” vet man alltså att den kommer hålla en definierad och verifierad kvalitetsnivå.

Juridiskt är poängen med att använda en ”Betrodd tjänst” för digital signering är att man signaturen dels följer formkraven för eIDAS regelverket (om man nu har det behovet) och dels kommer ha en så god kvalitet att eventuellt bestridande i en domstol kommer vara utsiktslöst.

Autentisering

Distribuerad autentisering och kryptering via PKI – ”direkt underskrift”

Digitala signering har historiskt varit när knutet till certifikatshantering och PKI.

Tanken har varit att man via certifikat och krypteringsnycklar både hanterar auktorisation och den kryptering som behövts för att producera och signera digitala oförändringsbara dokument. Den som signerar måste alltså ha ett certifikat i form av en certifikatsfil på sin dator, det är den som autentiserar personen. E-delegationen kallar det här ”Direkt underskrift”.

Poängen med det här är att ingen serversida krävs för signering. Två personer skulle med certifikat och lokal mjukvara på sina datorer kunna utföra signeringen fullt ut.

För att det här ska fungera så måste man ju på ett säkert sätt distribuera dessa certifikat så att rätt person har rätt certifikat. Det kräver alltså en PKI – en lösning för att distribuera certifikat/nycklar till användarna.

Att implementera en bra PKI - att på ett säkert och effektivt sätt att sätt distribuera och livscykelhantera tusentals distribuerade certifikatsfiler - är något få organisation har varit framgångsrika med det. Därför har digital signering i sin tur alltid varit en gigantisk utmaning.

En av de lösningar där det idag fortfarande finns ett digitalt certifikat i bakgrunden är det traditionella datorbaserade BankId:t. Här används bankernas Internetbanker som PKI mekanism.

Centraliserad autentisering och kryptering via tjänster – ”Indirekt underskrift”

Den traditionella PKI-baserad tillvägagångssättet har alltså visat sig vara tämligen svårhanterligt.

Vad som i stället har växt fram på senare tid är en mycket mer praktiskt modell baserat på centrala tjänster och generella autentiseringsmekanismer.

Troligen är det detta som E-legitimationen avser med termen ”Indirekt underskrift”.

Något förenklar fungerar det så här:

1. Användarna loggar in i en central signeringstjänst.
2. Användarna som ska signera autentisieras med de mekanismer som vi normalt använder i våra IT lösningar. Det kan vara AD, SWAMID, Mobilt BankId, eIDAS identitet osv.
3. Användarna signerar dokumentet (egentligen: användarna godkänner att systemet signerar dokumentet).
4. Signeringstjänsten producerar dokumentet med sitt eget server certifikat, alternativt engångscertifikat som den centrala tjänsten hanterar helt internt.

Möjligen kan centrala tjänster intuitivt kännas som ett mindre säkert sätt att göra digitala signaturer, men i praktiken är det säker så länge den centrala tjänsterna håller en kontrollerad och känd kvalitet med avseende på säkerhet, vilket är avsevärt lättare i en centraliserad lösning. Se vidare resonemangen runt ”Betrodda tjänster”.

Verifiering av signaturer

I efterhand vill man kunna verifiera signaturer och de som har signerat.

En signatur är producerad utifrån ett certifikat som är utställt av någon form av betrodd part. Certifikatet har en giltighetstid. En digital signatur kan alltså ha ”gått ut”. Det gäller ju inte traditionella signaturer. Utifrån sitt use case får man fundera på om detta ha någon betydelse.

Det finns även två aspekter på verifieringen:
1) Den tekniska verifieringen och
2) Den ”mjuka” verifieringen som görs av mottagaren

Juridik och teknik for dummies

Juridiken for dummies

Syftet med en digital signering (oavsett hur vi definierar begreppet) är att verifiera en avsikt, överenskommelse, förbindelse, intyg etc mellan en eller flera parter. Det fallet som är enklast att resonerar runt är en överenskommelse i format av ett avtal mellan två parter, så låt oss använda det som ett exempel.

Skulle en tvist uppstå där endera parten bestrider överenskommelsen kommer det att tas upp som en tvist mellan parterna i en domstol. Då är det fri bevisprövning som gäller.

Vid den prövningen kommer man granska validiteten av det digitalt signerade materialet (vilket alltså kan, men inte behöver, vara ett fristående dokument).

Det här betyder att man inte kan säga att en viss lösning är ”100% legalt bindande” eller något i den stilen. Det finns (med undantag av eIDAS, där finns vissa standarder) inte några formella krav på hur en digital signatur ska se ut, göras eller implementeras. Istället handlar det om att göra det tillräckligt troligt i en domstol att de signerade parterna och överenskommelsen var de som anförs.

Översatt till termer av teknisk lösning betyder det alltså i praktiken att de berörda parterna måste gör en bedömning om den lösning man använder kommer hålla en i en domstol. Om den lösning man valt är bra nog vet man alltså inte med säkerhet förrän en domstol avgjort just det specifika fallet.

Däremot finns det ju lösningar som betraktas som best practices, dvs de ha prövats i rättsliga sammanhang och befunnits tillräckligt ”bra”, så egentligen är det här inte så dramatiskt som det kan låta.

Om man benar vidare i det här finns det i huvudsak tre saker man kan bestrida i relation till dokumentet och signaturen:

- Integriteten, dvs ”Dokumentet och/eller signaturen har förändrats sedan jag/vi skrev på det”
- Autentiseringen dvs ”Det är inte jag som skrivit på dokumentet” (eng :Non-repudiation) och
- Tidsstämpling, dvs ”Jag skriv inte på det här vid den tidpunkten”

När det gäller integriteten så finns det för fristående digitala dokument standardmässiga lösningar som gör det omöjligt att ändra dokumentet eller signaturen i efterhand. Här är det för ett fristående dokument inte något problem att möta kraven. Svårare blir det så klart om det inte rör sig om ett fristående dokument utan det handlar om integriteten i ett IT system, men i praktiken är det nog inte ett stort problem givet att IT systemet möter normala best practices när det gäller integritet och säkerhet.

Ungefär samma som ovan gäller tidsstämpling, lösningar finns.

Avsevärt värre är det när det gäller autentisering, dvs invändningen ”Det är inte jag som skrivit på dokumentet”. För att kunna bevisa det krävs en hel del, och därför handlar mycket av de lösningsmässiga utmaningarna i det här området om hur man tekniskt autentiserar parterna vid tillfället för signeringen och hur man i efterhand verifierar dem.

Det är också här det här med ”Betrodda tjänster” kommer in. Om en ”Betrodd tjänst” använts så finns en känd och kontrollerad kvalitet på lösningen i vilken signaturen avgivits. I praktiken innebär det att man kan ta för givet vad utfallet i en domstol kommer bli – det ska vara utsiktslöst att hävda att man inte skrivit på dokument.

Slutligen en lite udda aspekt på det här med tvister. Om parterna *uppfattar* lösningen som så bra att de troligen skulle förlora i en domstol minskar risken för att ”orättmätiga” tvister uppstår. Att parterna tex förstår att och hur deras identitet är verifierad vid signeringstillfället kan alltså ha ett egenvärde.

Tekniken för dummies

Integritet

Integritet handlar om att se till att ”dokumentet” och signaturer inte kan ändras i efterhand. För fristående dokument åstadkommer man med hjälp av digitala krypteringsnycklar och ett ”fingeravtryck” av dokumentet. Det kan låta komplicerat, men man behöver inte förstå hur det här går till rent teknisk, inte ens som lösningsarkitekt. För den nyfikne finns dock massor av beskrivningar av detta på nätet.

Resultat av en sådan dokumentsignering blir ett fristående digitalt dokument, till exempel en .pdf-fil, som inte kan ändras i efterhand och som innehåller information om vilka som signerat dokumentet.

När det inte rör sig om fristående dokument måste systemet som helhet verifieras ur ett integritetsperspektiv.

Autentisering

Låt oss då gå vidare till den svårare delen - att säkert identifiera den signerade parten, dvs autentisering.

Det är ju helt centralt för lösningarna är hur de signerade parterna autentiseras. Ett dokument signerat av personerna A och B är ju helt värdelöst om man inte på något sätt verifierat att A och Bs identiteter i samband med signeringen. (Egenskapen att man inte kan förkasta en underskrift kallas ibland non-repudiation).

I stycket ”Autentisering” beskrivs autentisering mer i detalj, men sammanfattningsvis finns i grunden finns två sätt, via hantering av privata nycklar/certifikat eller via samma typer av autentiseringsmekanismer som vi normalt använder i våra applikationer (SWAMID, BankId etc.)

Varianter på lösningsmönster

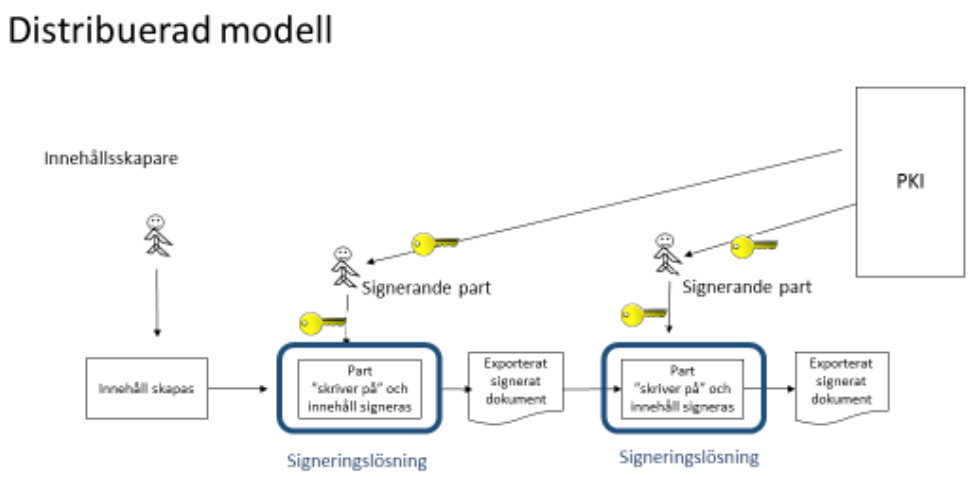
Lösningar för digital signering kan implementeras enligt ett antal olika mönster.

Notera att mönstren nedan inte är etablerade begrepp, det är en uppdelning gjort i detta dokument för att försöka kategorisera olika lösningsmässiga angreppssätt.

Distribuerad

Ett distribuerat mönster är baserat på (PKI-)distribution av certifikat och nycklar till alla involverade parter. Mönstret beskrivs även på annat ställe i detta dokument. Mönstret bygger också på en distribution av mjukvaror för signering.

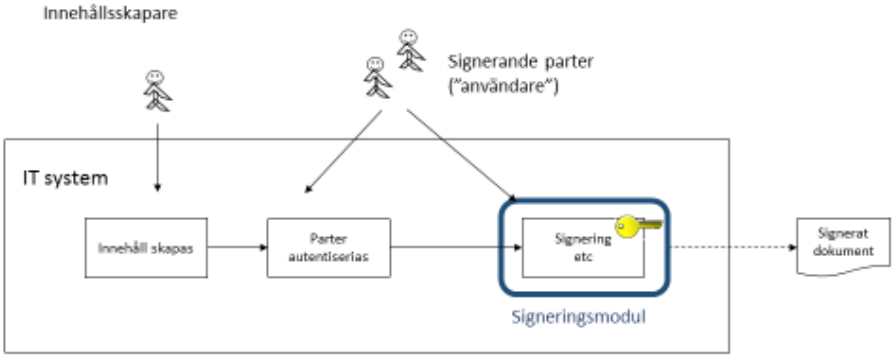
Det här är den traditionella modellen och den har väl aldrig varit riktigt framgångsrik på grund av svårigheten att distribuera certifikat/nycklar och mjukvara för signering.



Integrerad
En integrerat mönster innebär en applikation som har många andra syften implementerar en systemintern funktion för digital signering.

Om vi tänker oss att Ladok implementerade en intern funktion för att producera .pdf filer för studieintyg utifrån innehållet i Ladoks databas så skulle vi ha ett exempel på detta.

Integrerad modell



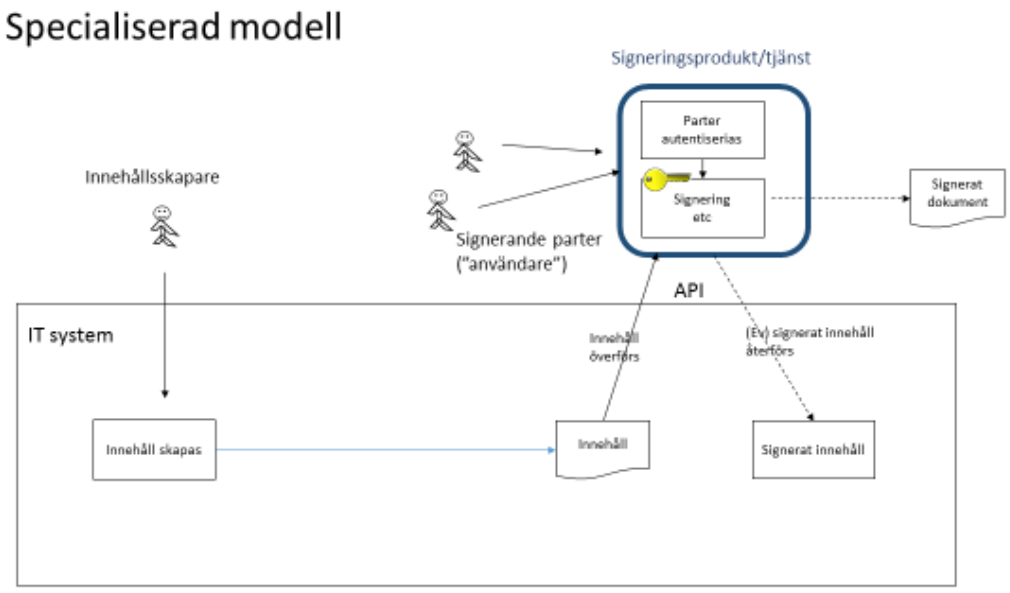
Specialiserad

Ett specialiserat mönster innebär att vi har en fristående specialiserad applikation som bara har till syfte att hantera digital signering och (möjligen) export av dokumentet .

Innehållet i form av ett dokument API:as in i signeringslösningen, parterna loggar in i systemet, signerar dokumentet och exporterar eventuellt sedan ut det som ett fristående dokument.

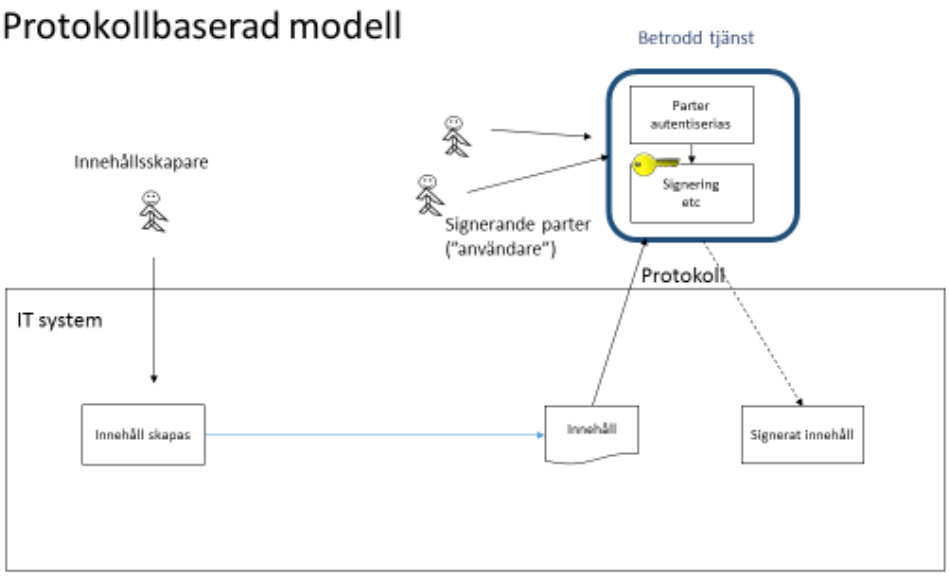
Exempel är fristående produkter för digital signering som tex DocuSign eller Adobe Sign.

Lösningen kan levereras som molntjänst eller på loka infrastruktur.



Protokollbaserad
Ett protokollbaserat mönster är snarlikt det som beskrivs som specialiserat ovan. Skillnaden är att applikationen som innehåller det data som ska signeras implementerar ett protokoll mot en viss signeringslösning samt att lösningen endast hanterar autentisering och signering, inget annat.

Exempel på sådan är e-legitimations signeringsstandard. I detta fall kommer vår applikation stödja ett standardprotokoll som ger möjlighet att utföra signering via e-legitimation.



Produktbaserad

I ett produktbaserat mönster interagerar vår applikation med en specialiserad signeringstjänst/-produkt via ett API.

I detta mönster anropar applikationen signeringstjänsten för att få signeringen utförd. De signerande parterna gör signeringen, mer eller mindre transparent, mot signeringslösningen.

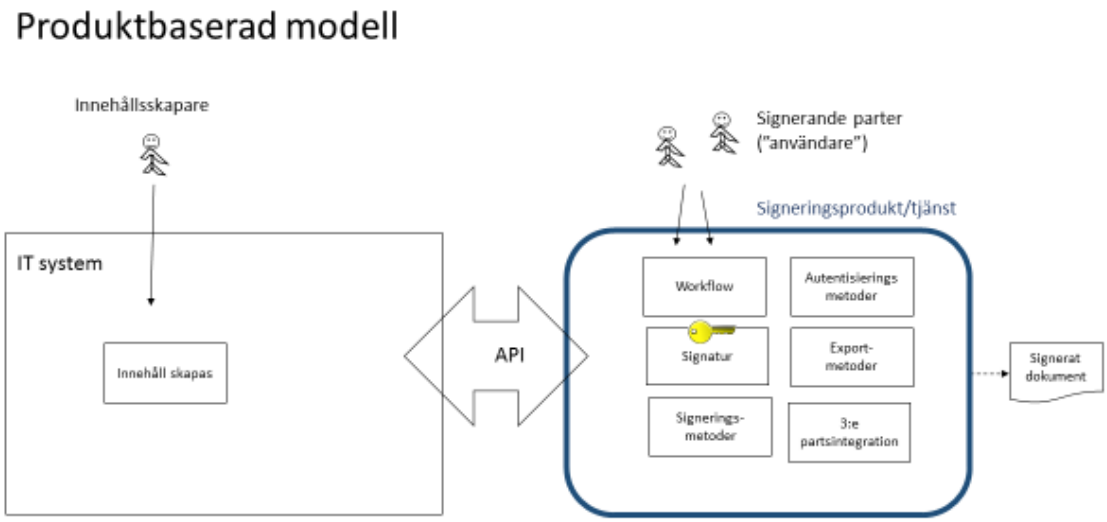
I grunden handlar det alltså om att externalisera signeringslösningen ur applikationen men fortfarande ha möjlighet till hög automationsgrad.

Fördelarna med detta mönster är flera:

- Produkten kan förväntas stödja en stor uppsättning signerings- och autentiseringsmetoder, till exempel e-legitimation, SWAMID, Nationella lösningar, Google, proprietära flerfaktorlösningar, olika signerings- och krypteringsalgoritmer osv.
- Produkten kan förväntas ha och stödja ett antal olika varianter på nyckelhantering.
- Produkten kan förväntas ha ett ganska omfattande process- och orkestreringsstöd för att till exempel hantera en kedja av signeringar från olika parter osv.
- Produkten kan förväntas producera, publicera och returnera fristående dokument i flera olika format.

- Ny funktionalitet (nya autentiseringsmekanismer, filformat, signeringsalgoritmer etc) implementeras av produktägaren och kommer nyttjaren till godo utan förändringar i applikationen.

Comfact och Docusign är exempel på sådana lösningar.

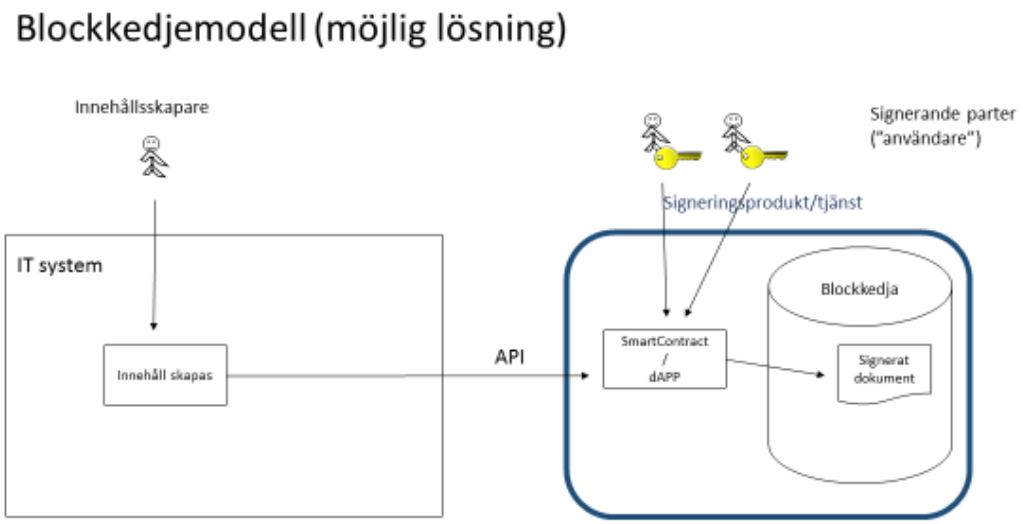


Blockchainbaserad

Någonstans vid horisonten hägrar även signeringslösningar baserade på blockchaininfrastruktur.

Blockkedjor har ett antal egenskaper som gör dem lämpliga för att hantera signaturer, identiteter och dokumentsignaturer - de är öppna för vem som helst, omöjliga att förändra, kan hålla transaktioner, är baserade på kryptering, inkluderar redan nyckel- och identitetshantering, blir sannolikt extremt billiga, osv.

Mönstermässigt blir det enkelt beroende på att alla användare, både enskilda och företag, får nyckelhanteringen som en del av sitt konto på plattformen. En enkel dApp signerar innehållet med de signerades nycklar och spara det (krypterat eller öppet beroende på önskemål) på blockkedjan.



Signeringslösningar kommer byggas ovanpå nästa generations dApp blockkjedjor som Cardano, NEO och EOS, men om det är något som kommer få genomslag är så klart omöjligt att säga nu.

Lösningsfunktionalitet

För att ge en känsla av vilka olika krav man kan ställa på en lösning kommer här en exempellista på funktionaliteter och ett resonemang runt dessa.

Autentiseringsfunktionalitet

Autentisieringsmekanismer

Som redan diskuterats kan alla de sätt vi normalt använder för att autentisera användare i våra IT system också användas i signeringslösningar. Antalet olika metoder som en viss lösning stöder kan variera stort, från en enda proprietär lösning till en hel palett av olika metoder.

Självklart vill vi inte hitta på en speciell autentiseringsmekanism för just signering, vi vill återanvända sådant som redan finns och används.

I vår värld är ju tex ett rimligt krav att lösningen ska stödja autentisering via SWAMID, det är ju vårt vanligaste sätt att autentisera en användare i vår värld och den är i allra högsta grad lämplig som autentisering vid signering.

Eftersom vi är myndigheter är det även troligt att vi behöva stödja signering baserat på eIDAS autentisering.

Vid val av lösning bör man även fundera över hur enkelt det är att lägga till nya autentiseringsmekanismer. Gör lösningens arkitekturer det enkelt eller svårt? Hur ser leverantörens strategi ut för detta?

Tillitsnivåer

En annan faktor att beakta är vilken utsträckning lösningen hanterar tillitsnivåer.

Istället för att välja en viss autentiseringslösning vill vi kanske hellre välja en tillitsnivå och sedan tillåta alla autentiseringsmekanismer/parter som når upp till denna nivå. Alternativt kan vi tillåta alla autentiseringsmekanismer men vilja hålla reda på vilken tillitsnivå var och en av dessa hade vid signeringsögonblicket.

Den information om vilken autentiseringsmekanism och vilken tillitsnivå som var aktuellt vid signeringen vill vi antagligen lagra både i systemet och som del av signaturen i ett fristående dokument.

Olika typer av signaturer

Notera att signaturtyperna nedan inte är etablerade begrepp, det är en uppdelning gjort i detta dokument för att försöka kategorisera olika lösningsmässiga angreppssätt.

Ritsignatur

En digital signatur kan i sin enklaste form vara baserad på att en oautentiserad användare skriver sin signatur på tex en telefon (”ritsignatur”) som sedan sparas som en bild som paketeras ihop med dokumentet. Det motsvarar direkt en papperssignatur.

I dag finns väldig få use case där man har anledning att nöja sig med en lösning som bara baseras på en ”ritsignatur” och inget annat. Någon typ av digital autentisering i samband med signeringen är oftast enkel att åstadkomma och bör ses som ett minimum. Ett av de få fall där man stöter på rena ritsignaturer idag är tex vid varuleveranser. Om en ritad namnteckning är den enda formen av autentisering är det här ju det självklart väldigt svag juridiskt.

Certifikatsbaserad signatur

Vid certifikatsbaserad signatur används certifikat lagrade lokalt på de signerades datorer/devices. De fungerar både som autentiseringsmekanismer och som nycklar för krypteringen av signaturen.

Dokument exporterade ur sådana lösningar är knutna till parternas certifikat/nycklar (”partsberoende certifikat”).

Kvaliteten i signaturen är avhängig PKI-infrastrukturens integritet – om certifikat och nycklar inte distribueras på ett säkert sätt är inte heller signaturerna baserad på detta säkra.

Kvaliteten i signaturen är även avhängig det signerande systemens nyckelhantering. I den klassiska distribuera modellen delegeras rätten att göra signaturer till de system som har nycklarna och den gäller så länge certifikatet inte är revokerat. I en centraliserad modell har man bara ger rätt att utfärda en signatur åt gången. Det betyder att en centraliserad har klara fördelar med avseende på detta.

Autentiseringsbaserad signatur

Vid autentiseringsbaserad signatur autentiseras användare i signeringsinfrastrukturen med hjälp av externa autentiseringsmekanimer (eIDAS autentisiering, Bankid, en länk som skickats till användaren via email, en kod via SMS, facebookinloggning, dosa, biometri osv).

Dokument exporterade ur sådana lösningar är baserade på certifikat/nycklar knutna till signeringsinfrastrukturen (”serverstämpling”)

Workflow och notifieringar

Signering sker ju nästan alltid som del i en (verksamhets)process. För att stödja och automatisera den är det ju fördelaktigt om lösningen har element av workflow, notifiering osv. Hur stor grad av detta lösningarna har varierar från att vara en rå hård/mjukvarulösning som utför signaturer och inget annat till att vara närmast en affärslösning med omfattande workflow, notifieringar, support på olika devices osv.

API:er

Ofta är e-singering som sagt bara en liten del av en större verksamhetsprocess som redan är implementerad i ett verksamhetssystem. Då är det naturligt att man vill integrera in signeringsdelarna i den redan existerande applikationen på ett sådant sätt att e-signeringen inte känns som en ”extern” lösning för användaren.

Många signeringslösningar erbjuder ett API för just detta ändamål. Om ett API finns och hur omfattande det är varierar från leverantör till leverantör.

Bra API:er utökar möjligheten att stödja olika sorter use case dramatiskt.

Digitala signaturer vs. andra use case

Det finns mycket annan funktionalitet som man lätt förväxlar med digitala signaturer. Det beror på att många use case/lösningar är en mix av digital signering, workflowstöd, arkivering, åtkomststyrning, kryptering av dokument osv. Det kan vara svårt för en verksamhetsperson att förstå vad som är vad av detta eftersom det i lösningarna gränssnitt lätt integreras ihop.

För oss som jobbar med att ta fram lösningar är det därför viktigt att lyssna till vad verksamheten egentligen efterfrågar. Det vanligaste är nog faktiskt att man med ”digitala signaturer” egentligen menar olika formar av digital stöd för att hantera dokument. Det är inte ens alltid så behovet handlar om för digitala signaturer, ofta räcker med att lägga dokumenten i en applikation som kräver inloggning.

Lyssna alltså nog på vad verksamheten efterfrågar och ställ följdfrågor. Ska ett digital dokument fristående produceras? Varför räcker inte den vanliga autentiseringen för att knyta en användare till en avsikt? Har behovet omfattande krav runt workflow?

Vilka use case lämpar sig typiskt för digital signering?

När man titta på use case för digital signering ser man ganska snart ett antal faktorer som de lämpliga use casen har gemensamt.

- Man har behov av ett signerat **fristående digital dokument** som kan distribueras till många olika eller okända parter.
  Så länge materialet aldrig ska lämna IT systemet behövs väldigt sällan eller aldrig digital signering, då är systemets autentiserings-/auktorisationsmekanismer tillräckliga.

- Det signerade **materialet ska arkiveras men kommer bara behövas accessas undantagsvis**.
  Alla former av avtal och beslut har ju egenskapen att behöver finnas som verifiering men de bara undantagsvis faktiskt kommer att behöva användas (typiskt vid en tvist). Ett signerat dokument är ett väldigt arkiveringsvänligt format.

- Det material man signerar **lämpar sig att sammanfattas i ett dokument**.
  Textdata avsett för människor är ofta mer praktiska att hålla i ett dokument än att lagra i en applikation.

- Det rör sig om **stora volymer**.
  När lärosätet sluter samma avtal med många parter (typiskt studenter) finns ofta ett business case i termer av effektivisering. Det kanske ligger mer i digitaliseringen av processen, men å andra sidan innehåller processen ofta inte så mycket mer än just signering och kan man då digitalisera den så har man gjort jobbet.

Det här är krav som om det föreligger indikerar att lösningar för digital signering kan vara aktuella.

Omvänt, det typiskt dåliga use caset (och i särklass vanligaste) är där man idag har ett signeringsförfarande av ett pappersdokument men där signeringen inte fyller något legal funktion och dokumentet i sig aldrig kommer att användas senare. Den här typen av use case handlar egentligen inte om signering, signeringens syfte är här att verifiera den manuella processen – dvs att ”alla har sett pappret”. Sådant ska implementeras som en funktion i ett IT system, någon digital signering behövs inte.

I linje med ovan bör man alltid fråga sig om det är signering man är ute efter eller om det egentligen är processtöd man behöver. Signering är nästan utan undantag ett steg i en längre process. Om processen innehåller ett antal steg varav signeringen bara är ett så är det en processdrivande applikation man behöver, inte (bara) en signeringslösning.

Use case

För att konkretisera har vi identifierat ett antal för lärosäten vanliga use case. Tanken är att man som arkitekt ska kunna relatera ett eller flera av sina egna use case till dessa och på så sätt hitta ett resonemang runt lösning.

UC1 - Digitalt signerat avtalsdokument med student

Beskrivning: Lärosätet sluter avtal med studenter.
Exempel: Avtal om hyra av studentbostad. Detta case har kommit från SU:s fastighetsavdelning.
Krav och förutsättningar för exempel use caset:

- avtalet ska finnas som ett digitalt dokument (tex en pdf),
- Dokumentet ska:
  - vara helt fristående från ett specifikt system
  - arkiveras på lärosätet under hela avtalsperioden
  - vara signerat av både lärosätet och student
- det ska gå att verifiera att de signerade parterna
- signaturerna ska gå att verifiera under hela avtalsperioden
- det ska gå att verifiera att dokumentet inte ändrats
- vara signerat av både lärosätet och student
- studenten kan vara svensk eller utländsk
- studenten ska inte behöva ha ett konto på lärosätet

Är use caset/use casen legitimt? Ja. Det här är inte orimligt att lösa via digital signering.
Finns ett business case? Ja, det är troligt att det här kan effektivisera avtalsslutande mellan studenter och lärosäte genom mindre pappers och posthantering.
Liknande use case: Liknande kan vara avtal om nyttjande av IT tjänster, användaravtal, mjukvarulicenser eller mjukare saker som tex att studenten signar av på lärosätets värdegrund. För dessa case är nog ofta ett signerat dokument ett praktiskt sätt att persistera saker, det är lätt och lämpligt att externalisera lösningen till en tjänst eftersom det drastiskt minskar applikationens användarbas – de flesta användare behöver inte in i systemet, bara signeringstjänsten.

UC2 - Signera interna beslut

Beskrivning: Ett antal interna parter på lärosätet är involverade i ett beslut och de ska alla signera beslutet.
Exempel: Finansiering och genomförande av ombyggnadsprojekt, SU:s fastighetsavdelning.
Krav och förutsättningar för exempel use caset:

- avtalet ska finnas som ett digitalt dokument (tex en pdf),
- Dokumentet ska:
  - vara helt fristående från ett specifikt system
  - arkiveras på lärosätet under överskådlig tid
  - vara signerat av alla involverade i beslutet
- det ska gå att verifiera de signerade parterna
- signaturerna ska gå att verifiera under överskådlig tid
- det ska gå att verifiera att dokumentet inte ändrats
- vara signerat av alla involverade i beslutet

Är use caset/use casen legitimt? Tveksamt i just exempel use caset, utmaningen här handlar nog snarare om workflow och processtödsbehov än signering för legala ändmål. Å andra sidan är ett fristående signerat dokument ett väldigt praktiskt sätt att persistera den här typen av informations.
Finns ett business case? Tveksamt. Man ska ha stora mängder beslut av den här karaktären och stor formalisering av processerna i så fall. Och då handlar det nog antagligen egentligen om processtöd mer än signering. Har man redan processtödet och bara vill lägga till signeringen är det ett annat läge, då skulle man kunna integrera en färdig extern signeringstjänst inifrån applikationen.
Liknande use case: Studieplaner för doktorander. Olika typer av "kollektiva" beslut på lärosäten där man har den här kravbilden. Köp av interna tjänster mellan avdelningar, som tex köp av IT-tjänster från IT avdelning.

UC3 - Tjänstetillsättning

Beskrivning: Tjänstetillsättning. En tjänst ska tillsättas och såväl externa som interna parter är involverade i beslutet.
Exempel:
Krav och förutsättningar för exempel use caset:

- avtalet ska finnas som ett digitalt dokument (tex en pdf),
- Dokumentet ska:
  - vara helt fristående från ett specifikt system
  - arkiveras på lärosätet under överskådlig tid
  - vara signerat av representanter från lärosätet och externa personer
- det ska gå att verifiera de signerade parterna
- fler än två signerade parter
- signaturerna ska gå att verifiera under överskådlig tid
- det ska gå att verifiera att dokumentet inte ändrats
- de signerande parterna kan vara både interna och externa parter
- de signerande parterna kan vara både svenska och utländska

Är use caset/use casen legitimt? Absolut ett legitimt use case i meningen av att det är av stor vikt att rätt personer skriver på och att det i efterhand går att verifiera vilka som gjort det.
Finns ett business case? Knappast. Volymerna är nog för små. Pappershantering blir billigare än IT stöd.
Liknande use case: ?

UC3 - Signerat av dokument av externa part

Beskrivning: En extern person framställer och signerar ett dokument som ska skickas in till lärosätet.
Exempel: Vid lärarnas praktik ute på skolorna (VFU) skriver producerar handledaren ett dokument (VFU rapport) som summerar studentens insats. Eftersom det är ett central underlag för betyg, måste på något sätt verifieras att det inskicka dokumentet verkligen kommer från handledaren i fråga. Handledarna har inget användarkonto i något av SU:s applikationer, idag rör det sig om 5000 – 6000 handledare.
Krav och förutsättningar för exempel use caset:

- rapporten ska finnas som ett digitalt dokument (tex en pdf),
- Dokumentet ska:
    - vara helt fristående från ett specifikt system
    - arkiveras på lärosätet under överskådlig tid
    - vara signerat av externa part
- det ska gå att verifiera den signerade läraren
- signaturerna ska gå att verifiera under överskådlig tid
- det ska gå att verifiera att dokumentet inte ändrats
- de signerande parterna är externa utan konto på lörosätet

Är use caset/use casen legitimt? Ja. Det här är ett reellt problem. I brist på lösning för digital signering användes engångslänkar som skickades till den emailadress man har associerad till läraren i LMS:et. Egentligen möter det inte kraven.
Finns ett business case? Ja. Det blir många VFU rapporter att hantera.
Liknande use case: ?

UC4 – Registerutdrag

Beskrivning: En extern person begär ett registerutdrag från lärosätet. Begäran ska signeras digital.
Exempel: PUL 26 § Ansökan om registerutdrag - en ansökan enligt första stycket skall göras skriftligen hos den personuppgiftsansvarige och vara undertecknad av den sökande själv.
Krav och förutsättningar för exempel use caset:

- ansökan ska finnas som ett digitalt dokument (tex en pdf),
- Dokumentet ska:
  - vara helt fristående från ett specifikt system
  - arkiveras på lärosätet under överskådlig tid
  - vara signerat av extern part
- det ska gå att verifiera vem som signerat det
- signaturerna ska gå att verifiera under överskådlig tid
- det ska gå att verifiera att dokumentet inte ändrats
- de signerande parterna är externa utan konto på lärosätet

Är use caset/use casen legitimt? Oklart. Helt klart är att personen måste identifieras I ansökningsögonblicket och att det framställda dokumentet bara ska få accessas av den som begärt det. Det senare sker idag med rekommenderat brev. Frågan är vad som gäller övriga krav, år det här egentligen bara ett autentisieringsbehov? Fyller signeringen idag egentligen bara ett identifieringsbehov? Eller är det verkligen krav på signering av ett dokument, dvs det ska kunna hanteras som ett fristående dokument?
Finns ett business case? Oklart. Beror på omfattningen av begäran om registerutdrag och i vad mån vi kan styra hur begäran om sådant görs.
Liknande use case: Är det legitimt så är nog även tex GDPR "rätten att bli glömd" ett annat case på samma tema.

UC5 - Digitalt signerade studieintyg av lärosätet

Beskrivning: Lärosätet utfärdar studieintyg av olika slag (betyg, xamen osv) som mottagaren, tex en arbetgivare vill kunna verifiera mot lärosätet.
Exempel: Även om lärosäten kan ha lokal utbildningar så ligger den absolut volymen av detta i Ladok. Finns krav runt detta på Ladok?
Krav och förutsättningar för exempel use caset:

- ansökan ska finnas som ett digitalt dokument (tex en pdf),
- Dokumentet ska:
  - vara helt fristående från ett specifikt system
  - arkiveras på lärosätet under överskådlig tid
  - vara signerat av lärosätet
- signaturen ska gå att verifiera under överskådlig tid
- det ska gå att verifiera att dokumentet inte ändrats

Är use caset/use casen legitimt? Ja, vissa lärosäten gör redan detta. I ett större perspektiv och på en längre horisont är det så klart rimligt att studenterna ska kunna få betyg som ett digitalt signerat fristående dokument.
Finns ett business case? Inte för lärosäten i dagsläget eftersom man ändå måste ha pappersprocesserna kvar, men det är ett rimligt krav från studenterna.
Liknande use case: Alla former av intyg runt att en student har examinerats och/eller deltagit i utbildningar, seminarier etc. I alla fall där vi idag delar ut ett påskrivet papper om sådant.

UC6 - Digitalt signerat avtalsdokument med extern part

Beskrivning: Lärosätet sluter affärsavtal med en extern part.
Exempel: Avtal om köp av mjukvara.
Krav och förutsättningar för exempel use caset:

- avtalet ska finnas som ett digitalt dokument (tex en pdf),
- Dokumentet ska:
  - arkiveras på lärosätet under hela avtalsperioden
  - vara signerat av både lärosätet och motparten
- det ska gå att verifiera att den signerade parterna
- signaturerna ska gå att verifiera under hela avtalsperioden
- det ska gå att verifiera att dokumentet inte ändrats

Är use caset/use casen legitimt? Ja.
Finns ett business case? För lärosätet finn inget business caset svagt. Volymen finns hos leverantören. De flesta leverantörer har massor av kunder och vill använda samma lösning för alla sina avtal, det kommer aldrig att vara aktuellt i dessa case att använda en lösning som lärosätet tillhandahåller.
Liknande use case: ?

UC7 – Intern beslutsprocess utan fristående dokument

Beskrivning: En process där ett antal olika parter i och utanför organisationen ska ta och verifiera interna beslut.
Exempel: Lönerevision, behörighetstilldelning.
Krav och förutsättningar för exempel use caset:

- inget behov av ett fristående signerat dokument finns
- arkivering av avsikten ska ske på lärosätet
- det ska gå att verifiera parterna
- det ska gå att verifiera att materialet inte ändrats

Är use caset/use casen legitimt? Nej. Eftersom det inte finns något krav ett fristående dokument och use caset handlar till väldigt stor del om workflow och till väldigt liten del om explicit signering passar denna typ av use case bättre i en applikation med normal inloggning, förslagsvis en workflow-/processcentrisk sådan.
Finns ett business case? NA

Under projektets gång har diskuterats att en lösning för digital signering skulle levereras av SUNET.

Fördelarna skulle vara det vanliga för en SUNET tjänst i förhållande till de nyttjande lärosätena:

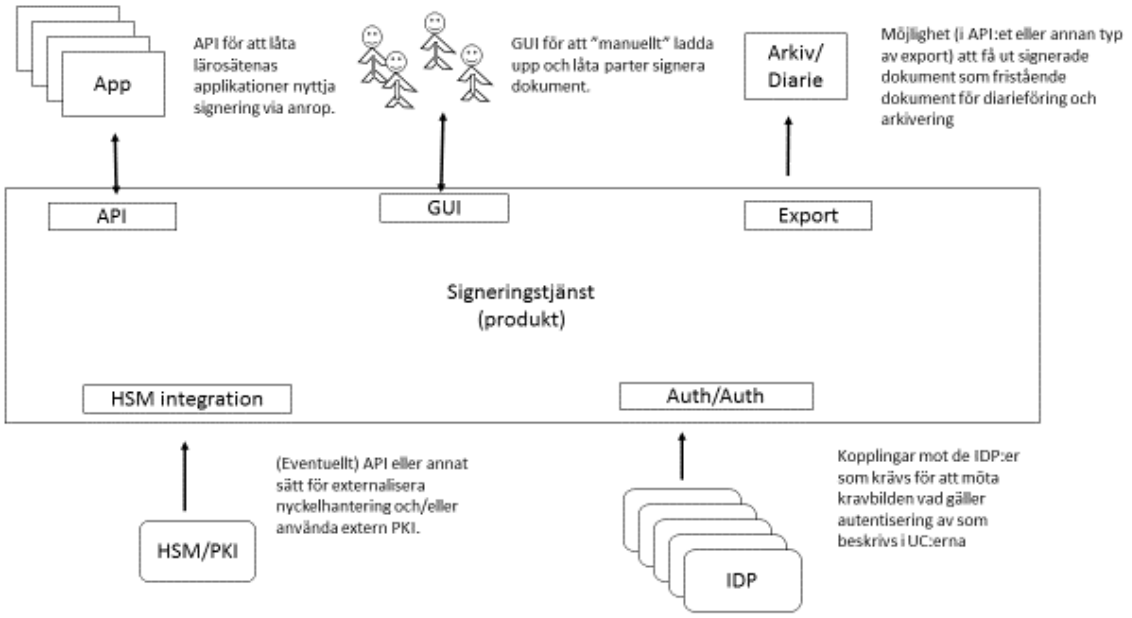
- out-of-the-box lösning redo för lärosätena att använda
- gemensam upphandling och leverantörskontakter ger mindre jobb
- skalfördelar
- specialisering i support
- anpassningar som krävs för lärosätesvälden, tex i termer av dokument arkivering, nyckehantering m.m.
- etc

Så vitt vi som gjorde denna utredning kan se finns inget egenvärde i att alla lärosäten implementerar sin egen lösning för digital signering. Tvärt om förefaller det finnas potential för både bättre lösning, bättre ekonomi och bättre lösningskvalitet genom att inrätta en gemensam tjänst.

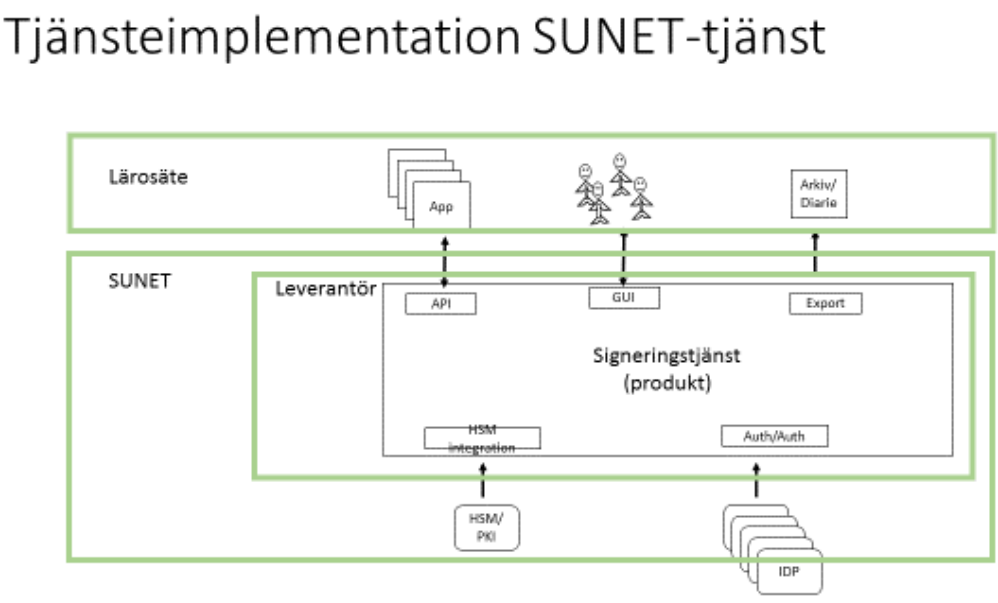
Det troliga är att SUNET skulle upphandla en lösning från tredje part, dvs ett produkt/tjänstebolag som levererar lösningar för digitala signaturer.

Vidare är det troligt att lösningen skulle se ut ungefär så som beskrivs i mönstret ”Produktbaserad” ovan, både med avseende på mönster och funktionalitet.

Följande beskriver en trolig kandidatarkitektur.



Följande beskriver rollspelet mellan de olika parterna:



Inkubator och ATI kommer som uppföljning till detta projekt sondera intresset för en SUNET-levererad tjänst.

Vi uppskattar om ni kontaktar SUNET eller ATI om ert lärosäte är intresserad av en sådan tjänst. Ju fler som är intresserade desto bättre lönsamheten i en sådan lösning.