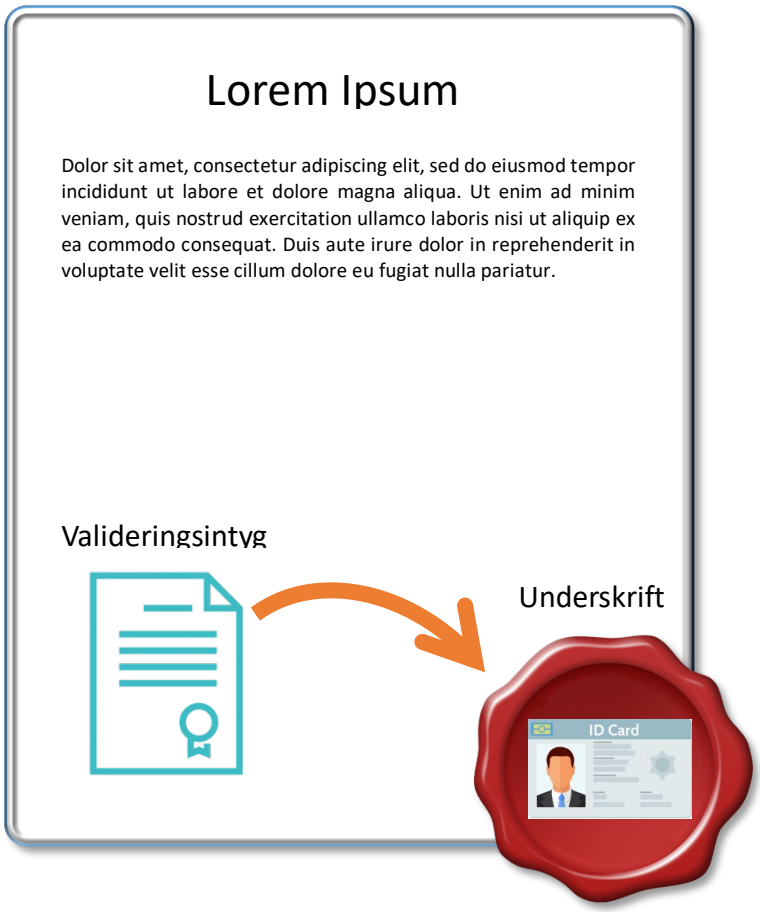
Arkivering av elektroniskt underskrivna dokument med valideringsintyg



En elektronisk underskrift binder ett elektroniskt dokument till en undertecknares unika identitet. Genom underskriften kan vem som helst verifiera vem som skrivit under och vad som skrivits under genom att verifiera underskriften med publikt publicerade verifieringsnycklar.

En stor utmaning med elektroniska underskrifter är dock att denna möjlighet att verifiera underskriften med publikt tillgänglig information är tidsbegränsad. En sådan tidsbegränsning skapar problem för elektroniska handlingar där underskriften måste kunna bevaras och valideras under lång tid, till exempel vid upprättande av elektroniska avtal.

I detta kortfattade PM introduceras valideringsintyget som en smidig och enkel lösning på arkiveringsproblematiken kring elektroniska underskrifter, med vars hjälp en elektronisk underskrift kan valideras långt in i framtiden till låg kostnad och utan onödig komplexitet.

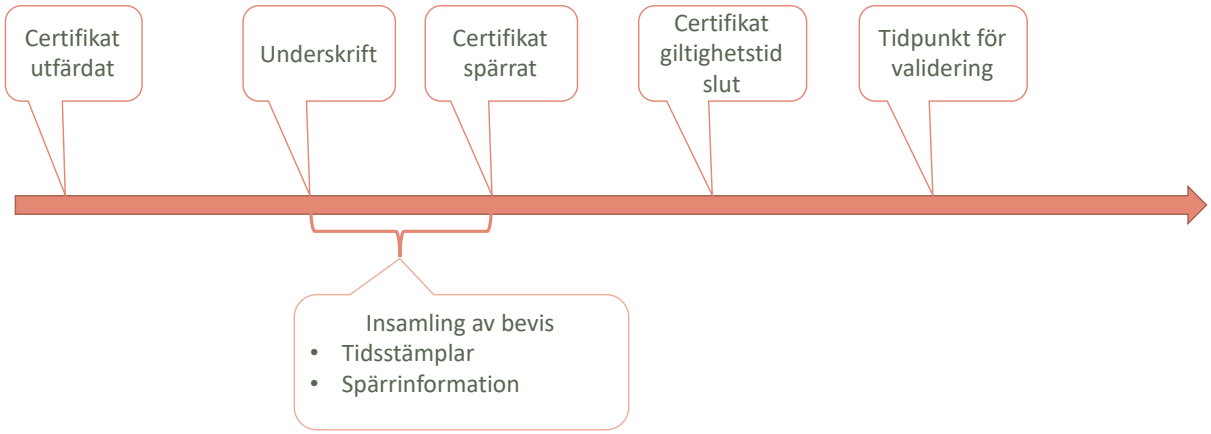
Tidsbegränsningen för elektroniska underskrifter

Elektroniska underskrifter är tidsbegränsade av främst två faktorer:

- Nycklar och kryptoalgoritmer blir gamla och försvagas med tiden.
- Underskriftscertifikatet som intygar undertecknarens identitet har en begränsad giltighetstid och kan dessutom bli spärrat.

Kryptografiska algoritmer och nycklar som väljs med omsorg bör vara tillförlitliga under relativt lång tid, men för elektroniska dokument som måste kunna valideras under väldigt lång tid kan detta vara den svåraste utmaningen då det innebär att elektroniska bevis eroderar på en ganska fundamental nivå. Problemet med certifikat som spärras eller löper ut, är däremot ett enklare, men å andra sidan mer konkret problem, som kan aktualiseras efter relativt kort tid efter det att en elektroniskt undertecknad handling mottagits.

Underskriftscertifikatet fyller funktionen av en elektronisk ID-handling som binder de underskriftsnycklar som använts för att skriva under till identiteten på undertecknaren. Undertecknaren, vars identitet styrks i certifikatet blir därmed ansvarig för underskriften och dess legala konsekvenser.



Följande tidsaxel illustrerar den elektroniska underskriftens livscykel som styrs av ett antal tidpunkter som kan infalla på olika ställen och i olika ordning på tidsaxeln. Detta sträcker sig från tidpunkten då underskriftscertifikatet utfärdades fram till tidpunkten då en validering skall göras lång tid efter det att certifikatets giltighetstid löpt ut.

För att kunna genomföra en sådan validering måste man kunna fastställa att certifikatet inte var spärrat vid underskriftstillfället, vilket i sin tur kräver bevis för att underskriften genomfördes vid en tidpunkt innan certifikatet antingen spärrades eller löpte ut.

Skulle ett certifikat vara spärrat vid valideringstillfället så kan underskriften inte valideras med mindre än att man kan visa att dokumentet undertecknades innan certifikatet spärrades. Elektroniska underskrifter saknar ofta en säker uppgift om tidpunkten när underskriften skapades, en s.k. tidsstämpel, utfärdat av oberoende tidsstämplingstjänst. I avsaknad av sådan tidsstämpel blir en underskrift automatiskt ogiltig när ett certifikat spärras, även om det sker efter det att underskriften skapades. Detta beroende på att det

inte går att påvisa när dokumentet skrevs under. Om signaturen tidsstämplats så är dock underskriften giltig om tidsstämpeln bevisar att underskrift skedde innan certifikatet spärrades.

Utfärdare av certifikat är endast skyldiga att tillhandahålla uppgift om spärrning under certifikatets giltighetstid. När denna tidpunkt löpt ut finns inte längre någon möjlighet att kontrollera certifikatets giltighet mot en spärrtjänst. Detta gör att certifikatets giltighetstid utgör en bortre gräns för när underskriften kan valideras om inte underskriften kompletteras med annat bevismaterial.

Strategier för långtidsvalidering

För att möjliggöra validering efter lång tid krävs att man tillför intyg från betrodd part rörande förhållanden som är avgörande för underskriftens giltighet. Detta kan röra sig om att man tillför tidsstämplar som bevisar när en underskrift utförts, eller intyg om att ett visst certifikat inte var spärrat vid en given tidpunkt.

Den enklaste formen av externt intygande är helt enkelt att man för loggar över att en elektronisk underskrift kontrollerades vid mottagandet och befanns giltig. En sådan lösning har ganska uppenbara brister genom att loggen inte låser dokumentets utformning, och om dokumentet skulle modifieras efter loggningen så kan inte loggen användas för att upptäcka en sådan modifiering. Logglösningen ställer därför högre krav på att lagrade elektroniska handlingar integritetsskyddas.

Två aktuella strategier som däremot innebär att man faktiskt kan verifiera den ursprungliga underskriftens äkthet är **Arkivtidsstämpel** och **Valideringsintyg**

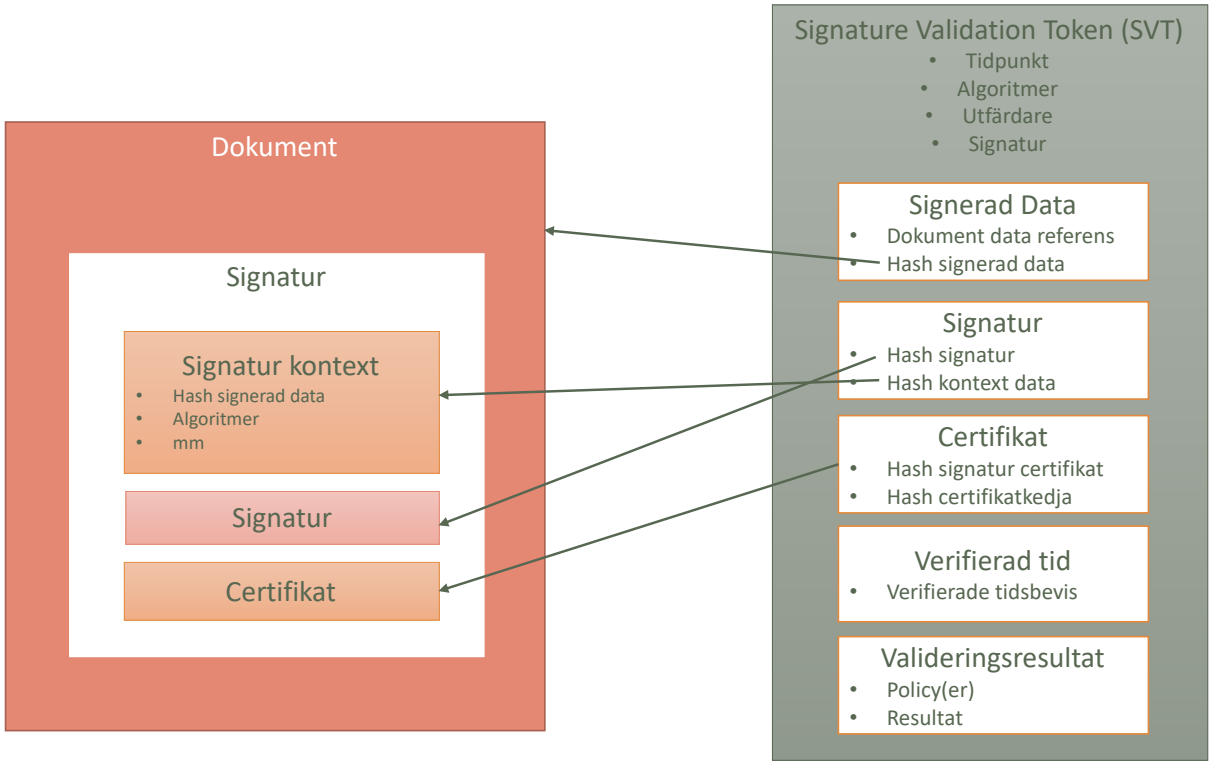
Arkivtidsstämpel som bl.a. realiseras av ETSI LTA signaturer (Long Term Archival) innebär att man samlar ihop all tillgängliga valideringsdata i form av tidsstämplar, certifikat och spärrinformation och tidsstämplar all denna information, inklusive den ursprungliga handlingen.

Den stora utmaningen med arkivtidsstämpling är att valideringsprocessen kan bli enormt komplex över tiden på grund av rekursivitet. Rekursivitet uppstår när bevis måste stödjas av bevis som måste stödjas av bevis, o.s.v. i långa beviskedjor. Detta förvärras över tiden och kan medföra en exponentiell komplexitetsökning i vissa fall.

Valideringsintyg – ett enklare alternativ

Valideringsintyg är ett samlat intyg från en betrodd valideringstjänst att denna validerat en elektronisk underskrift, när valideringen utfördes och resultatet av valideringen.

Valideringsintyget utgör en betydligt enklare modell jämfört med arkivtidsstämpling genom att ersätta komplexa beviskedjor med ett enda intyg som intygar allt som krävs för att validera underskriften i framtiden.



Valideringsintyget (SVT = Signature Validation Token) åstadkommer detta genom att i ett och samma intyg styrka:

- Den underskrivna handlingens innehåll
- När intyget utfärdades (funktionen av tidsstämpel)
- Underskriftens utformning och äkthet
- Underskriftscertifikatets giltighet
- Intyg om tidsstämplar som validerats

Vinsten med denna metod är att problemet med rekursivitet helt undanröjs genom att intygsbehovet reduceras till ett intyg som valideras med en signatur från en betrodd tjänst. Eftersom allt intygas i ett och samma intyg så undanröjs behovet av att validera alla individuella spärrlistor och certifikat som måste valideras i fallet med arkivtidsstämplar.

Ytterligare en vinst är att valideringsintyget även löser problemet med algoritmer och nycklar som blir för gamla eftersom valideringsintyget även intygar såväl dokumentets utformning som vilka signaturdata och certifikat som validerats. Detta kan helt ersätta behovet av att validera ursprungliga nycklar och algoritmer.

Det finns även juridiska fördelar som bör övervägas i juridisk analys. Valideringsintyg erbjuder en enklare logik där ett enda intyg från trovärdig tjänst visar underskriftens giltighet. Detta skall ställas mot lösningar med avsevärt högre komplexitet där många olika bevis måste samverka i en komplex beviskedja.

Utfärdande av valideringsintyg

Valideringsintyg utfärdas av en fristående valideringstjänst som validerar den elektroniska underskriften och utfärdar ett intyg om utförd validering i form av ett valideringsintyg. Valideringsintyget lagras i den elektroniskt underskrivna handlingen så att den sedan alltid finns tillgänglig vid framtida validering av underskriften.

All framtida validering av underskriften kan nu ske med stöd av valideringsintyget.

Det är således lämpligt att berika underskrivna handlingar med valideringsintyg så fort som handlingen undertecknats av alla som skall underteckna handlingen, och innan handlingen arkiveras.

Om behov uppstår i framtiden kan valideringsintyg förnyas genom att ett nytt valideringsintyg utfärdas baserat på ett tidigare valideringsintyg som ersätter det gamla. Vid normal tillämpning är det dock inte tänkt att valideringsintyg skall behöva förnyas om det inte rör sig om arkivering under mycket långt tid där kritiska algoritmer som tillämpats vid utfärdande av gamla intyg inte längre anses vara säkra.

Standardisering

En viktig fråga som avgör användbarheten av valideringsintyg är om det är avgörande att alla använder samma lösning och att en sådan lösning därför är standardiserad.

När det gäller lösningar för långtidsvalidering finns dock väldigt begränsade behov av standardiserade lösningar eftersom det är förlitande part själv, och inte den som skriver under, som avgör hur arkivering skall gå till och hur man väljer att säkra bevis för underskriftens äkthet som kan valideras i framtiden.

Idag löser många myndigheter frågan på helt egna sätt. Ofta sker detta endast genom att logga det faktum att handlingen signerats och av vem, utan tillämpning av starka kryptografiska bevis.

Det viktigaste är att den lösning som tillämpas är ändamålsenlig och representerar en god avvägning mellan risk, effektivitet och kostnad.

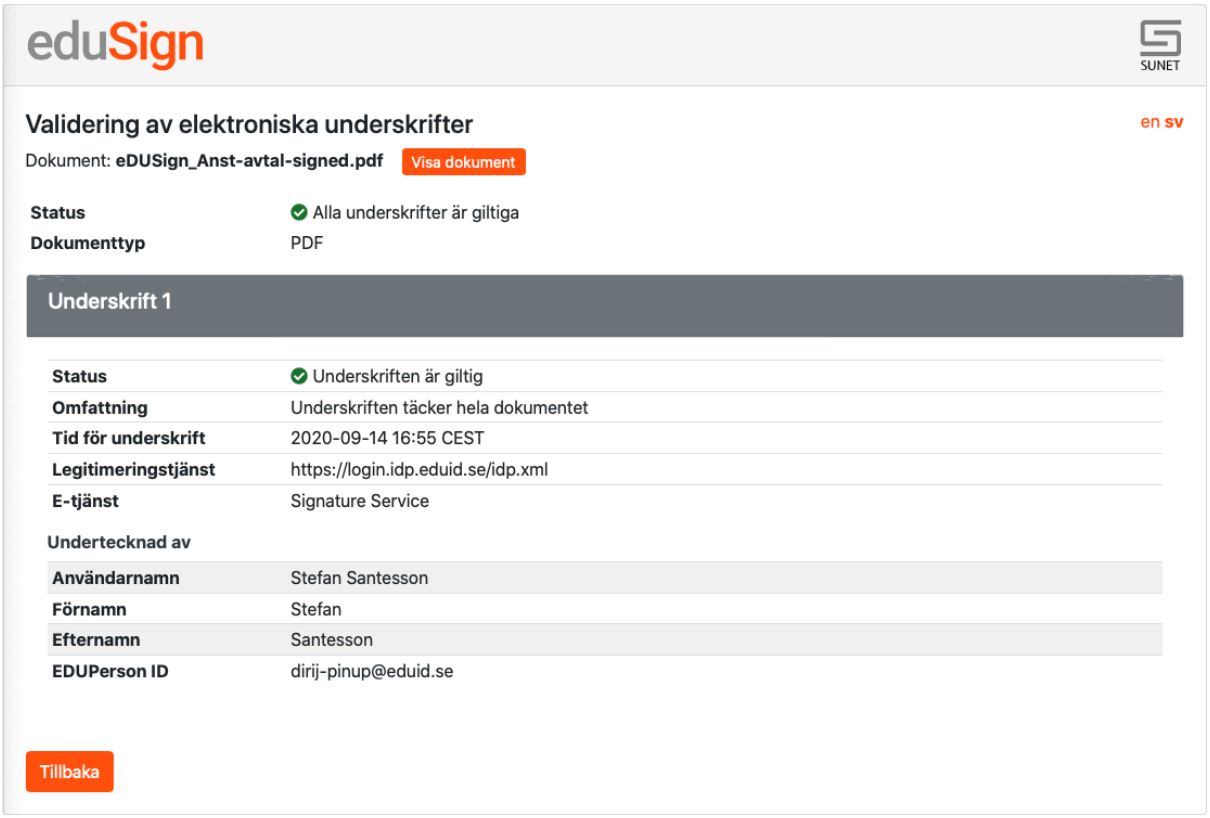
Standardisering underlättar dock tillgång till kostnadseffektiva lösningar och en allmän acceptans och därför pågår även aktiviteter med syfte att standardisera ett format för valideringsintyg inom IETF (Internet Engineering Task Force). Nuvarande förslag på dataformat för valideringsintyg finns publicerat på GitHub under Sweden Connect:s tekniska ramverk (https://github.com/swedenconnect/technical-framework/):

Dokument	Länk
SVT basformat	https://docs.swedenconnect.se/technical-framework/updates/15_-_Signature_Validation_Token.html

PDF profil	https://docs.swedenconnect.se/technical-framework/updates/16_-_PDF_Profile_for_Signature_Validation_Tokens.html
XML profil	https://docs.swedenconnect.se/technical-framework/updates/17_-_XML_Profile_for_Signature_Validation_Tokens.html

eduSign

SUNET ingår i ett forskningsprojekt som finansieras med stöd av Vinnova och som syftar till att ta fram och prova tillämpning av valideringsintyg inom skolsektorn.



Denna tjänst kommer tillhandahålla möjligheter att berika validerade underskrivna handlingar med valideringsintyg. Dels kommer det finnas möjlighet vid validering att manuellt ladda hem det validerade dokumentet med valideringsintyg och dels kommer tjänsten att tillhandahålla ett REST API som kan användas av e-tjänster direkt för att på automatisk väg såväl validera underskrivna handlingar med eller utan valideringsintyg samt om så önskas, att berika underskrivna handlingar med valideringsintyg.

Valideringstjänsten byggs med öppen källkod vilket möjliggör för institutioner att bygga och driftsätta sin egen valideringstjänst.