

SUNET & digitala signaturer

Det finns ett stort intresse för att Sunet ska göra något inom området digitala signaturer. Under 2017-2018 drev Sunet Inkubator ett projekt med mål att inventera användningsfall som kan vara aktuella för digitala signaturer. I rapporten "En kokbok i digital signering" beskrev Mats Törnblom från Stockholms universitet 7 typfall med utgångspunkt från behov uttryckta av ett antal av landets lärosäten.

Rapportens slutsats är att Sunet bör undersöka förutsättningarna för att etablera en tjänst för digitala signaturer i syfte att kunna erbjuda stöd för några eller alla av dessa användningsfall.

Detta PM försöker helt kort inventera de alternativa lösningar för digitala signaturer som finns på marknaden och identifiera några viktiga skillnader mellan dessa. Detta PM utgör inte någon fullständig analys av hur typfallen i Inkubator-rapporten matchas av nedanstående alternativ utan är avsedd att utgöra underlag för en förstudie.

Inventering av alternativa e-signaturlösningar

Det finns i huvudsak 4 alternativ på marknaden:

- Docusign eller motsvarande tjänst baserad på *ritsignaturer*
- Adobe Sign dvs digitalt signerade PDF:er
- Leverantör av [godkänd sk fristående underskriftstjänst](#) ffa för signering av XML
- Fristående underskriftstjänst i Sunet regi (också för signering av XML)

Alternativ 3 och 4 är baserade på de e-signaturer som tagits fram av E-legitimationsnämnden (nu en del av DIGG.se). Detta är defacto-standarden för e-signaturer på myndigheter idag.

Alternativ 3 dominerar idag användningen av e-signaturer på myndigheter utanför sektorn. Detta alternativ implementeras ofta genom ett avrop från ett ramavtal hos Kammarkollegium och är i princip en molntjänst som drivs av ett antal leverantörer inom landets gränser.

Alternativ 4 handlar om att ta fram och driva en e-signaturstjänst i egen regi i Sunet. Sannolikt skulle detta arbete ske i nära samverkan med ett antal andra myndigheter (bla Pensionsmyndigheten) vars processer ger upphov till liknande behov. Sunet har redan flera viktiga förutsättningar på plats, bla säker nyckelhantering.

Dessa två alternativ har naturligtvis helt olika egenskaper, tex är ritsignaturer inte alls lika tekniskt säkra som digitala signaturer med RSA-nycklar men ur ett verksamhets- och juridiskt perspektiv är dessa i många avseenden jämförbara.

Ett litet antal lärosäten har redan genomfört egna projekt ffa med Adobe Sign. Användningen av Adobe Sign är också det enda alternativet som ger signerade PDFer som går att verifiera direkt i acrobat. Detta är viktigt om mottagaren av ett dokument ska kunna verifiera signaturen.

Bland övriga myndigheter är signerade XML-dokument defacto-standard och signaturen används ffa för att åstadkomma en hög grad av tilltro till lagrade transaktioner och skickas mer sällan direkt till en slutkund för verifiering.

De olika alternativen är mer eller mindre enkla att integrera mot men gemensamt för alla alternativ är att det finns en icke försumbar integrationskostnad och antagligen krävs någon form av ärendehanterings- eller dokumenthanteringssystem som fungerar som gränssnitt mot användaren för att flera av de användningsfall som presenteras i Inkubator-rapporten ska fungera i praktiken.

Viktiga skillnader mellan alternativen

Här följer en sammanställning av några olika aspekter som skiljer de olika lösningarna åt. Från tabellen framgår det rätt tydligt att valet inte är helt enkelt. Alla urvalskriterier som samtliga alternativ uppfyller är utelämnade. Många av dessa (tex att det finns ett API för integration) är onekligen viktiga men hjälper oss inte att välja bland alternativen eftersom alla 4 alternativen har APIer för integration.

	DocuSign	Adobe Sign	Digg e-signatur leverantör	Digg e-signatur i Sunet regi
Levereras inom EU/EES?	nej	nej	ja	ja
Prismodell	per användare	per signatur	per signatur	driftskostnad
Swamid?	ja ¹	ja ²	nej ³	ja
Signera PDF?	ja	ja	ja	ja
Signera XML?	nej	nej	ja	ja
Kryptografiska signaturer?	nej	ja	ja	ja
Avtal finns?	nej	ja	ja	ja

¹ integration krävs

² integration krävs

³ endast Svensk e-legitimation stöds officiellt av de flesta leverantörer

Sunet kontrollerar kryptonycklar?	nej	nej	nej	ja
Sunet är tjänsteleverantör?	nej	nej	nej	ja
Sunet är kontraktspart?	ja	nej	nej	ja

En första observation är att det är endast två av dessa alternativ där Sunet rimligen kan bidra med något värde:

- Alternativ 1: Sunet *upphandlar* en ritbaserad signaturtjänst, integrerar med Swamid och erbjuder en paketerad tjänst (i likhet med många andra tjänster)
- Alternativ 4: Sunet *driver en tjänst* i likhet med hur Swamid fungerar.

Övriga lösningar är baserade på molntjänster med existerande avtal då alltså Sunet varken kan vara involverad i driften av tjänsten eller etableringen av ett avtal. Värdet som Sunet bidrar med i dessa fall är alltså mycket litet.

En annan viktig skillnad är prismodellen. De flesta tjänster har en prismodell som är nyttjande-baserad. Detta kan betyda avsevärda kostnader i praktiken. Kostnaden för alternativ 3 är i praktiken ca 2 kr per signatur. För vissa tillämpningar - t ex utfärdande av signerade studieintyg kan antalet signaturer och därmed kostnaderna bli stora nog att det kan löna sig att utforska alternativ 4 som också har andra fördelar (tex att sektorn har full kontroll över kryptografiskt material).