E-SIGNERING

TL;DR

E-signatur är inte ett lagkrav utan måste motiveras av verksamhetsbehov

Inom Svensk statlig förvaltning finns en officiell standard för e-signatur

Moln-tjänster av typ DocuSign löser delvis andra problem och kan också ha en roll att spela

BAKGRUND

Elektroniska underskrifter (e-signaturer) är ett knepigt område. Det råder förvirring både kring mål, mening, krav och begrepp. Under de senaste året har Sunet allt oftare fått fråga om vi inte ”borde göra något kring e-signaturer”. Vi tror att det är dags att bena ut och sammanfatta frågan en gång för alla.

Ett av problemen med området är att det är lätt att sväva ut och inkludera allt som på något sätt involverar en digital signatur. Låt oss alltså börja med några ...

AVGRÄNSNINGAR

Teknisk informationssäkerhet är nästan alltid baserad på någon form av tillit och teknisk tillit är nästan alltid baserad på någon form av digitala signaturer. I begreppet *e-signatur* ligger dock oftast ett fokus på användning av digitaliserade underskrifter som stöd i förvaltningsprocesser snarare än ett fokus på den teknik som används – en PDF med en inklistrad bild av en namnteckning kan också vara en form av e-signatur.

En e-signatur är helt enkelt en teknisk representation av en underskrift eller myndighetsstämpel.

Under 2015 drev Sunet tillsammans med Chalmers, Linköpings Universitet, Linnéuniversitetet samt Örebro Universitet ett projekt på initiativ av IT-chefsforum där vi försökte reda ut de juridiska förutsättningarna för e-signaturer. Det vi kom fram till kan sammanfattas såhär: Lagen ställer (nästan) inga formkrav på underskrifter. Det betyder konkret att det inte (med några få undantag som inte berör högskolesektorn) finns några krav på hur underskrifter skall representeras IT-system.

Inget i Svensk lag säger alltså att bara för att man väljer att representera (tex) ett kontrakt som en PDF i ett dokumenthanteringssystem så måste PDF:en vara signerat med ett X.509 certifikat.

Frågan är alltså...

VARFÖR BRY SIG OM E-SIGNATURER?

Den frågan är motiverad. Om det inte finns några formkrav på underskrifter så kan man helt enkelt representera underskrifter som information i en databas. Dock finns det andra hänsyn än rent juridiska som kanske spelar större roll vid design av IT-system. Det är som alltid verksamheten som måste ställa krav som sedan eventuellt kan behöva uppfyllas genom att e-signaturer används. Låt oss titta på några exempel på behov som e-signaturer kan uppfylla:

1. **Arkivbarhet**. En e-signatur gör det möjligt att flytta ut ett objekt från det IT-system där det skapades samtidigt som det fortfarande går att verifiera att objektet (tex ett beslut eller ett betyg) utfärdats av någon person eller roll som hade rätt befogenhet.
2. **Säkerhet**. En e-signatur gör (beroende på teknologi-valet) det omöjligt att förfalska information i efterhand och stärker därför informationskvaliteten. Detta kan vara viktigt om informationen kommer användas vid revision eller liknande.

SÅ VAD SKA MAN GÖRA?

Det finns numera en teknisk specifikation inom Svensk offentlig förvaltning som beskriver hur ELN vill att e-signaturer ska fungera. Denna specifikation är baserad på OASIS DSS som är en standard som beskriver hur man kommunicerar med en signatur-tjänst på

nätet.

En av de mest långlivade intellektuella snedstegen i denna branch (ffa i Sverige) har kretsat kring uppfattningen att digitala signaturer implicit innebär ett krav på att den privata nyckeln som används vid den tekniska signaturen måste finnas på samma utrustning som den som utför signeringen. Detta ledde till oerhört komplicerade tekniska lösningar som involverar ”smarta” kort, applikationer som måste installeras och underhållas på en massa olika operativsystem för att inte tala om drivrutiner för kortläsare mm.

I och med att ELN bildades och började jobba för några år sedan kunde vi tänka om och få acceptans för tanken att det är skillnad på de nycklar som används för signeringen och de nycklar som ger rätt att utföra signeringen. Denna tanke har lett oss till en modell för e-signering (eller e-underskrift som ELN vill att vi kallar det) som både är säkrare och enklare att integrera än det som fanns tidigare och som dessutom passar bra ihop med federerad identitet.

Den tekniska arkitekturen som ELN beskriver i sina specifikationer är anpassad för Sveriges nya e-legitimationsstandard men det finns inget som hindrar att vi inom högskolesektorn använder samma ramverk anslutet till SWAMID.

& SÅ VAR DET DET HÄR MED DOCUSIGN…

Det finns idag ett antal molntjänster som använder begreppet ”digital signature” i sin beskrivning. Ett exempel är DocuSign vars främsta USP länge handlade om att vara duktig på att generera trovärdiga ”handstilsversioner” av ett namn som klistras in som bild i en PDF.

Detta handlar idag framför allt om workflow-motorer som fokuserar på kontrakts- och avtalshantering men som ändå kan vara mycket användbara eftersom de erbjuder APIer som är väl anpassade för moderna IT-ekosystem.

Vissa av dessa tjänster erbjuder även stöd för digitala signaturer som tillval. Väljer man denna typ av tjänst så gör man det nog dock av andra skäl än för att uppfylla högt ställda krav på arkivmöjlighet och säkerhet.

Eftersom vi i Sverige inte har något formkrav på underskrifter verkar det alltså inte finnas några direkta hinder för att använda en tjänst som DocuSign för att tex sköta kontraktshanteringen på en myndighet. Frågan man bör ställa sig är nog snarare om en sådan tjänst erbjuder tillräcklig säkerhet samt hur man ska bära sig åt om man tvingades flytta hela kontraktsdatabasen från en tjänst till en annan.

Självklart finns det också tillämpningar där sådana hänsyn inte spelar någon roll, tex kortlivade dokument där det är viktigare med smidig integration än att allt går att arkivera.

VAD TILLFÖR SUNET?

Detta är en berättigad fråga. Sunet strategi säger tydligt att Sunet bara ska göra tjänster där Sunet tillför ett värde. I detta fall finns det några uppenbara saker som Sunet kan tillföra förutom att agera samordnare och diskussionspartner:

- Integration med SWAMID.
- Drift av teknisk tillitsinfrastruktur, tex säker nyckelhantering i HSM:er

Drift av säker nyckelhantering är naturligtvis inte ett krav om man använder tjänster som DocuSign men är ett absolut krav om man ska använda sig av ELN e-signaturstandard där signaturer sker med sk stämpelcertifikat som är kopplade till varje myndighet och är beroende av en infrastruktur som kan generera nya nycklar och certifikat för varje underskrift.

Nästa steg skulle kunna vara att Sunet undersöker formerna för ett samarbete kring både DocuSign-liknande tjänster samt kring ELN e-underskriftstjänster. Det finns antagligen utrymme för mer än en lösning inom detta område. Vad tycker du? Hör av dig och berätta!

Skriven av

LEIF JOHANSSON

Blogs about past, present and future technology initiatives in the CTO-blog.