Riksarkivet

Rapport

Författare	Avd	Telefon	Datum	Version	Sida
Benjamin Yousefi	DOI	010-476 72 98	2014-10-07	1.3	1 (85)
Projekt **Arkiv E** **Delprojekt 3: Framställning och bevarande av elektroniska signaturer**	Noteringar Direktiv DOI 2013:1 Dnr RA 20-2013-1154				

Framställning och bevarande av elektroniska signaturer

Innehållsförteckning

1. Inledning

1.1. Förkortningar

a.	avsnitt,
b.	bilaga
n:n	paragraf, avsnitt eller sida med tillhörande stycke *exempel* § 7:2 paragraf 7, stycke 2 a. 7.1:2 avsnitt 7.1, stycke 2 s. 71:2 sida 71 stycke 2
s.ä.	se även

AL	Arkivlag (1990:782)
FL	Förvaltningslag (1986:223)
BrB	Brottsbalken
DES	Direktiv om elektroniska signaturer; Europaparlamentets och rådets direktiv 1999/93/EG av den 13 december 1999 om ett gemenskapsramverk för elektroniska signaturer
LKES	Lag (2000:832) om kvalificerade elektroniska signaturer
OSL	Offentlighets- och sekretesslagen (2009:400)
TF	Tryckfrihetsförordningen

1.2. Bakgrund

Detta arbete framställdes inom ramen för Riksarkivets projekt ”ArkivE”: Dnr RA-20-2013-1154; Direktiv DOI 2013:1, den 18 mars 2013, som delprojekt 3: Framställning och bevarande av elektroniska signaturer. Ansvarig för arbetet var Benjamin Yousefi i EUF (Enheten för utveckling och e-förvaltning) under DOI (Divisionen för offentlig informationshantering).

1.3. Syfte

1.3.1. Huvudprojektet

Det övergripande effektmålet för projektet ArkivE är ”[a]tt de format för framställning och bevarande av elektroniska handlingar som används inom offentlig förvaltning är ändamålsenliga och uppfyller de krav som ställs genom arkiv- och offentlighetslagstiftning samt att handlingarna kan bevaras i ursprungligt skick.”

Projektmålet är ”[a]tt utveckla och tillhandahålla underlag till föreskrifter, rekommendationer och vägledningar som kan tillgodose lagstiftningens krav på en god offentlighetsstruktur, och som är anpassat till dagens teknikberoende förvaltning.”

1.3.2. Delprojekt 3

1.3.2.1. Effektmål

Delprojektets effektmål är ”[a]tt elektroniskt underskrivna handlingar och e-signaturer hanteras utifrån bestämmelser i TF och AL samt att handlingarna kan bevaras för framtiden med det innehåll och de egenskaper de ursprungligen haft, dvs i ursprungligt skick”.

1.3.2.2. Delprojektmål

Delprojektmålet är ”[a]tt genomföra en kartläggning/utredning av den föreslagna lösningen för e-signaturer utifrån offentlighets- och arkivperspektiv. Kartläggningen ska utgöra underlag för en översyn av nuvarande föreskrifter, RA-FS 2009:2 samt en vägledning som tas fram av enheten för Utveckling och e-förvaltning.”

1.3.2.3. Avgränsningar

Delprojektet ska inte se över den tidigare rapporten Elektroniskt underskrivna handlingar, men ska peka på eventuella brister i rapporten.

1.3.3. Leverans

I den övergripande leveransen förväntades ”framställning och bevarande av elektroniska signaturer” och ”utredning avseende formatval för e-signaturer”, medan i delprojekt direktivet angavs ”[r]apport med analys av den föreslagna lösningen för elegitimationer samt förslag på åtgärder inom normering och främjande.”

1.4. Disposition

1.4.1. Tolkning av direktivet

Målet med projektet är att leverera underlag till framtida produkter, såsom författningar och publikationer. Detta har tolkats, tillsammans med delprojektmålets användning av ordet ”kartläggning”, att leveransen rent faktiskt ska utgöra något som närmast kan likna ett ”referensverk”.

Det övergripande effektmålet och delprojekteffektmålet, tillsammans med den övergripande leveransen, har tolkats som att arbetet ska omfatta bevarandet av digitalt signerat dataobjekt. I delprojektmålet framgår att den ”förslagna lösningen för e-signaturer” och att delprojektleveransen ska omfatta en ”analys av den förslagna lösningen för elegitimationer”.

Leveransen förväntar även förslag på åtgärder inom normering och främjande. Detta har tolkats att utforma en modell eller liknande konstruktion för analys och värdering.

1.4.2. Upplägg

Mot bakgrund av a. 1.4.1 Tolkning av direktivet, framställningen är organiserad i sex huvudavsnitt:

- 2, Elektroniska signaturer, reder ut ämnesområdets begreppsapparat;
- 3, Teknik, beskriver tekniken bakom ämnesområdet;
- 4, Infrastruktur, redogör för juridiska och organisatoriska infrastrukturer bakom ämnesområdet;
- 5, Bevarande av elektroniska signaturer för en obestämd framtid, sammanfattar metoder för och faktorer som påverkar långtidsbevarandet av elektroniska signaturer;
- 6, Riksarkivets perspektiv på ämnesområdet samt en modell för analys och värdering.[1]

1.5. Avgränsningar; framtida kompletteringar

Följande områden har avgränsats bort, men bör införlivas vid ett eventuellt fortsatt arbete, i syfte att mer utförligt komplettera och koncentrera denna framställning.

1.5.1. Federation

Frågor som berör ”federation” måste uppdateras, juridiskt såväl som tekniskt, eftersom vid skrivande stund (hösten 2013) så pågår fortfarande arbetet med svensk federation.

1.5.2. Format

Endast formaten för elektroniska signaturer har redovisats. Formaten för den elektroniska signaturens komponenter, exempelvis tidstämpeln, certifikat eller återkallelsestatus, har inte analyserats.

Långtidsbevarandet av elektroniska signaturer förutsätter att alla relevanta komponenter bevaras, men det är bevarande av signaturens autenticitet som är av särskild betydelse (jfr ArkivE ”kontorsdokument”). Den metod för långtidslagring av elektroniska signaturer som standardiserads i de format som undersökts är [rekursiv] tidstämpling. Detta innebär att komponenternas format är sekundär till att bevara autenticiteten.

Det kan emellertid visa sig vara nödvändigt att analysera den elektroniska signaturens övriga komponenter vid en eventuell rekommendation av tekniska riktlinjer (se vidare a. 1.5.6, Modell för teknisk analys).

1.5.3. Gällande rätt

Det juridiska avsnittet behandlar den svenska implementeringen av DES, men inte själva direktivet. Genomgång av direktivet skulle ha varit önskvärt, men inte längre aktuellt, eftersom EU arbetar i skrivande stund (hösten 2013) med en förordning avseende elektroniska betrodda tjänster, vilket ska ersätta DES. Det kommer att vara nödvändigt att uppdatera arbetet när förordningen träder i kraft.

[1] Kommer att publiceras vid en senare tidpunkt.

1.5.4. Illustrationer

På grund av tidsbrist saknas illustrationer för avsnitten 4.1.6 Certifikat och 4.5 Federation. Framtida uppdateringar kan åtgärda denna brist.

1.5.5. Modell för policy

Valideringen av en elektronisk signatur kan vara avhängig en policy, och en avsaknad av policy kan nervärdera signaturens autenticitet. Olika utfärdare av elektroniska signaturer kan ställa olika krav på elektroniska signaturer, exempelvis för fakturor, kontrakt, eller intyg, med följd att framställningen och valideringen av elektroniska signaturer kan avgrena och komplic eras (jfr a. 3.3.6.6, Exempel på hur XAdES variationerna kan byggas på varandra; s.ä. a. 5.1.2, Policy). Problemet kan liknas vid idén av en standard och implementeringen av den standarden. Det kan vara nödvändigt att närmare analysera frågan, och eventuellt uppställa en modell för framställningen av policy (jfr a. 1.5.6, Modell för teknisk analys).

1.5.6. Modell för teknisk analys

Medan det kan diskuteras om tekniska frågor ska behandlas av Riksarkivet så finns det en risk att implementeringen av elektroniska signaturer för långtidsbevarande kan få skiftande tillämpningar över utfärdare eftersom behoven varierar (se 1.5.5, Modell för policy), frågorna är komplicerade och ”andra intressen” kan verka; liknande problematiken med idén av en standard och implementeringen av den standarden. Det kan därför finnas ett behov att nyansera långtidslagringen av signaturer genom att producera underlag för valen av tekniska komponenter eller inköp av tjänster. Det kan exempelvis röra sig om att sammanställa underlag för algoritmer för kondensat och kryptering som rekommenderas eller avråds, hur sammansättningen av signaturen tillsammans med dataobjektet kan ta form, och rekommenderade standard för certifikat och återkallelsestatus (a. 3.3.6.6, Exempel på hur XAdES variationerna kan byggas på varandra; jfr teoretisk och praktisk PDF/A).

2. Elektroniska signaturer

Detta avsnitt beskriver de faktorer och relationer, samt de ord och begrepp som associeras med dem, som tillsammans åsyftar ”elektronisk signatur”. Beskrivningen är abstrakt och härledd från metoder som är tillgängliga för att producera elektroniska signaturer samt den lagstiftning som gäller på området [2013].

2.1. Elektronisk och digital signering samt elektronisk underskrift

En ”elektronisk signatur” är den formella benämningen i svensk och EU-rätt för motsvarigheten till ”egenhändig underskrift” i digital miljö. ”Digital signatur” i jämförelse används ibland som en synonym till elektronisk signatur, men kan ha innebörden av att vara en särskild implementering av elektroniska signaturer. Elektronisk signering kan därför ses som en övergripande definition, vilket exempelvis infattar angivelse av sitt namn i anslutning till en text eller uppgift i elektroniskt form (Elektronisk dokumenthantering, Riksarkivet [Lagerlöf & Leman] Rapport 2000:1 s. 23, jfr prop. 1999/2000:117 s. 19:5; jfr Wikipedia ”Electronic signature” och ”Digital signature”).[2]

I svensk lag används ”avancerad elektronisk signatur” och ”kvalificerad elektronisk signatur” (se LKES § 2 jfr DES). Digitala signaturer, som en särskild implementering av elektroniska signaturer, bör motsvara ”avancerade elektroniska signaturer” (Ds 1998:14, a. 2 Vad en digital signatur är, jfr Elektronisk dokumenthantering, Riksarkivet [Lagerlöf & Leman] Rapport 2000:1, s. 17; jfr Statskontorets rapport 2003:13 s. 22, ”… mer avancerade, och säkrare, formen av elektronisk underskrift…”).

Den elektroniska signeringen har två funktioner. Den elektroniska signaturen sammankopplar data/information till en källa [undertecknaren]. ”Styrkan” av denna koppling kan sedan i olika grader bindas genom tekniska metoder i syfte att säkerställa att data/informationen faktiskt härrör från angiven signatur. För att uppnå detta måste man även säkerställa att data/information som signerats är detsamma som undertecknaren ursprungligen signerade [innehållets integritet]; den elektroniska signeringens andra funktion.

Det följer av den elektroniska signaturens ändamål att den inte har som funktion att skydda innehållet från obehörig insyn [konfidentialitet].

2.1.1. Elektronisk underskrift

I E-legitimationsnämndens modellbeskrivning av ”Svensk e-legitimation” används ”elektronisk underskrift” (jfr ”underskriftstjänster” i ”Federationen”, se vidare a. 4.5.3) istället för ”elektroniska signaturer”, i enlighet med SAMSET-projektets[3] slutsatser om förväxlingsrisk med andra typer av signaturer (Svensk e-legitimation s. 5:2; jfr SOU 2010:104 b. 10 a. 7, i för-

[2] Jfr LKES § 2:2 och 2:3, samt prop. 1999/2000:117 s. 39:3, elektronisk signatur är bara ”… en teknisk metod och [behöver inte] vara knuten till en fysisk person.”.

[3] <skatteverket.se/privat/etjanster/samsetelegitimationforidentifieringunderskrift.4.18e1b10334ebe8bc800046.html> hämtat sommaren 2013.

arbeten och lagkommentarer framkommer en liknande uppfattning, ”att en underskrift ska vara elektroniskt” har tolkats [felaktigt] som om att det *måste* vara en kvalificerad elektronisk underskrift, jfr a. 2.1.3, Juridiskt perspektiv.).

I RSV M 2003:24 (Grundläggande riktlinjer för myndigheternas användning av e-legitimationer och elektroniska underskrifter) definieras ”elektronisk underskrift” som en [synonym till] ”avancerad elektronisk signatur”, medan ”kvalificerad elektronisk signatur” tillämpas i sin ursprungliga bemärkelse. Detta kan jämföras med hur riktlinjen definierar ”elektronisk signatur”: ”En digital namnteckning som inte behöver uppfylla myndigheternas krav på elektronisk underskrift”. Mot bakgrund av det anförda, och diskussionen i a. 2.1.3, Juridiskt perspektiv., verkar ”elektroniskt underskrift” motsvara ”avancerad elektronisk signatur” med eventuella myndighetskrav med ambition att uppnå nivån av kvalificerade elektroniska signaturer (jr SOU 2010:104 a. 3.7:1, ”[tjänst för att skapa elektroniska underskrifter] bör om möjligt utformas dels så att kvalificerade certifikat utfärdas momentant, dels så att en säker anordning för signaturframställning tillhandahålls så att de elektroniska underskrifterna **kan anses** vara kvalificerade.”, betoning inte i original, jfr. s. 71:2).

2.1.2. Oavvislighet

Oavvislighet (eng. ”non-repudiation”) är ett begrepp som innebär att en person som vidtagit en åtgärd inte i efterhand ska kunna förneka att åtgärden vidtagits. Åtgärden kan syfta på en konkret handling som att exempelvis skicka eller ta emot ett meddelande eller upprätta innehållet i ett meddelande (Statskontorets rapport 2003:13 a. 3.8).

2.1.3. Juridiskt perspektiv

2.1.3.1. Rättslig effekt

Den ”rättsliga effekten” [bevisverkan och rättslig verkan] av elektroniska signaturer kan särskiljas som att ha en gemensam utgångspunkt med inskränkande undantag.

Huvudregeln kan sägas vara att ingen elektronisk signatur får förvägras rättslig verkan eller inte godtas som bevis enbart på den grunden att den är elektronisk. En elektronisk signatur *ska* jämställas med [tillerkänns samma rättsliga verkan som] en ”analog signatur” [egenhändig underskrift] när den är en kvalificerad elektronisk signatur, det vill säga en särskild typ av elektroniska signaturer. Detta utesluter emellertid inte att elektroniska signaturer med en *lägre* säkerhetsnivå än kvalificerade elektroniska signaturer *kan* jämställas med ”analoga signaturer” (prop. 1999/2000:117 s. 58:4, man får dock inte uppställa *högre* säkerhetskrav än kvalificerade elektroniska signaturer; jfr SOU 2010:104 a. 7, Juridiska frågor om Säkerhetsnivå).

Elektronisk signatur	Erkännande	Säkerhetsnivå
Kvalificerad	Tillräckligt	Maximum
Inte en kvalificerad, det vill säga, avancerade eller ”annan”	Möjligt	Lika med eller under men inte högre än maximala säkerhetsnivån

Undantagen, som indirekt inskränker den elektroniska signaturens rättsliga verkan i förhållande till den ”analoga signaturen”, är att den kan nekas på andra grunder, såsom att den inte uppfyller formkrav eller att det inte är tillåtet att använda elektroniska medel eller, när inom den offentliga sektorn,[4] ytterligare villkor uppställs på den elektroniska signaturen (jfr prop. 1999/2000:117 s. 78:3, kravet på ”underskrift” i författningar utesluter som huvudregel elektroniska signaturer). Undantaget omfattar enbart den elektroniska signaturens rättsliga verkan och inte dess bevisverkan i domstolsförfarande, på grund av den rättsliga principen om ”fri bevisföring” i svenska domstolar (LKES § 17, se vidare prop. 1999/2000:117 a. 6.11, Kvalificerade elektroniska signaturer, se särskilt s. 56:7-57:1, jfr 57:6, 58:3).

En myndighet kan med stöd av LKES § 17 uppställa ytterligare villkor för elektroniska signaturer, såsom att tekniska beskrivningar över formatet måste bifogas, förutsatt att villkoren inte utgör ett högra krav på vad som krävs av kvalificerade elektroniska signaturer. Fråga om villkoren omfattar innehållet som signerats eller bara själva signaturen (prop. 1999/2000:117 s. 59:5-6). Detta utesluter dock inte helt att höga krav kan under vissa omständigheter uppställas inom särskilda områden (prop. 1999/2000:117 s. 60:2).

Alla typer av elektroniska signaturer

Tillåtet att fullgöra ett rättsligt förfarande med elektroniska medel?

Uppfyller eventuella myndighetsvillkor?

2.1.3.2. Fråga om undertecknaren kan vara en juridisk person

Begreppet elektroniska signaturer använder uttrycket utställare, vilket kan vara en juridisk såväl som fysisk person (LKES § 2:2; prop. 1999/2000:117 s. 39:3, en elektronisk signatur är bara ”… en teknisk metod och [behöver inte] vara knuten till en fysisk person.”). Begreppen ”avancerad elektronisk signatur” och ”kvalificerad elektronisk signatur” uppställer emellertid rekvisitet ”undertecknare”, vilket måste vara en fysisk person (LKES § 2:3-4 tillsammans med § 2:5).

Det framgår emellertid att under vissa omständigheter (se avsnitt 2.1.3.1, ”Rättslig effekt”), om övriga rekvisit är uppfyllda, det vill säga en tillräcklig hög säkerhetsnivå är uppfyllt (se och jfr LKES § 2:3 a-d), kan en ”elektronisk signatur” ha samma rättsliga verkan som en ”avancerad elektronisk signatur” eller ”kvalificerad elektronisk signatur”. Ett liknande resonemang fördes i förarbetet avseende certifikatutfärdare; en certifikatutfärdare [juridisk person] kan signera sitt certifikat med en elektronisk signatur som motsvarar säkerhetsnivån för ”avancerad elektronisk signatur” eftersom det skulle uppfylla ändamålet med kraven som uppställs i DES (prop. 1999/2000:117 s. 42:7-43:1; jfr LKES § 6:1 p. 8, där det uttryckligen anges).

Medan en ”undertecknare” inte kan vara en juridisk person så kan en utställare signera en elektronisk signatur som kan likställas med en avancerad eller kvalificerad elektronisk signatur.

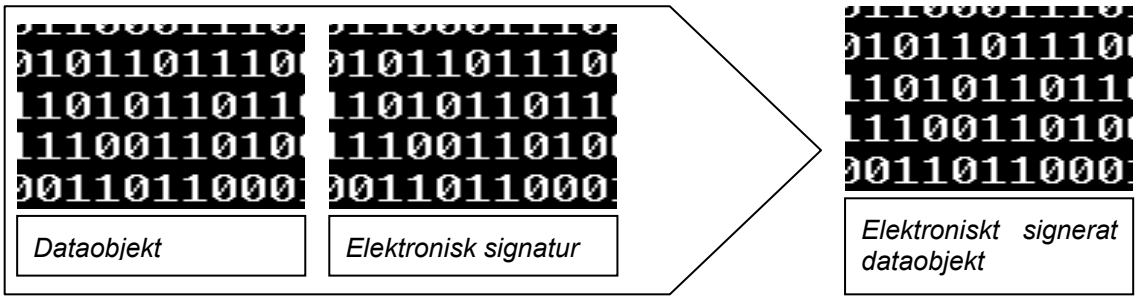
[4] I kommunikation med eller mellan myndigheter.

2.2. Elektroniskt signerat dataobjekt

En elektronisk signatur **1(2)** hänvisar till en ”digital konstellation” [ett dataobjekt], **2(2)** och sammanbinder referensen till objektet med ett ”subjekt” [utställaren[5]]. En elektronisk signatur utgörs således av två logiska, och tekniskt separata, led för att identifiera data och utställaren men vars resultat blir en komponent: den elektroniska signaturen.

Det dataobjekt som den elektroniska signaturen hänvisar till utgör en annan, logisk och teknisk separat, komponent, och tillsammans med den elektroniska signaturen utgör dessa komponenter ett dataobjekt som är elektroniskt signerat.[6]

Uttrycket dataobjekt är särskilt konstruerat för denna framställning. ”Dataobjekt” är en ”abstrakt samlingsbegrepp” och kan exempelvis åsyfta en ”handling”, ”dokument”, ”bild”, eller enstaka uppgifter. Vanliga abstrakta uttryck är annars, exempelvis, ”elektronisk handling”, ”elektronisk dokument” eller ”elektronisk urkund” (Statskontoret 2003:13, s. 7:4, 10:1), vilka kan jämföras med LKES § 2:2 ”elektronisk data”.

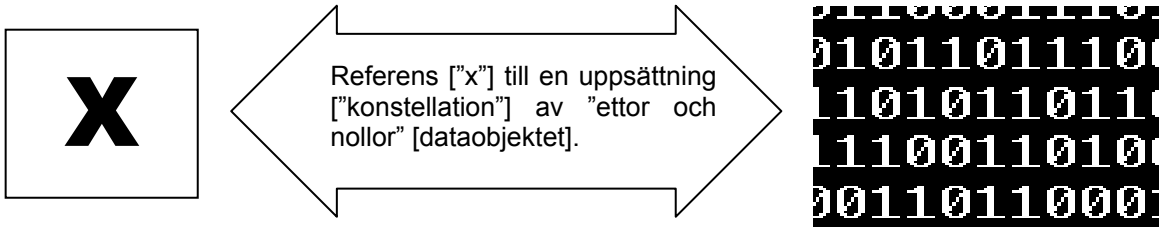


[5] Se LKES § 2:5, ”fysisk person som behörigen innehar en anordning för signaturframställning”, jfr ”utställare i LKES § 2:2, vilket kan vara fysisk såväl som juridisk person (prop. 1999/2000:117 s. 39:3; se vidare a. 2.1.3.2, ”Fråga om undertecknaren kan vara en juridisk person”).

[6] Se LKES § 2:2, ”elektronisk signatur: data i elektronisk form som är fogade till eller logiskt knutna till andra elektroniska data och som används för att kontrollera att innehållet härrör från den som framstår som utställare och att det inte har förvanskats”

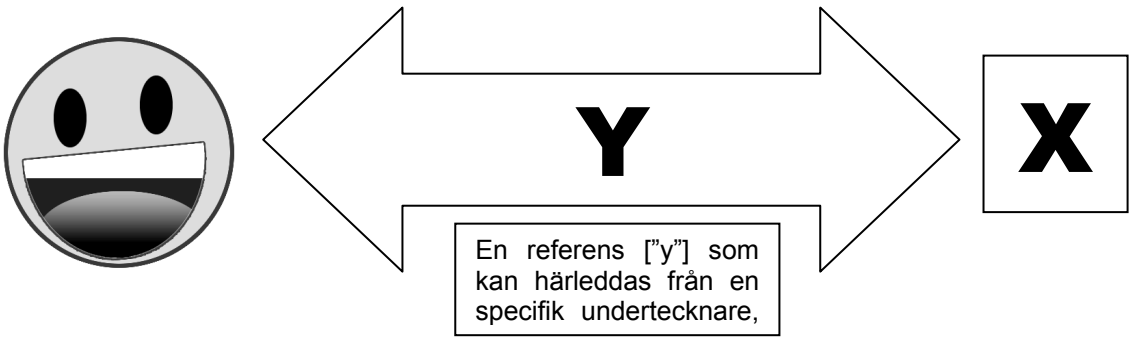
2.3. Elektronisk signering

2.3.1. Dataobjektets identifikation



Referensen “x” identifierar dataobjektet och skapas med hjälp av en *metod*. Metoden ska säkerställa att referensen är unik för uppsättningen av ettor och nollor, och att alltid samma referens ges för samma uppsättning av ettor och nollor.

2.3.2. Utställaren



Referensen ”y” skapas med hjälp av en *metod*. Metoden ska säkerställa att referensen är unik för ”x” och att bara utställaren kan ha skapat referensen, det vill säga, utställaren har ”refererat” till dataobjektet och därigenom ”godkänt” dataobjektets innehåll. Referensen ”y” kan kallas för själva ”signaturen”.

2.3.3. Signering

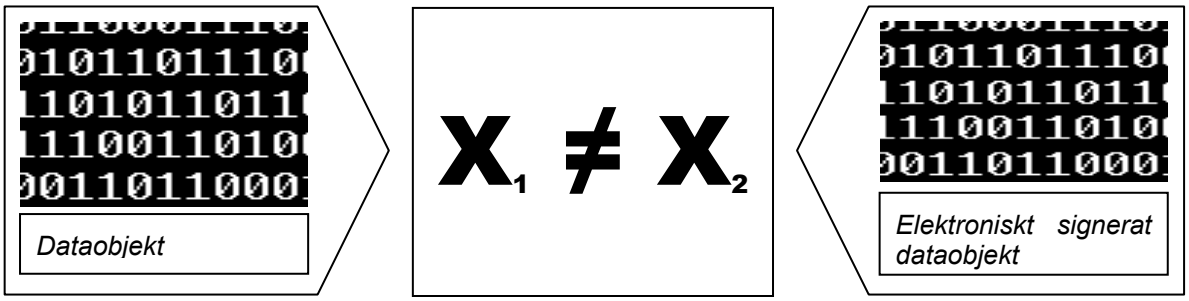
Signering av en elektronisk signerat dataobjekt innebär att:

1. en metod väljs och tillämpas för att generera referensen [x] till dataobjektet,
2. en metod väljs och tillämpas för att generera signaturen [y].

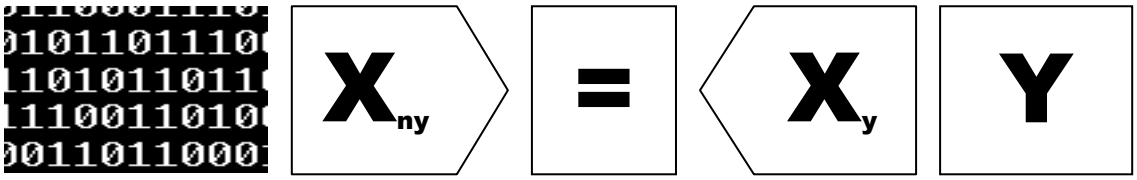
Den elektroniska signeringen kan sedan sammankopplas med dataobjektet med resultat av ett nytt dataobjekt vars innehåll utgörs av den elektroniska signaturen och dataobjektet; ett elektroniskt signerat dataobjekt.

När en elektronisk signatur sammankopplas med dataobjektet representerar dessa två ett ”nytt” dataobjekt. Det nya dataobjektet kan komma att ha en egen, unik, referens [x_2] som

inte överensstämmer med original-dataobjektets referens [x $_1$] som signerats. Detta har dock att göra med data objektets ”format” och hur den hanterar bifogade digitala objekt, såsom elektroniska signaturer.[7]



2.3.4. Verifiering



Verifiering av en elektronisk signerat dataobjekt innebär att:

1. en ny referens skapas till dataobjektet [x $_{ny}$] genom att tillämpa samma metod som användes av utställaren för att skapa sin referens [x $_y$],
2. en jämförelse görs mellan den nya referensen [x $_{ny}$] och den signerade referensen [x $_y$],
3. om referenserna är ekvivalenta är dataobjektet samma objekt som signerades, annars är dataobjektets innehåll inte detsamma som det dataobjekt som utställaren signerade.

Det framgår av processen att tillgång till dataobjektet är nödvändigt i syfte att utföra verifieringen.

2.4. Elektronisk stämpel

Begreppet ”stämpel” har observerats användas i två skilda sammanhang.

[7] Se exempelvis sr_003232v010101p, ESI; PAdES; Printable Representations of Electronic Signatures, a. 4.3 jfr 4.4.

I det ena fallet åsyftar ”stämpel”, i princip, en synonym för ”signatur” eller ”underskrift”, men istället för att vara knuten till en specifik fysisk person så är utställaren en juridisk person, exempelvis en myndighet.[8]

I det andra fallet åsyftar ”stämpel” en form av integritetskontroll av ett dataobjekt, vanligtvis en ”tidstämpel”. En tidstämpel intygar att ett dataobjekt existerade vid en viss tidpunkt genom att signera ”referensen” till dataobjektet tillsammans med information om tidpunkten av signeringen [stämplingen] (SOU 2010:104 b. 17 s. 307 och a. 13; Statskontorets rapport 2003:13 s. 45, a. 6.2; sr_003232v010101p, ESI; PAdES; Printable Representations of Electronic Signatures, a. 4.5).

[8] Vägledning från e-delegationen, ”Elektroniska original, kopior och avskrifter” (2012-06-07), a. 1.2, 1.3, 2.3.5. ”(Elektronisk) stämpel”, RSV M 2003:24, ”Avancerad elektronisk stämpel e-stämpel: Ett elektroniskt bevis, som motsvarar en elektronisk underskrift och intygar vilken organisation som har ställt ut handlingen”. Jfr Statskontorets rapport 2003:13 s. 55. Jfr Prop. 1999/2000:117 s. 38.

3. Teknik

Detta avsnitt beskriver den teknik som tillämpas [2013] för att framställa och verifiera ett elektroniskt signerat dataobjekt. Denna process redovisas från tre perspektiv:

- de funktioner i ett program som verkställer och verifierar ett elektroniskt signerat dataobjekt.
- de tekniska processer som skapar och verifierar ”signaturen”.
- den elektronisk signerade dataobjektets sammanställning, det vill säga, hur komponenterna, och dess beståndsdelar hanteras och lagras; format.

3.1. Program

Ett program för att framställa och verifiera elektroniska signaturer och avancerade elektroniska signaturer betecknas juridiskt som ”anordning för signaturframställning” i LKES (§ 2:7).

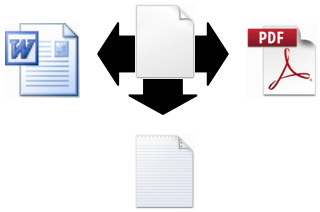
Ett program för att framställa och verifiera kvalificerade elektroniska signaturer betecknas som ”säker anordning för signaturframställning” i LKES (§ 2:8). Anordningen anses ”säker” om den uppfyller vissa, i LKES § 3, angivna krav för signaturframställning (jfr dock Kommissionens Beslut (2009/767/EG) av den 16 oktober 2009, artikel 1, vilket medger undantag till att säkra anordningar ska användas för kvalificerade elektroniska signaturer för tjänster inom den inre marknaden under vissa omständigheter (beslutet är reviderat genom beslut 2010/425/EU den 28 juli 2010 utan att förändra artikel 1.1); SOU 2010:104 a. 4.1).

Ett ”säkert” program ska säkerställa att signaturframställningsdata får ett tillfredställande skydd mot förfalskning och obehörig åtkomst, är unik, och ”inte kan härledas” (jfr prop. 1999/2000:117 s. 70, ”smarta kort” som praktiskt exempel). Vidare ska anordningen inte förändra data som ska signeras av eller förhindra presentation av data för undertecknaren. Att signaturframställningsdata ”inte kan härledas” torde åsyfta att, exempelvis, det inte ska vara möjligt att deduktivt, med hjälp av annan information, möjligtvis den ”offentliga nyckeln”, beräkna den hemliga nyckeln (jfr Prop. 1999/2000:117 a. 6.8 som inte berör frågan).

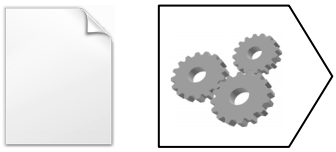
För avancerade och kvalificerade elektroniska signaturer ska den elektroniska signaturen vara skapad med ”hjälpmedel” [den hemliga nyckeln] som endast undertecknaren kontrollerar (LKES § 2:3:c). Fråga om ”kontroll” omfattar fysisk eller logisk kontroll (SOU 2010:104 s. 72:2, gällande rätt utesluter inte en logisk kontroll över hjälpmedlet; s.ä. a. 4.1.1, Förvaringsskyldighet,).

3.2. Signering och verifiering

3.2.1. Signering



”Dataobjektet”, i detta fall en sedvanlig ”fil” som exempelvis kan vara ett PDF-dokument, MS-Word-dokument eller en ”vanlig” textfil.



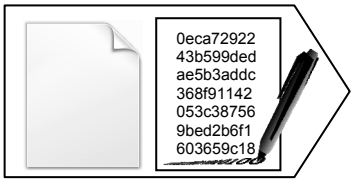
b60bb3c08a545c11f
f60e117c2f9e43e19
6454c603ba1abe4b
75ebf750688435

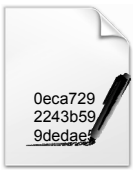
Dokumentets hashvärde beräknas med en hashfunktion. I detta exempel har algoritmen SHA-256 använts för att generera hashvärdet ”b60bb3c08a545c11ff60e117c2f9e43e196 454c-603ba1abe4b75ebf750688435” av textsträngen ”Dataobjekt exempel”.

b60bb3c08a545c1
1ff60e117c2f9e43
e196454c603ba1a
be4b75ebf750688
435

0eca7292243b599dedae5
b3addc368f91142053c387
569bed2b6f1603659c187
a05244114c24c506889e5
dc3a854d7c2330366d1f4d
f5acf569…

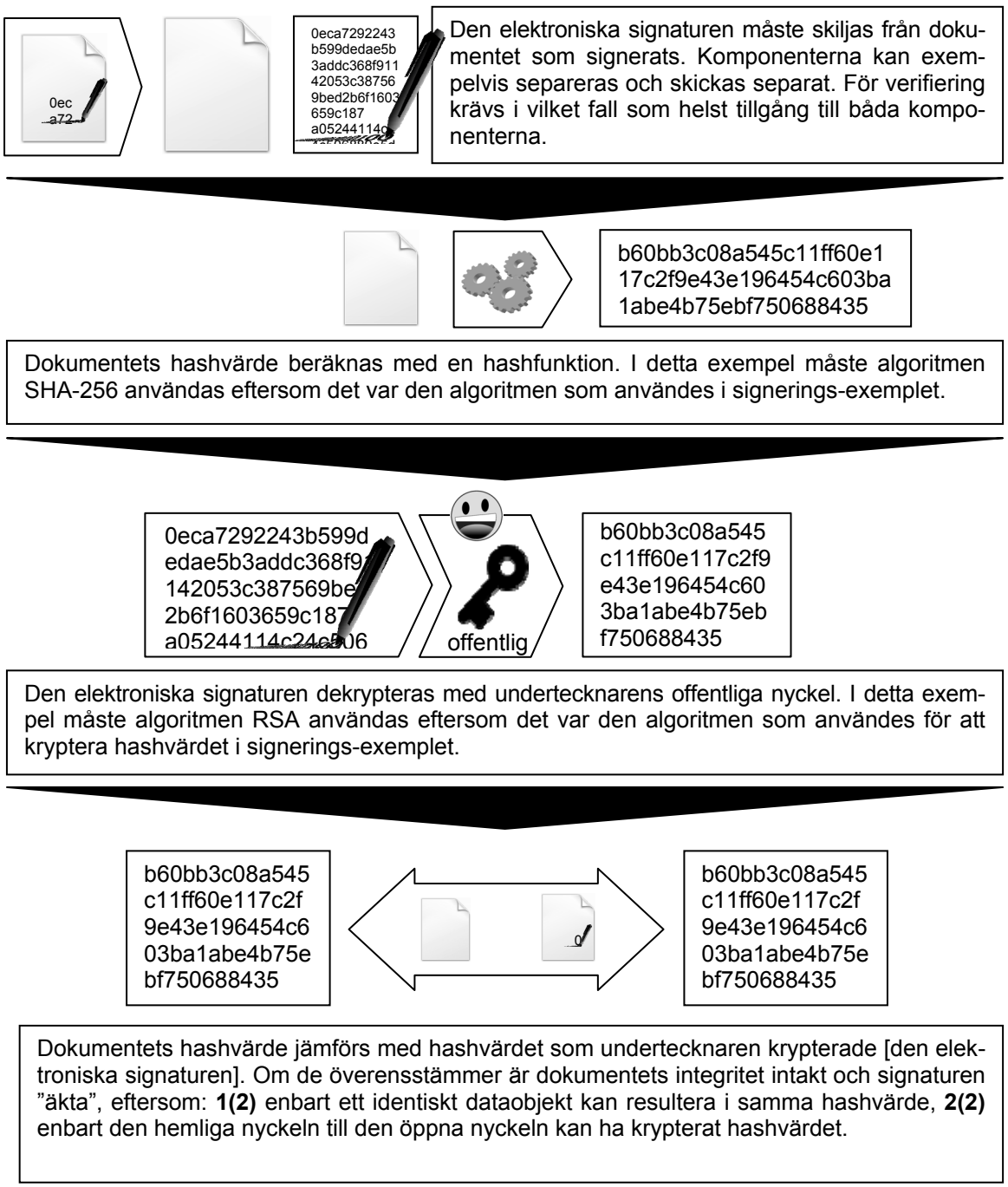
Dokumentets hashvärde krypteras med undertecknarens hemliga nyckel. I detta exempel har algoritmen RSA använts för att kryptera hashvärdet. Den krypterade hashvärdet är den elektroniska signaturen, d.v.s., ”0eca7292243b…”.





Dokumentet tillsammans med den elektroniska signaturen utgör ett elektroniskt signerat dokument. Hur komponenterna lagras beror på dokumentformatet.

3.2.2. Verifiering



Den elektroniska signaturen måste skiljas från dokumentet som signerats. Komponenterna kan exempelvis separeras och skickas separat. För verifiering krävs i vilket fall som helst tillgång till båda komponenterna.

Dokumentets hashvärde beräknas med en hashfunktion. I detta exempel måste algoritmen SHA-256 användas eftersom det var den algoritmen som användes i signerings-exemplet.

Den elektroniska signaturen dekrypteras med undertecknarens offentliga nyckel. I detta exempel måste algoritmen RSA användas eftersom det var den algoritmen som användes för att kryptera hashvärdet i signerings-exemplet.

Dokumentets hashvärde jämförs med hashvärdet som undertecknaren krypterade [den elektroniska signaturen]. Om de överensstämmer är dokumentets integritet intakt och signaturen ”äkta”, eftersom: **1(2)** enbart ett identiskt dataobjekt kan resultera i samma hashvärde, **2(2)** enbart den hemliga nyckeln till den öppna nyckeln kan ha krypterat hashvärdet.

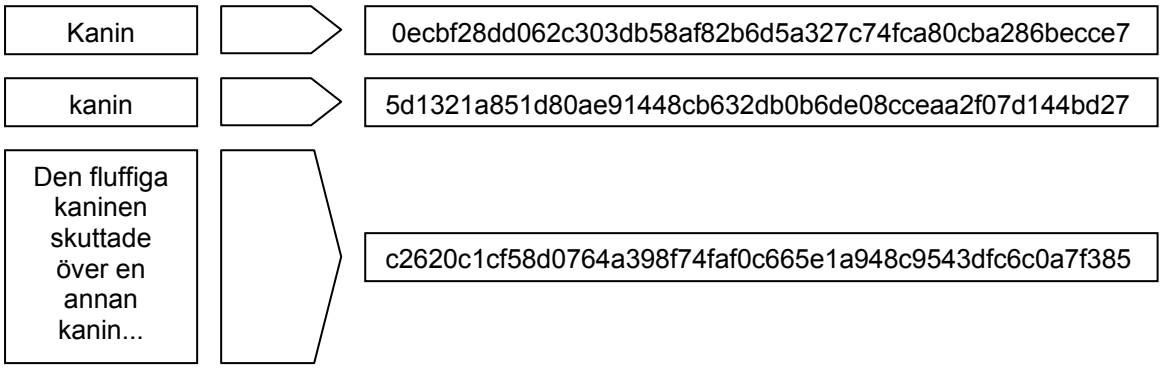
3.2.3. Hashfunktionen

En hashfunktion eller hashalgoritm skapar en referens till ett dataobjekt. Referensen ska

- vara lätt att beräkna (inte processorintensivt),
- unik för dataobjektet, det vill säga dataobjektet och varje *exakt kopia* av dataobjektet, men aldrig i något annat fall, ska alltid få samma referens,[9]
- aldrig möjliggöra att dataobjektet kan återskapas med hjälp av själva referensen [envägsfunktion, det vill säga, hashfunktionen kan bara ”koda” men inte ”avkoda”], samt
- aldrig skapa samma referens för två *olika* dataobjekt [kollisionsresistans].

”Referensen” kan, bland annat, kallas: checksumma, fingeravtryck, hashsumma, hashvärde, kondensat, kontrollsumma.[10] Den korrekta terminologin är emellertid ”kondensat” eller en variation av ”hash” (Wikipedia ”Hash funktion” och ”Hash function”; se också Wikipedia ”Cryptographic hash function”, kryptografiska hashfunktioner används för att utföra ”checksummor”/”kontrollsummor” och ”fingeravtryck” och därav användningen av termerna som synonymer även om tekniskt inkorrekt; jfr Digital Signatures [2002], s. 88).

Hashvärdet skapas utifrån dataobjektet, och kan ses som en komprimerad mängd eller längd av dataobjektet. Värdet kan variera beroende på hashfunktionen, men är alltid samma värde för samtliga referenser skapade med samma hashfunktion.



SHA-256 hashalgoritmen genererar en hashvärde på 256 bitar, vilket motsvarar en textsträng med 64 symboler. Notera skillnaden mellan ”**K**anin” och ”**k**anin”, samt att textlängden i tredje exemplet inte påverkar hashvärdets längd.

3.2.4. Krypteringen och dekryptering

Kryptering innebär att information förändras från att tolkas med en viss mening till en annan, vanligtvis helt orelaterad och förvrängd bortom all igenkännlighet, mening. Dekryptering innebär att information återställs till sin ursprungliga mening.

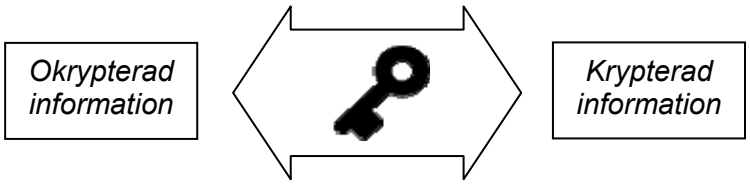
[9] ”Lavin effekt”, små förändringar av information medför att man får ett helt annat värde (Statskontorets rapport 2003:13 s. 23).
[10] Engelska, exempelvis, hash code, hash sum, hash value, checksum.

Begreppsapparaten för metoden är att man krypterar och dekrypterar informationen med hjälp av symetriska eller asymmetriska ”nycklar”.

Det ska särskild noteras att endast signeringen berörs av krypteringsprocessen, och det signerade dataobjektet, ”innehållet”, inte på något sätt krypteras. En kryptering av dataobjektet är emellertid möjligt, och har en liknande krypteringsprocess.

3.2.4.1. Symmetrisk

Symmetrisk kryptering innebär att man använder samma nyckel för kryptering och dekryptering. ”Nyckeln”, som består av ”ettor och nollor”, kan kopieras i flertal exemplar.



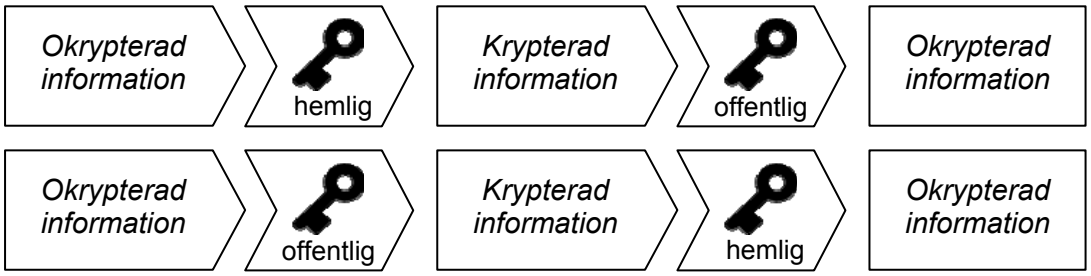
Symmetrisk kryptering är beprövad och snabb. Hanteringen av nyckeln kan emellertid skapa svårigheter i att säkerställa att rätt person får ett exemplar (Ds 1998:14 s. 19:1).

3.2.4.2. Asymmetrisk

Asymmetrisk kryptering innebär att man använder två olika nycklar för kryptering och dekryptering: en ”hemlig” (alternativt ”privat”; engelska ”private”),[11] eller ”signaturframställningsdata” (LKES § 2:6, prop. 1999/2000:117 s. 70), och en ”offentlig” (alternativt ”publik” eller ”öppen”; engelska ”public”) (Ds 1998:14 s. 19:3), eller signaturverifieringsdata (LKES § 2:9, prop. 1999/2000:117 s. 70).

”Nycklarna”, som består av ”ettor och nollor”, kan kopieras i flertal exemplar. Medan den offentliga nyckeln kan distribueras fritt, och tillåtas kopieras av vem som helst, ska den ”hemliga” nyckeln, som namnet antyder, hållas hemligt.

[11] Benämningen ”hemlig” används här i enlighet med prop. 1999/2000:117 s. 40:2.



Nycklarna kompletterar varandra i en riktning; krypterad information med en nyckel kan inte dekrypteras med samma nyckel.

Asymmetrisk kryptering möjliggör att någon med tillgång till den offentliga nyckeln kan säkerställa att information härrör från en specifik utfärdare, eller ”hemlig nyckel” associerad med utfärdaren.

Tekniken möjliggörs med hjälp av komplexa algoritmer, vilket kräver mycket processkraft, och att det inte ska vara möjligt att härledda den ena nyckeln med hjälp av den andra nyckeln (Ds 1998:14 s. 19:1, 20:6; Prop. 1999/2000:117 a. 4.3.1 Kryptografisk teknik med hemliga och öppna nycklar, jfr LKES § 3 p. 2.).

3.2.4.3. Kryptering

Exempel på ett hashvärde, ”indata”, som krypterats; ”utdata”.

Indata	**Utdata**
0ecbf28dd062c303db58af82b6d5a327c74fca80cba286becce7a222d555b954	2bbeda948252666d2e667e0b26dfee5d2f548a08315186a45308c9027eb3a60dfe899b4261342724b4e04794fcee5f1a09d1c7c922f46954d62a62faa06cdb1b8b14319762bc59a468d3b86ab9029cbb071058dea9be13d3e5615356b5ad88d4d8b3a390cc84a03a555a4ab8236109caa6636bb9262ecd53320b47ecfc94a2e5f453a44707ced510f4ee4cbea2cf4e987a8bbb2ce62ac0a4775edc4a599cc23c78fd0ee8fa809b346c7e829e05122bcb2a9a52904fda69ceef666314f0940c0e3592c19940ef5f9e5c663b24b2f65bc3d27a555a152ea3d57adf475da60be0b3ae874465bff455611c2bdd8740bfdc1659211bb4176d53449b524cbfd881d897

Notera att kryptera samma indata igen inte resulterar i samma utdata som första krypteringen.

Indata	**Utdata**
0ecbf28dd062c303db58af82b6d5a327c74fca80cba286becce7a222d555b954	2584b77474181cd369c6d5808b1d3c565ed75c547a2a54a7cd6fbfc168816e47bdea19c9a8fd1b556346e698603e46c220e18972376771b862ef44877d0fa5247cc90949c90d7129de0571c0e1198ef22f077cc341f591230b23a1201686cae5b669a565eff4203464d1761c8213c32abd6c7633cd0a33f99f08128df546e07a2fe9bcadd9ee5a3578db3d9ddea08ceee229be6954e9c03a3412ba638521bd6753945eff176e89c4f40680100a01125b58a0c39c56547f8aa35cf3bd0100bf94177de64f5a287629841f4d356e363287fbbc89f927842bfbe3e3d2b19a972157fbd39f66fbea5db7857fa2cb64125a8b0f98c4aa936060a4f29f3bcd7ca30272

3.2.4.4. Dekryptering

Exempel på krypterad data, ”indata”, som dekrypterats; ”utdata”.

Indata	Utdata
2bbeda948252666d2e667e0b26dfee5d2f548a08315186a45308c9027eb3a60dfe899b4261342724b4e0479 4fcee5f1a09d1c7c922f46954d62a62faa06cdb1b8b14319762bc59a468d3b86ab9029cbb071058dea9be13d 3e5615356b5ad88d4d8b3a390cc84a03a555a4ab8236109caa6636bb9262ecd53320b47ecfc94a2e5f453a4 4707ced510f4ee4cbea2cf4e987a8bbb2ce62ac0a4775edc4a599cc23c78fd0ee8fa809b346c7e829e05122b cb2a9a52904fda69ceef666314f0940c0e3592c19940ef5f9e5c663b24b2f65bc3d27a555a152ea3d57adf475 da60be0b3ae874465bff455611c2bdd8740bfdc1659211bb4176d53449b524cbfd881d897	0ecbf28dd062c3 03db58af82b6d5 a327c74fca80cb a286becce7a22 2d555b954

Indata	Utdata
2584b77474181cd369c6d5808b1d3c565ed75c547a2a54a7cd6fbfc168816e47bdea19c9a8fd1b556346e69 8603e46c220e18972376771b862ef44877d0fa5247cc90949c90d7129de0571c0e1198ef22f077cc341f5912 30b23a1201686cae5b669a565eff4203464d1761c8213c32abd6c7633cd0a33f99f08128df546e07a2fe9bcad d9ee5a3578db3d9ddea08ceee229be6954e9c03a3412ba638521bd6753945eff176e89c4f40680100a01125 b58a0c39c56547f8aa35cf3bd0100bf94177de64f5a287629841f4d356e363287fbbc89f927842bfbe3e3d2b19 a972157fbd39f66fbea5db7857fa2cb64125a8b0f98c4aa936060a4f29f3bcd7ca30272	0ecbf28dd062c3 03db58af82b6d5 a327c74fca80cb a286becce7a22 2d555b954

3.3. Format

Avsnittet är begränsat till standarder från ETSI (”European Telecommunications Standards Institute”) eftersom dessa är: **(1)** särskild konstruerade för att bevara elektroniska signaturer under lång tid, och **(2)** förenliga med EU-rätten.

Format för en elektronisk signatur kan vara konstruerad på olika sätt. Generellt kan man särskilja tre komponenter: innehållet, signaturen och behållaren. Konstruktionen mellan dessa tre komponenter kan variera, men förenklat så finns det två typer av ”format”. En komponent kan vara ett ”huvudformat” som omsluter en eller flera komponenter som ”delmängdsformat”, eller så har varje komponent sin egen format oberoende av de andra komponenternas format.

I det första fallet kan formatet för behållaren omfatta innehållet och/eller signaturen, medan i det andra fallet kan innehållet och/eller signaturen ha ”egna format” och behållaren kan omsluta dem [andra format] antingen som ”de är” (accepterar alla typer av format) eller endast om innehållet och/eller signaturen är i en särskild format (men fortfarande avskild från behållarens format).

3.3.1.1. Innehåll

Innehållet [som signeras, det vill säga, ett hashvärde ska skapas från] kan exempelvis bestå av enbart ”text” eller en ”bild”, men även en mer komplex format, såsom ”MS Word Doc”, ”OpenOffice Doc”, ”PDF”. Vad som omfattas av innehållet kan variera beroende på formatet för innehållet eller behållaren. Innehållet kan exempelvis vara enbart viss ”text”, men också metadata, metastruktur och/eller annan struktur (jfr Statskontorets rapport 2003:13 s. 32).

3.3.1.2. Signatur

Formaten för signaturen omfattar det krypterade hashvärdet av innehållet, samt de komponenter som krävs för att signaturen ska vara giltig, exempelvis valideringsdata.

3.3.1.3. Behållare

Behållaren är det format som sammansätter innehållet och signaturen, vilket kan exempelvis vara i ”MS Word Doc”, ”OpenOffice Doc”, ”PDF”, ”OpenPGP Format” eller ”S/MIME”.

3.3.2. CAdES (CMS Advanced Electronic Signatures)

3.3.2.1. Funktion

CAdES är en standard upprättat genom ett europeiskt initiativ att standardisera elektroniska signaturer[12] i syfte att få produkter och lösningar för elektroniska signaturer att överensstämma med DES (ETSI TS 101 733 V2.2.1 (2013-04), b. G, a. G.1).

CAdES definierar format för elektroniska signaturer samt deras validering. Utmärkande är att CAdES särskilt beaktar behovet att validera signaturer för en längre tid, såväl ”långtidsgiltighet” som ”arkivering”. CAdES utgår från PKI och bygger vidare på bland annat RFC 3852 ”Cryptographic Message Syntax (CMS)”.[13]

3.3.2.2. Historik

Det första dokumentet, version 1.1.3 (maj 2000), publicerades som ETSI ES 201 733. Det andra dokumentet, version 1.2.2 (december 2000), och efterföljande versioner fram tills denna framställning (hösten 2013), publicerades som ETSI TS 101 733, där den senaste versionen är 2.2.1 (april 2013).[14] Fram tills version 2.2.1 behandlade dokumenten såväl format som policy för signaturer, men frågor om policy är numera definierade i TR 102 272, med undantag för policyn som berör ”teknisk konsistens” (”technical consistency”) vid validering av elektroniska signaturer.

Version 1.2.2, fick en IETF motsvarighet i form av informativ RFC 3126 (september 2001), ”Electronic Signature Formats for long term electronic signatures”, och kan ses som ett tillägg till RFC 2630 och RFC 2634. RFC 3126 ersattes senare av informativ RFC 5126 (februari 2008), ”CMS Advanced Electronic Signatures (CAdES)”, och är en transposition av, och ekvivalent till, ETSI TS 101 733 version 1.7.4, och formatet kan ses som ett tillägg till RFC 3852 och RFC 2634.

3.3.2.3. Grundläggande format

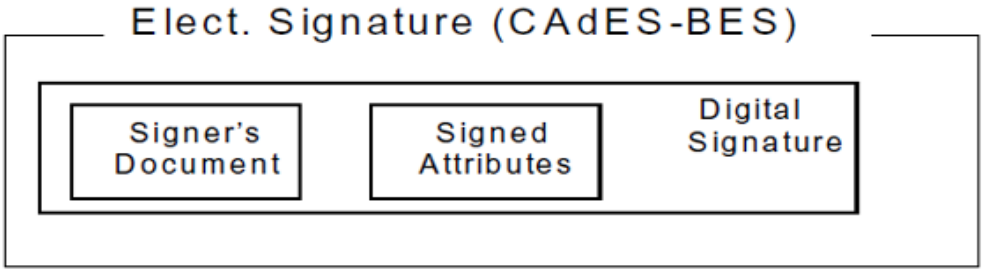
ETSI TS 101 733 V2.2.1 (2013-04) a. 4.3 Figurer i detta avsnitt är direkt hämtade från ETSI TS 101 733 V2.2.1 (2013-04) a. 4.3

CAdES är en kumulativ format, det vill säga, de olika variationerna av CAdES bygger på varandra. Grundformatet för en CAdES måste antingen vara BES eller EPES.

[12] EESSI (European Electronic Signature Standardization Initiative).
[13] För en fullständig källa se ETSI TS 101 733 V2.2.1 (2013-04), a. 2.
[14] ETSI TS 101 733 V2.2.1 (2013-04), s. 113.

CAdES-BES (CAdES Basic Electronic Signature)

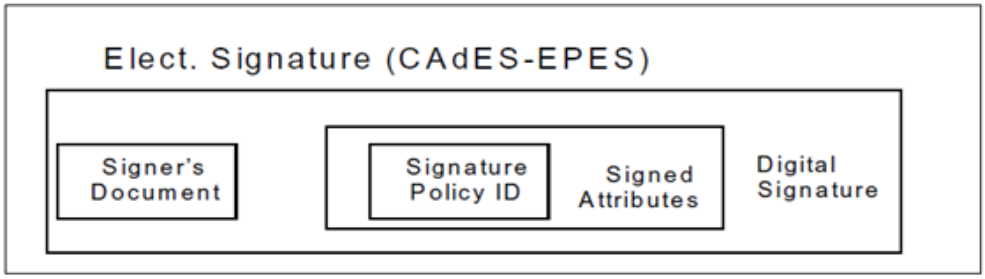
Det grundläggande formatet för CAdES måste innehålla **1(3)** det data som signerats, **2(3)** en uppsättning av obligatoriska attribut, **3(3)** samt den digitala signaturen som omsluter data och attributen. Formatet får eventuellt även innehålla en uppsättning av **(A)** signerade och **(B)** osignerade attribut. Samtliga 5 komponenter måste följa uppställda specifikationer i ETSI TS 101 733.



Formatet är det minsta som krävs för en elektronisk signatur, och uppfyller EU:s krav på ”elektroniska signaturer”, men har inte tillräckligt med information för att kunna valideras efter lång tid.

CAdES-EPES (CAdES Explicit Policy Electronic Signature)

CAdES-EPES utgår från BES och uppställer ytterligare ett obligatoriskt attribut; ett särskilt signerat attribut som anger en identifierare för den policy som ska tillämpas för att validera signaturen.



3.3.2.4. Utökade format eller format för valideringsdata

ETSI TS 101 733 V2.2.1 (2013-04) a. 4.4 Figurer i detta avsnitt är direkt hämtade från ETSI TS 101 733 V2.2.1 (2013-04) a. 4.4

I syfte att validera signaturer krävs valideringsdata, vilket består av:

- PKC (”Public Key Certificate” eller ”certifikat för publik nyckel”),
- återkallelsestatus för varje PKC,

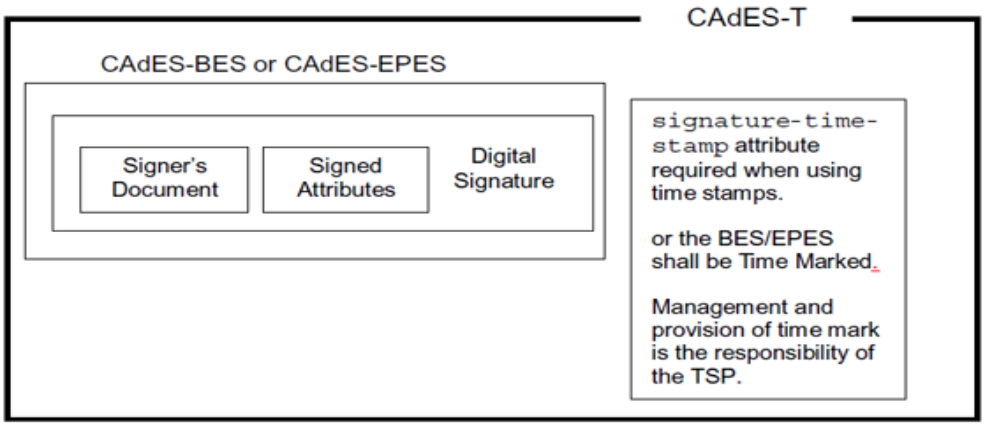
- Certifikatutfärdarens certifikat, samt dess CRL eller OCSP (”Online Certificate Status Protocol”),
- antingen en tillförlitlig tidstämpel på signaturen, eller ett tidmärke (”time-mark”) i revisionshistoriken (”audit log”),
- när tillämpligt, detaljerna kring policyn för signaturen som ska användas för att validera signaturen.

Valideringsdata kan sammanställas av signatären och/eller verifieraren, och när tillämpligt, i enlighet med kraven i angiven policy.

CAdES uppställer fem kumulativa variationer av CAdES -formatet för att omsluta valideringsdata i CAdES-BES eller CAdES-EPES. Dessa variationer bygger på varandra enligt följande succession: CAdES-T, CAdES-C, en av CAdES-X -variationerna, CAdES-A, och CAdES-LT (nervärderat).

CAdES-T (CAdES with Time)

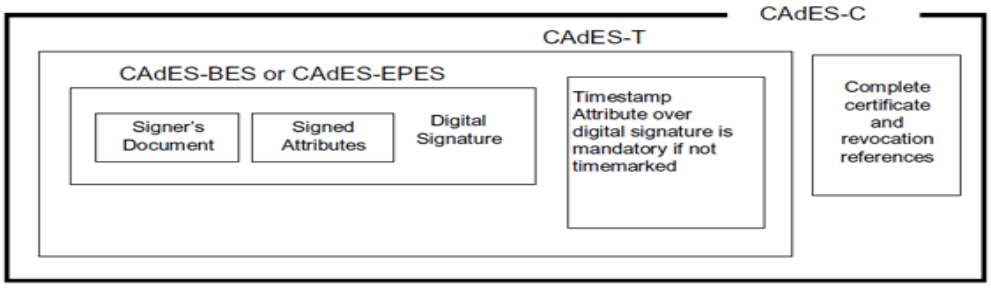
Det första tillägget till antingen CAdES-BES eller CAdES-EPES associerar en tillförlitlig tid till den elektroniska signaturen, vilket är det första steget till långtidsvalidering av elektroniska signaturer.



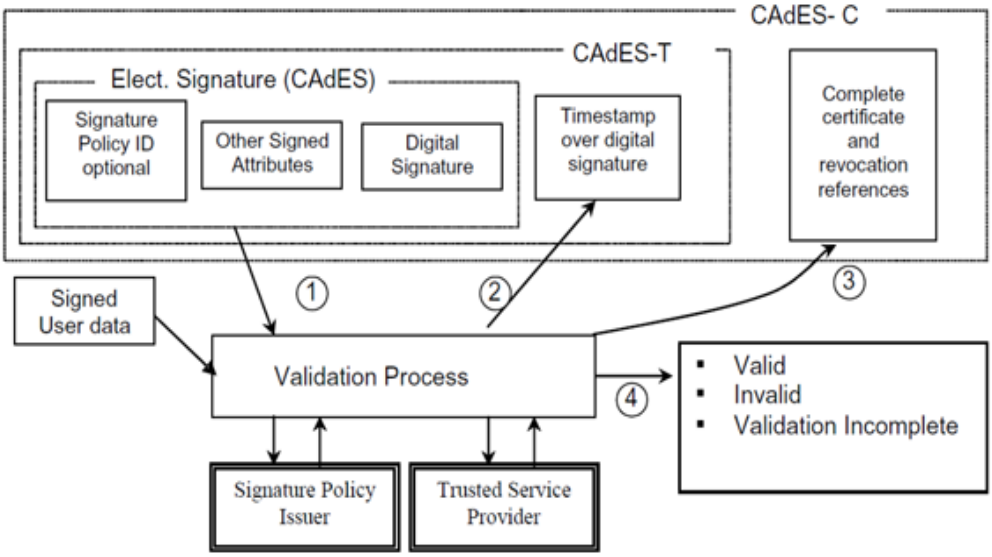
Den tillförlitliga tiden kan antingen anges som en tidstämpel i osignerat attribut, eller ett tidmärke, inte angiven i något attribut, utan hanterad av en betrodd tjänstetillhandahållare, med ansvar att vid behov tillhandahålla bevis på den tillförlitliga tiden.

CAdES-C (CAdES with Complete Validation Data References)

CAdES-C lägger till CAdES-T två osignerade attribut som anger hänvisningar till alla certifikat och CRL och/eller OCSP gensvar som används för att verifiera signaturen.[15] Bevarande av hänvisningar till information, istället för omslutning av information, möjliggör reducering av formats storlek.



Nedanstående exempel på hur komponenterna kan genereras visar att **(1)** efter att signering utförts (grundäggande CAdES) så kan man vid valideringsprocessen **(2)** tillägga en tidstämpel (CAdES-T), och även **(3)** fullständiga hänvisningar till certifikat och CRL och/eller OCSP gensvar (CAdES-C). Steg 2 och 3 kan göras av signatären såväl som verifieraren.

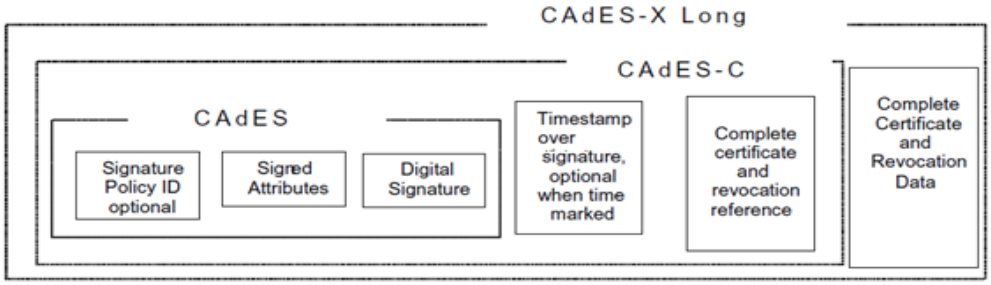


[15] Hashvärdet av data som det hänvisas till omsluts (ETSI TS 101 733 V2.2.1 (2013-04) b. C, a. C.4.4.1).

CAdES-X (Extended Electronic Signature Formats eller CAdES with EXtended Validation Data)[16]

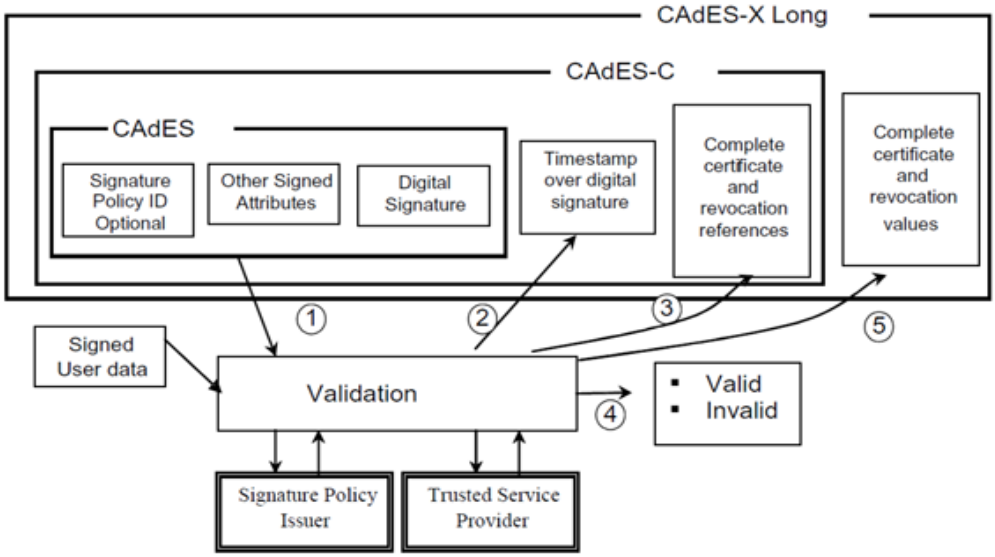
CAdES-X finns i ett antal variationer, vilka utökar CAdES-C, i syfte att möjliggöra verifikation efter en mycket lång tid, och förhindra vissa katastrofala situationer.[17]

Variation[18]	**Suffix**	**Funktion**
CAdES EXtended Long Electronic Signature	Long	Tillägger två attribut för att omsluta alla certifikat och CRL och/eller OCSP gensvar som används för att verifiera signaturen.
CAdES with Extended Long validation data		



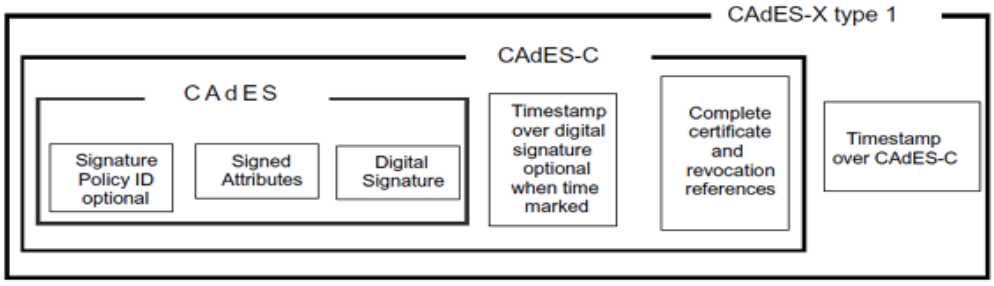
Nedanstående exempel bygger på CAdES-C och visar hur användaren eller verifieraren kan utöka signaturen till CAdES-X Long genom att **(5)** omsluta certifikat och CRL och/eller OCSP gensvar.

[16] Suffixen och deras förklaringar skiljer sig i a. 3.2 Abbreviations från a. 4 Overview.
[17] Verkar åsyfta att förhindra att någon kan använda ett falskt certifikat när nycklarna för en certifikatutfärdare äventyras (ETSI TS 101 733 V2.2.1 (2013-04) b. C, a. C.4).
[18] Suffixen och deras förklaringar skiljer sig i a. 3.2 Abbreviations från a. 4 Overview.

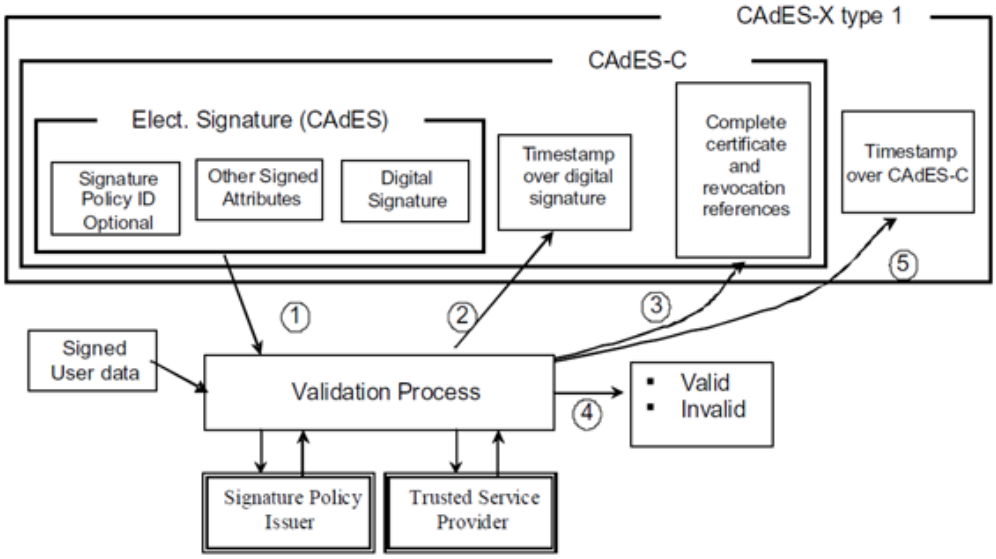


EXtended Electronic Signature with Time Type 1	Type 1	Tillägger ett attribut med värdet av en tidstämpel över hela CAdES-C.

CAdES-X Type 1 rekommenderas när man använder OSCP gensvar för att kontrollera ett certifikats tillstånd, samt ger en integritetsskydd över all data. Om valideringsdata omsluts, istället för att hänvisas till, så övergår CAdES-X Type 1 till CAdES-X Long Type 1 (ETSI TS 101 733 V2.2.1 (2013-04) b. C, a. C.4.4, C.4.4.1).

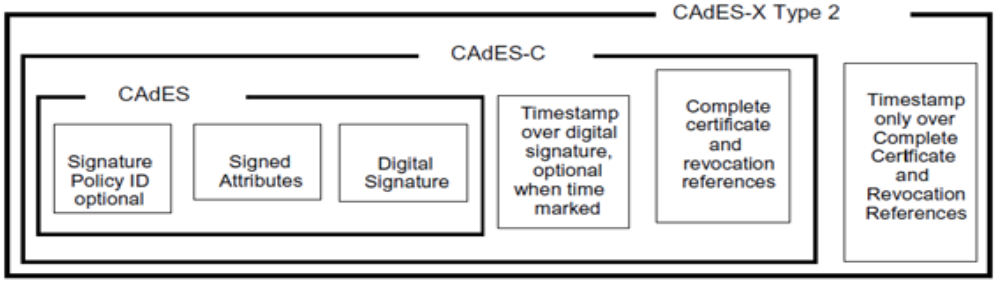


Nedanstående exempel bygger på CAdES-C och visar hur användaren eller verifieraren kan utöka signaturen till CAdES-X Type 1 genom att **(5)** tidstämpla CAdES-C.

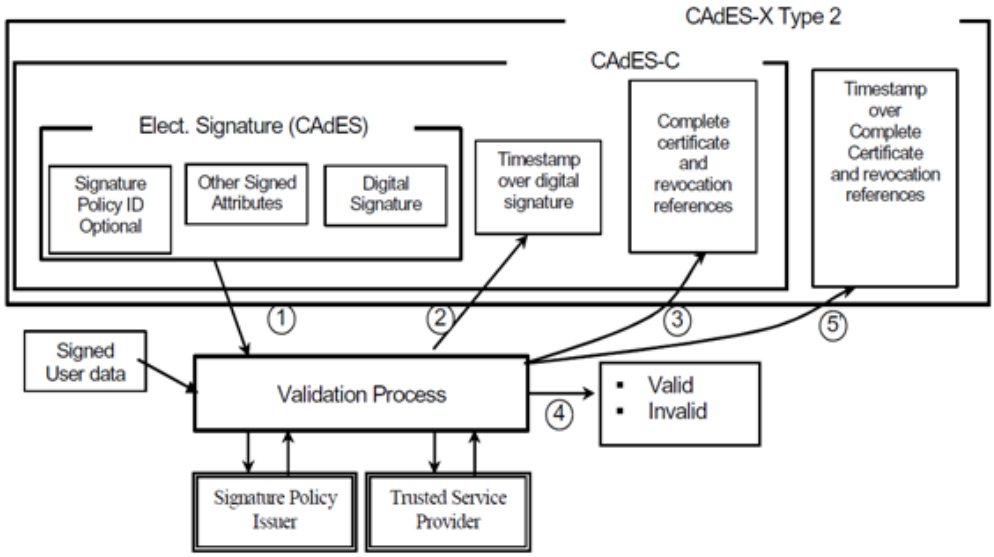


EXtended Electronic Signature with Time Type 2	Type 2	Tillägger ett attribut med värdet av en tidstämpel eller flera tidstämplar över alla hänvisningar till certifikat och CRL och/eller OCSP gensvar som används för att verifiera signaturen.

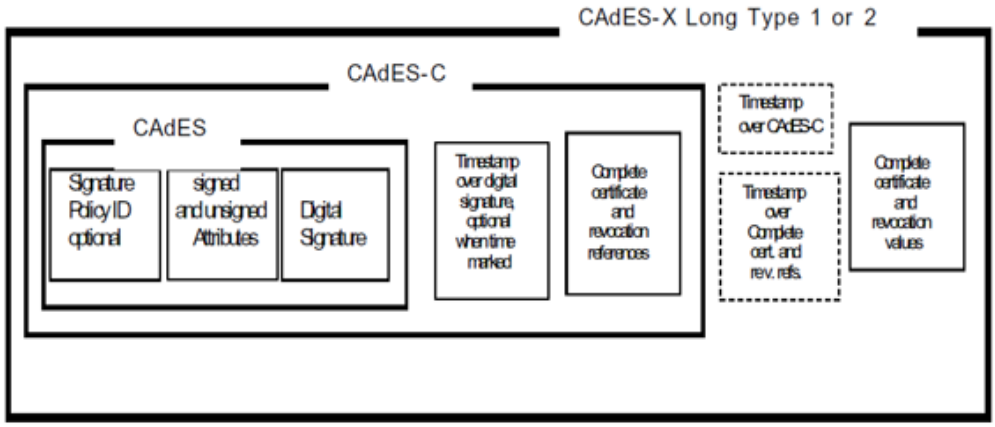
CAdES-X Type 2 rekommenderas när man använder CRL för att kontrollera ett certifikats tillstånd, eftersom det är möjligt att använda CRL i anslutning till andra signaturer som använder samma certifikatutfärdare och CRL (ETSI TS 101 733 V2.2.1 (2013-04) b. C, a. C.4.4, C.4.4.2).



Nedanstående exempel bygger på CAdES-C och visar hur användaren eller verifieraren kan utöka signaturen till CAdES-X Type 2 genom att **(5)** tidstämpla hänvisningarna till certifikat och CRL och/eller OCSP gensvar.



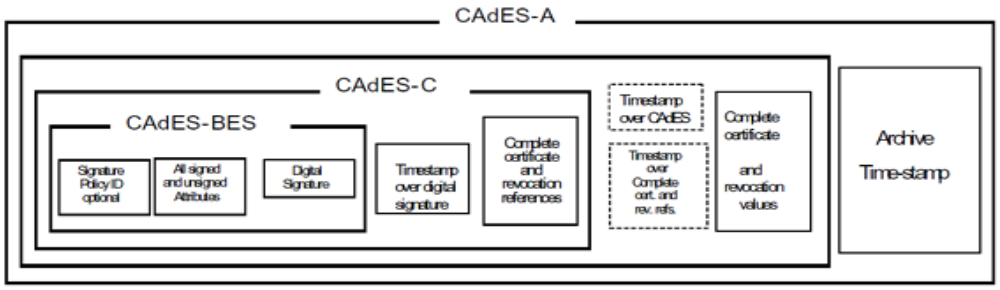
EXtended Long Electronic Signature with Time	Long Type 1 or 2	Är en kombination av ”Long” och antingen ”Type 1” eller ”Type 2”.



CAdES-A (CAdES with Archive validation data eller Archival Electronic Signature)[19]

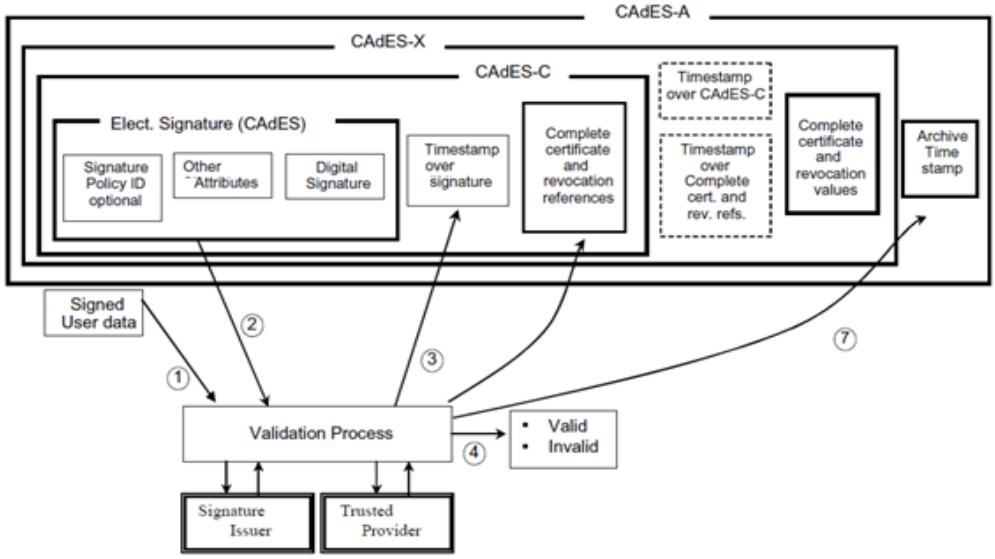
CAdES-A associerar en tidstämpel till en CAdES för att arkivera signaturer för lång tid. Successiva tidstämplar skyddar all material mot svaga hash algoritmer eller mot nedbrutna krypteringsmaterial eller -algoritmer.

Variation	**Funktion**
Archive-time-stamp (ATSv2) attribute	Tillägger ett eller flera attribut för tidstämplar över antingen CAdES-X Long eller CAdES-X Long Type 1 eller 2. ATSv2 ska inte längre användas och är endast beskriven för bakåtkompatibilitet. System kan verifiera signaturer skapade med ATSv2, och tillämpa ATSv3 för att utöka deras livslängd.

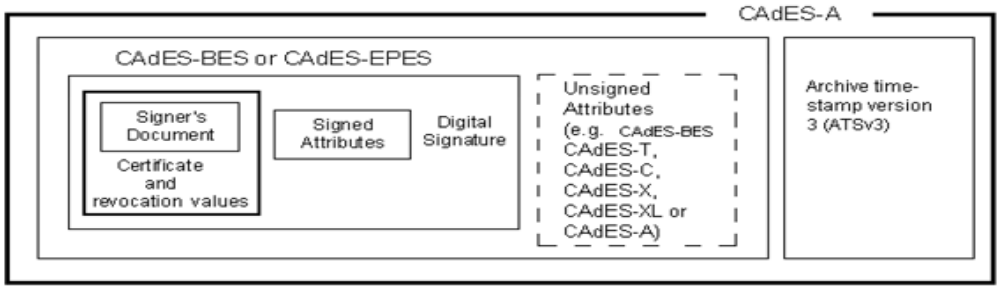


Nedanstående exempel visar hur användaren eller verifieraren kan utöka signaturen till CAdES-A genom att **(7)** tidstämpla CAdES-X.

[19] Suffixen och deras förklaringar skiljer sig i a. 3.2 Abbreviations från a. 4 Overview.



Archive-time-stamp (ATSv3) attribute	Tillägger ett eller flera attribut för tidstämplar för CAdES-BES, CAdES-EPES, CAdES-T, CAdES-C, CAdES-X, CAdES-XL eller CAdES-A.

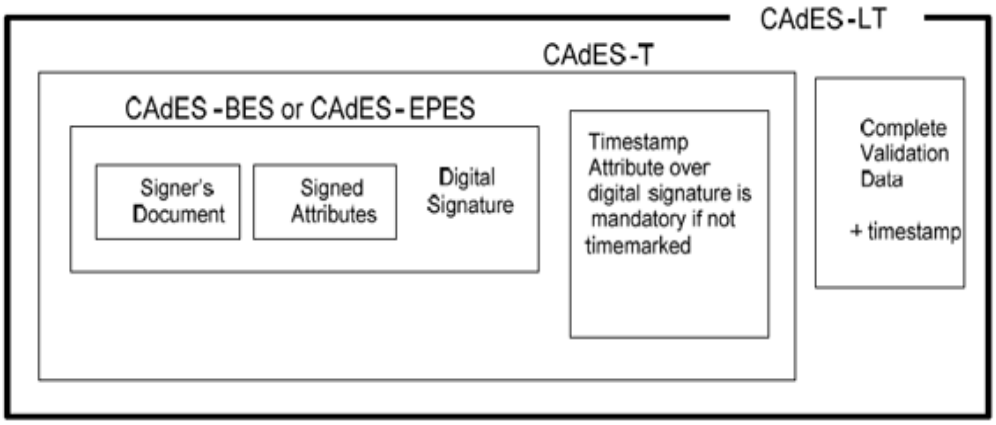


CAdES-LT (CAdES Long Term [Electronic Signature])

CAdES-LT kan bygga på CAdES-T, CAdES-C, CAdES-X Long, CAdES-X Long Type 1 or 2 eller en CAdES-A, och tillåter ett särskilt attribut för långtidsvalidering av signaturer, vilket i princip är snarlik CAdES-X Long och CAdES-A men är enklare att tillämpa och mer flexibel.[20] Successiva tidstämplar skyddar mot all material mot svaga hash algoritmer eller mot nedbrutna krypteringsmaterial eller -algoritmer.

Formatet är emellertid nervärderat [”deprecated”] för signaturer som redan inte har tillämpad ett sådant attribut för långtidsvalidering.

[20] Det finns ingen begränsning på den typ av information som attributen kan innehålla, exempelvis, certifikat eller CRL (ETSI TS 101 733 V2.2.1 (2013-04) b. B, a. B.3A).



3.3.3. CMS (Cryptographic Message Syntax)

3.3.3.1. Funktion

CMS beskriver en syntax för att digitalt signera, kondensera, autentisera eller kryptera arbiträr data i ett meddelande. Informationen behandlas i binär form.

3.3.3.2. Historik

CMS är IETF standard som bygger på PKCS #7. IETF utgav en informativ RFC (2315) om PKCS #7. CMS standardiserades i RFC 2630, ersatt av RFC 3369 (CMS) och 3370 (CMS algoritmer), ersatt av RFC 3852 (CMS), ersatt av RFC 5652 (CMS). RFC 3852 uppdateras genom RFC 4853 (multipla signatärer) och RFC 5083 (”Authenticated-Enveloped-Data” innehållstyp). RFC 3370 (CMS algoritmer) uppdaterades genom RFC 5754 (tillämpning av SHA2 i CMS).[21]

3.3.4. PAdES (PDF Advanced Electronic Signatures)

3.3.4.1. Funktion

PAdES är en standard som utökar PDF 1.7 (ISO 32000-1:2008), och däri angivna specifikationer för elektroniska signaturer, att möjliggöra elektroniska signaturer som är giltiga under lång tid och överensstämmer med DES.

PAdES bygger vidare på bland annat CAdES (TS 101 733) med vissa begränsningar,[22] och XAdES (TS 101 903) med vissa begränsningar[23] (ETSI TS 102 778-1 V1.1.1 (20009-07), a. ”Introduction” och a. 1).[24]

[21] http://tools.ietf.org/

[22] De utvecklade CAdES -formaten stöds inte.

3.3.4.2. Historik

ETSI TS 102 778-1

PAdES är uppdelad i fem delar: ETSI TS 102 778-n, där ”n” kan var 1 till 5 för respektive del. Den första delen är informativ, övriga delar är normativa.

Den första delen (Part 1: PAdES Overview - a framework document for PAdES), version 1.1.1, publicerades juli 2009, och beskriver generella drag i PAdES.

Den andra delen (Part 2: PAdES Basic - Profile based on ISO 32000-1), version 1.2.1, publicerades juli 2009, och specificerar en signatur i enlighet med ISO 32000-1 baserad på CMS. Den tidigare, och första versionen (1.1.1), av dokumentet publicerades april 2009 som TS 102 778.

Den tredje delen (Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles), version 1.1.1, publicerades juli 2009, och specificerar en signatur som baseras på CAdES-BES och CAdES-EPES i TS 101 733, med möjlighet att tillämpa CAdES-T.

Den fjärde delen (Part 4: PAdES Long Term - PAdES-LTV Profile), version 1.1.1, publicerades juli 2009, och möjliggör långtidsvalidering ([rekursiv] tidstämpling) av PDF signaturer, och kan användas tillsammans med del 2 (CMS) och 3 (PAdES-CMS, PAdES-BES, eller PAdES-EPES).

Den femte delen (Part 5: PAdES for XML Content - Profiles for XAdES signatures), version 1.1.1, publicerades juli 2009. Specifikationen har två underdelar, en om XML-dokument och en om XFA-formulär, varav respektive del består av två led.

Den första underdelen, och dess två led, berör båda omslutning av signerade XML-dokument i PDF. ”Profile for Basic XAdES signatures of XML documents embedded in PDF Containers” hanterar de grundläggande XAdES -formaten (XAdES-BES, XAdES-EPES, och XAdES-T), medan ”Profile for long-term XAdES signatures of XML documents embedded in PDF containers”, tillåter de mer utvecklade formaten (XAdES-C, XAdES-X, XAdES-XL och XAdES-A).

Den andra underdelen, och dess två led, berör båda formulär i XFA -formatet. ”Profile for Basic XAdES signatures on XFA forms” utgår från de grundläggande XAdES -formaten (XAdES-BES, XAdES-EPES, and XAdES-T), medan ”Profile for long-term validation XAdES signatures on XFA forms (XAdES-LTV)” tillåter de långtidsbevarandeformaten XAdES-XL och XAdES-A.

---

[23] Signerad rå XML-data i PDF som signeras kan inte utökas stödja långtidsvalidering, medan XML i XFA-format kan utökas stödja långtidsvalidering genom PDF -datastrukturer (ETSI TS 102 778-1 V1.1.1 (20009-07), a. 4.7).

[24] För en fullständig källa se a. 2 i respektive del av ETSI TS 102 778.

3.3.4.3. Kombinationer av format

PAdES tillåter en mer komplex struktur av signaturformat. Följande kombinationer är möjliga.

- Formatet PAdES-LTV kan tilläggas ett PDF-dokument med en elektronisk signatur i formaten: PAdES-CMS, PAdES-BES eller PAdES-EPES.
- Formaten PAdES-CMS, PAdES-BES eller PAdES-EPES, som kan utökas med PAdES-LTV, kan tillämpas på ett dokument som innehåller XAdES -signatur på XML data.
- Grundläggande XAdES[25] utan XFA, och grundläggande XAdES[26] och XAdES-LTV kan användas med PDF -signaturer baserade på vilken PAdES -format som helst, men en XAdES -signatur kan inte uppgraderas efter att en PDF -signatur har tillämpats på dokumentet.

3.3.4.4. Part 4: PAdES Long Term - PAdES-LTV Profile

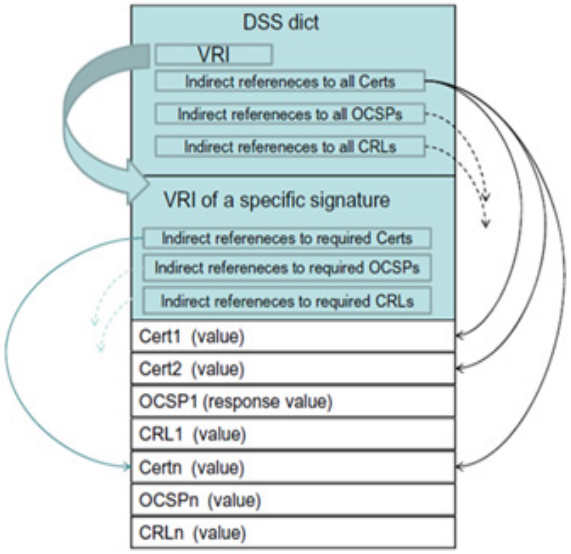
ETSI TS 102 778-4 V1.1.1 (2009-07), a. 1 Figurer i detta avsnitt är direkt hämtade från ETSI TS 102 778-4 V1.1.1 (2009-07), a. 4

Del 4 av PAdES -standarden tillåter långtidsvalidering (”LTV”; ”Long Term Validation”) av delarna 2 (CMS), 3 (CAdES) och 5 (XAdES). För CAdES specificerar PAdES-LTV funktionaliteter som är ekvivalenta till CAdES-Long och CAdES-A i TS 101 733. För XAdES specificerar PAdES-LTV funktionaliteter som är ekvivalenta till XAdES-XL och XAdES-A i TS 101 903.

LTV ska kunna tillämpas vid såväl signerings- som verifieringsprocessen av ett PDF -dokument.

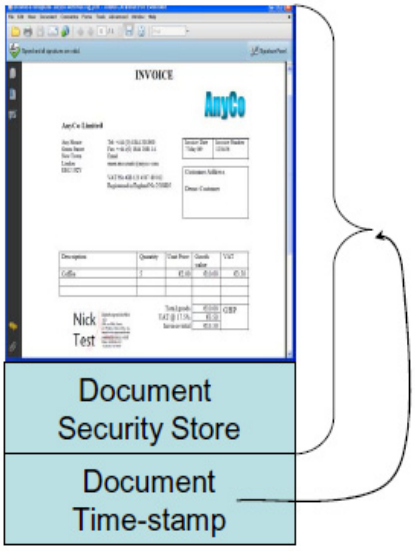
Del 4 utökar även ISO 32000-1 (PDF 1.7) med funktionalitet som krävs för att stödja LTV. Dessa utökningar ska skickas till ISO som förslag att inkluderas i nästa ISO 32000.

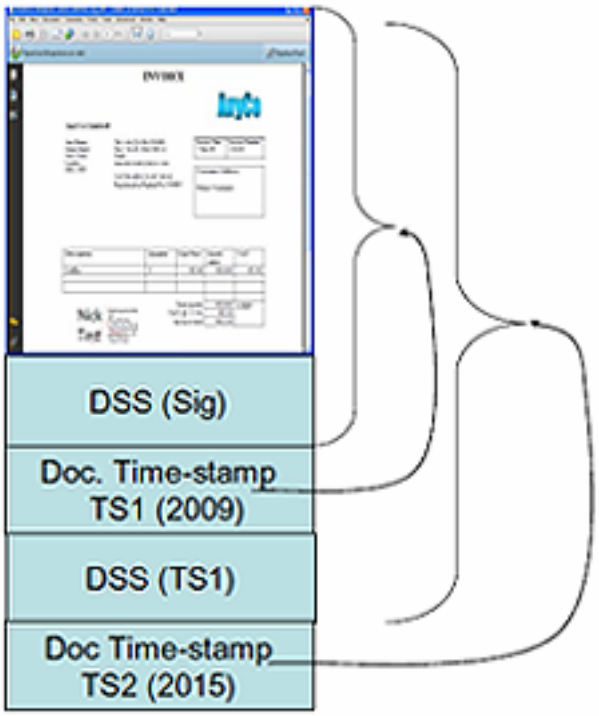
[25] I dokumentationen ”Basic XAdES”.
[26] I dokumentationen ”XAdES-Basic”.



PAdES-LTV använder DSS (”Document Security Store” eller dokumentsäkerhetslagring) och eventuellt VRI (Validation Related Information” eller valideringsrelateradinformation) för att omsluta valideringsdata (hänvisning tillåts inte) och validera signaturer (ETSI TS 102 778-4 V1.1.1 (2009-07), a. 4.2; ETSI TS 102 778-4 V1.1.1 (2009-07), b. A, a. A.1).

En dokumenttidstämplingsfunktion (”Document Time-stamp extension”) förser dokumentet och DSS med en tidstämpel. Valideringsdata för dokumenttidstämpeln kan sedan omslutas genom ytterligare en DSS, som i sin tur tidstämplas. Denna process är rekursiv och kan fortsätta för en obestämd framtid.





3.3.4.5. Part 5: PAdES for XML Content - Profiles for XAdES signatures

Figurer i detta avsnitt är direkt hämtade från ETSI TS 102 778-5 V1.1.1 (2009-07), a. 4 och 5

Del 5 av PAdES -standarden beskriver två fall där två typer av format kan tillämpas för att signera XML innehåll i PDF med XAdES -signaturer i enlighet med TS 101 903. Utgångspunkten är antingen:

- ett XML dokument som är helt eller delvis signerad med XAdES och, som sedan blir, omsluten i ett PDF-dokument,[27] eller
- en dynamisk XFA -formulär där all XML -data är signerad med XAdES eller de delar av XFA -formulär som är tillåtet att signeras är signerad med XMLDSIG[28] (ETSI TS 102 778-5 V1.1.1 (2009-07) a. 1, 4.1).

Det finns två typer av format, som kan tillämpas i två led:

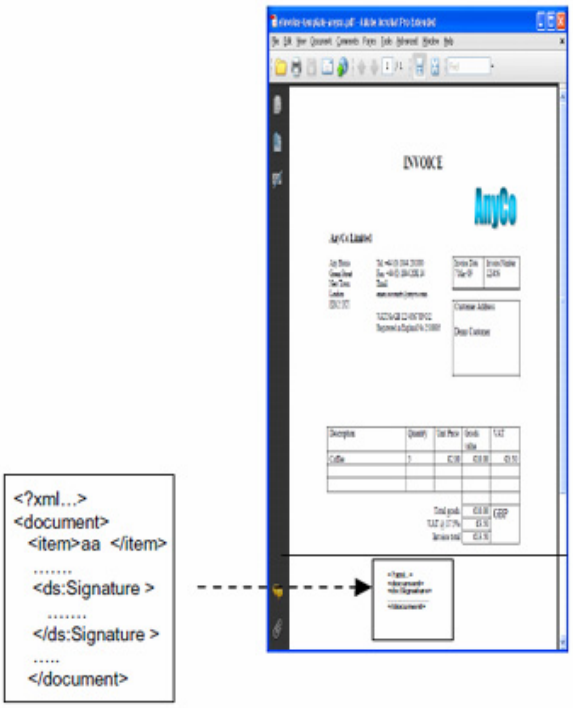
- en grundläggande format ämnad för den signerade parten; XAdES-BES, XAdES-EPES eller XAdES-T.
- ett format för långtidsvalidering av det grundläggande formatet (ETSI TS 102 778-5 V1.1.1 (2009-07) a. 1, 4.1).

[27] Signering av PDF-dokument innebär att XML -dokumentet inte längre kan utvecklas för långtidsvalidering eller ytterligare signaturer. PDF har emellertid certifikatsignaturer som tillåter uppgradering av signaturen i XML -dokumentet.

[28] Det finns särskilda regler för XMLDSIG, men eftersom XAdES bygger på XMLDSIG så omfattas XAdES av samma regler (ETSI TS 102 778-5 V1.1.1 (2009-07) a. 5.1).

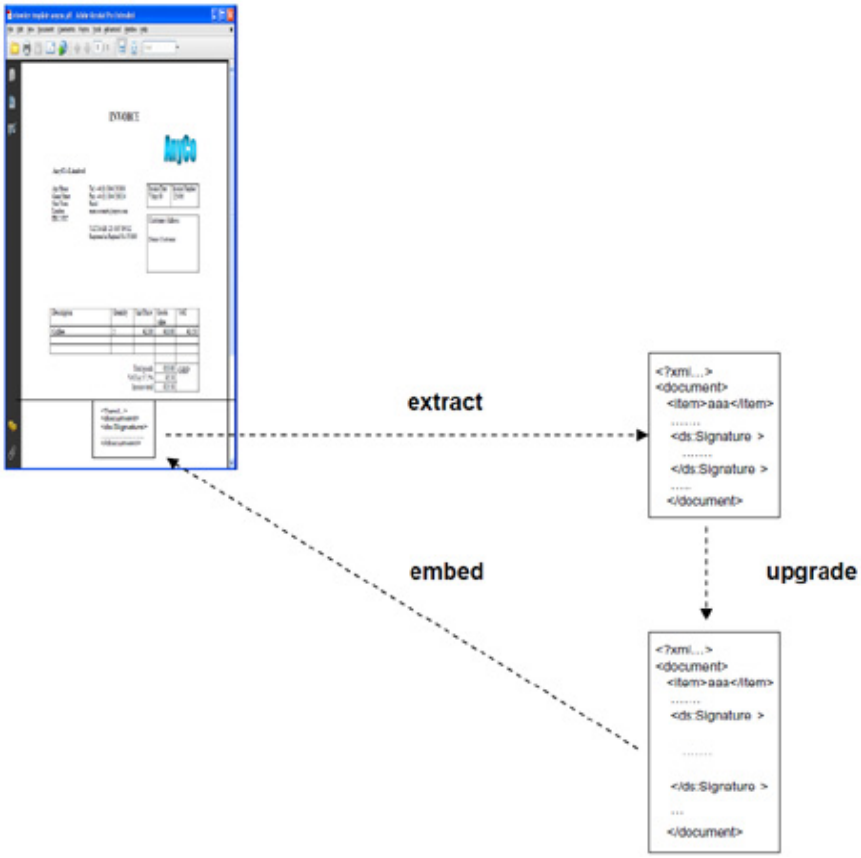
Profile for Basic XAdES signatures of XML documents embedded in PDF containers

Den första utgångspunkten, första ledet: ett XML -dokument signeras med en grundläggande format (XAdES-BES, XAdES-EPES eller XAdES-T) och omsluts i PDF -dokumentet (ETSI TS 102 778-5 V1.1.1 (2009-07) a. 4.1).



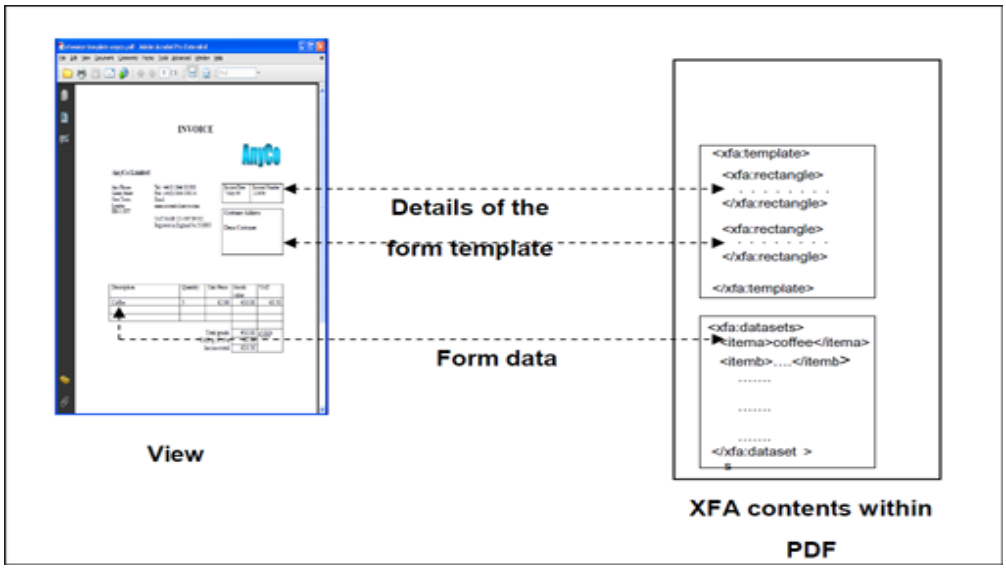
Profile for long-term XAdES signatures of XML documents embedded in PDF containers

Den första utgångspunkten, andra ledet: det omslutna XML -dokumentet extraheras, signaturen uppgraderas utanför PDF -dokumentet, och sedan omsluts åter igen i PDF -dokumentet. De mer utvecklade formaten som stöds är: XAdES-C, XAdES-X or XAdES-XL, XAdES-A (ETSI TS 102 788-5 V1.1.1 (2009-07) a. 4.1, 4.3.1).

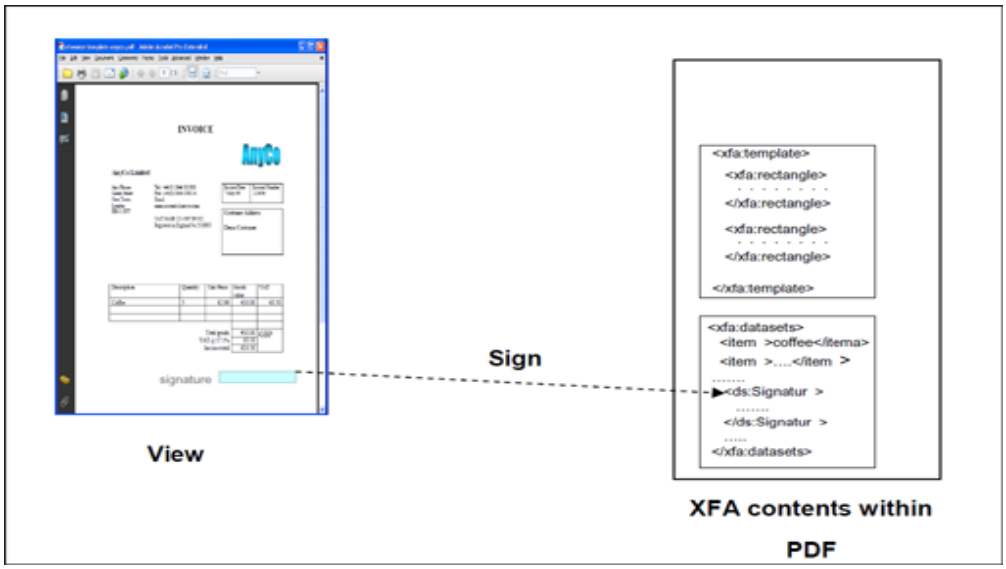


Profiles for XAdES signatures on XFA Forms

XFA består av element för en mall för formulären (”<xfa:template>”), och element för informationen användaren för in i formulären (”<xfa:datasets>”).

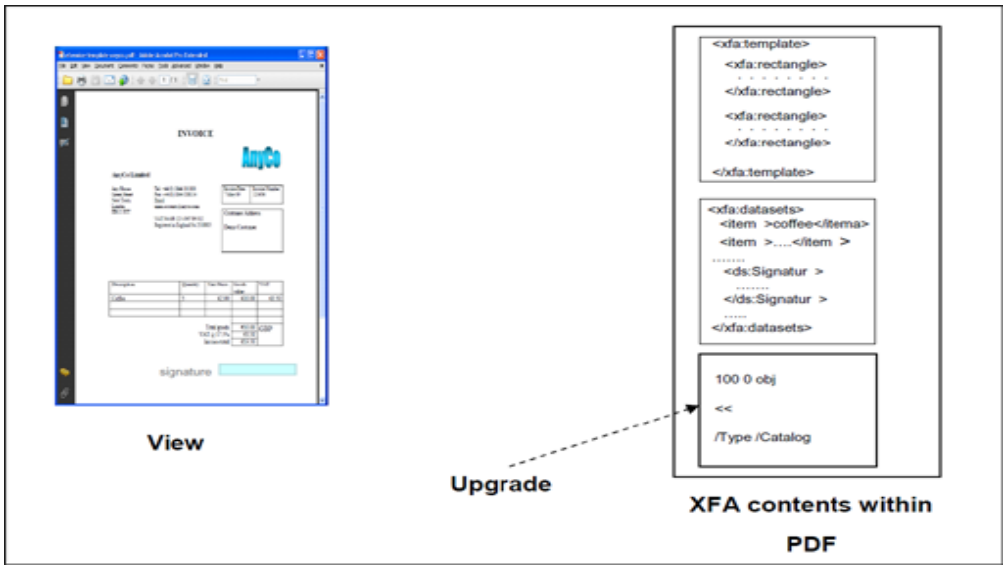


Den andra utgångspunkten, första ledet: signering av XML -data i XFA -formulär eller av tillåtna XML -innehåll i XFA -formulär med en grundläggande format (XAdES-BES, XAdES-EPES eller XAdES-T) (ETSI TS 102 788-5 V1.1.1 (2009-07) a. 5.1).



Profile for long-term validation XAdES signatures on XFA forms (XAdES-LTV)

Den andra utgångspunkten, andra ledet: den signerade XFA -formulären kan uppgraderas genom att omsluta valideringsdata (hänvisning tillåts inte) i dokumenttidstämplingsfunktionen och VRI i enlighet med TS 102 778-4 (se a. 3.3.4.4, Part 4: PAdES Long Term - PAdES-LTV Profile; ETSI TS 102 778-5 V1.1.1 (2009-07) a. 5.3.1). De mer utvecklade formaten som stöds är ekvivalenta funktioner till XAdES-XL och XAdES-A (ETSI TS 102 788-5 V1.1.1 (2009-07) a. 5.1), men inte XAdES-C och XAdES-XL (ETSI TS 102 788-5 V1.1.1 (2009-07) a. 5.3.1, eftersom det inte stöds av ordboken för VRI).



3.3.5. PKCS ("Public Key Cryptography Standards")

PKCS är en serie dokument publicerad från 1991 av "RSA Security", numera "RSA Laboratories" med syfte att stödja praktiska och interoperabla implementeringar av PKI -teknologin. Dessa dokument har i olika omfattningar använts av mjukvaruindustrin och resulterat i att många av dem blivit standarder för säkerhetsprocesser på Internet. IETF har godkänt flertal PKCS som RFC, och nya PKCS dokument fortsätter att utvecklas av RSA Laboratories.

PKCS	Namn	Beskriver	IETF
#1	RSA Cryptography Standard	Implementering av publik-hemlig -kryptering baserad på RSA -algoritmen.	IETF informativ RFC 2313, ersatt av RFC 2437, ersatt av RFC 3447.[29]

[29] http://tools.ietf.org/html/rfc3447

#2	Publicerades inte formellt som PKCS #2.	RSA -kryptering av meddelandekondensat (”hashvärden”); arbetet avbröts 2010 och konsoliderades senare med PKCS #1.[30]	
#3	Diffie-Hellman Key Agreement Standard	En metod för att implementera ”Diffi-Hellman key agreement” för säkra kommunikationer.	
#4	Publicerades inte formellt som PKCS #4.	RSA -nyckelsyntax; arbetet avbröts 2010 och konsoliderades senare med PKCS #1.[31]	
#5	Password-Based Cryptography Standard	Rekommendationer för implementering av lösenordbaserad kryptering.	IETF informativ RFC 2898.
#6	Extended-Certificate Syntax Standard	Syntax för ”extended certificates”.	
#7	Cryptographic Message Syntax Standard	General syntax för data som kan ha kryptering ansluten till den, såsom digitala signaturer.	IETF informativ RFC 2315 (PKCS #7), standardiserad i RFC 2630 (CMS), ersatt av RFC 3369 (CMS) och 3370 (CMS algoritmer). RFC 3369, ersatt av 3852 (CMS), och uppdaterad genom RFC 4853 (multipla signatärer) och 5083 (”Authenticated-Enveloped-Data” innehållstyp), men ersatt av RFC 5652 (CMS). RFC 3370 (CMS algoritmer) uppdaterad genom 5754 (använda SHA2 i CMS).
#8	Private-Key Information Syntax Standard	Syntax för publik-hemlig -nyckelinformation.	IETF informativ RFC 5208 (PKCS #8), ersatt av och standardiserad genom RFC 5958 (asymmetriska nyckelpaket).
#9	Selected Attribute Types	Valda typer av attribut för användning i PKCS #6, PKCS #7, PKCS #8, PKCS #10.	IETF informativ RFC 2985.
#10	Certification Request Syntax Standard	Syntax för begäran av certifiering av en publik nyckel, ett namn, och möjligtvis ett antal attribut.	IETF informativ RFC 2314 (PKCS #10), ersatt av RFC 2986 som uppdateras genom RFC 5967 (applikation/pkcs10 mediatyp).
#11	Cryptographic Token Interface Standard	”Cryptoki” [uttalas ”cryptokey”], en API (programgränssnitt), för mjuk- eller hårdvaramaskiner som hanterar krypterad information och krypteringsfunktioner.	

[30] Wikipedia ”PKCS”.
[31] Wikipedia ”PKCS”.

#12	Personal Information Exchange Syntax Standard [PFX]	Portabel format för lagring och transportering av en användares privata nycklar, certifikat och liknande information.	
#13	Elliptic Curve Cryptography Standard	[Pågående arbete] Aspekter av ”Elliptic curve cryptography”.	
#14	Pseudo-random Number Generation	[Pågående arbete.][32]	
#15	Cryptographic Token Information Format Standard	Användningen av krypteringssymboler för att låta en användare identifiera sig mot standardiserade program oavsett programmets implementering av cryptoki eller symbolgränssnitt.	
Digital Signatures [2002] http://tools.ietf.org/ http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/public-key-cryptography-standards.htm			

3.3.6. XAdES-BES (XML Advanced Electronic Signatures)

I figurerna i detta avsnitt har nedanstående symboler efter en XML-element följande betydelse.	
Frågetecken (?)	innebär att minst 0 eller 1 av föregående element förekommer.
Plus (+)	innebär att minst 1 eller fler av föregående element förekommer.
Asterix (*)	innebär att minst 0 eller fler av föregående element förekommer.

3.3.6.1. Funktion

XAdES är en standard som utökar ”XMLDSIG”[33] i syfte att definiera format för avancerade elektroniska signaturer som är giltiga under en lång tid och överensstämmer med DES. XAdES utgår från PKI och bygger vidare på bland annat CAdES (TS 101 733) (ETSI TS 101 903 V1.4.2 (2010-12), a. ”Introduction” och a. 1, s.ä. a. 6.1).[34]

3.3.6.2. Historik

Det första dokumentet, version 1.1.1 (februari 2002), publicerades som ETSI TS 101 903, där den senaste versionen är 1.4.2 (december 2010).[35] Dokumentet behandlar inte policyn för signaturer, hänvisning görs istället till TR 102 038 (informativ), med undantag för policy för att uppnå ”teknisk konsistens” (”technical consistency”) vid validering av elektroniska signaturer.

[32] http://tools.ietf.org/html/rfc3447
[33] IETF W3C XML-Signature Working Group: XML-Signature Core Syntax and Processing.
[34] För en fullständig källa se ETSI TS 101 903 V1.4.2 (2010-12), a. 2.
[35] ETSI TS 101 903 V1.4.2 (2010-12), s. 104.

3.3.6.3. Format för valideringsdata

I syfte att validera signaturer krävs valideringsdata, vilket består av:

- PKC (”Public Key Certificate” eller ”certifikat för publik nyckel”) och AC (”Attributes Certificate” eller ”certifikat för attribut”),
- återkallelsestatus för varje PKC och AC,
- Certifikatutfärdarens certifikat, samt dess CRL eller OCSP (”Online Certificate Status Protocol”),
- antingen en tillförlitlig tidstämpel på signaturen, eller ett tidmärke (”time-mark”) i revisionshistoriken (”audit log”),
- när tillämpligt, detaljerna kring policyn för signaturen som ska användas för att validera signaturen.

Valideringsdata kan sammanställas av signatären och/eller verifieraren, och när tillämpligt, i enlighet med kraven i angiven policy.

XAdES uppställer fem kumulativa variationer för att omsluta valideringsdata. Två av dessa, XAdES-T och XAdES-C, tillhör de grundläggande formaten, medan övriga tre, XAdES-X, XAdES-X-L, och XAdES-A, tillhör de utökade formaten.

3.3.6.4. Grundläggande format

ETSI TS 101 903 V1.4.2 (2010-12), a. 4.4
Figurer i detta avsnitt är direkt hämtade från ETSI TS 101 903 V1.4.2 (2010-12), a. 4.4

XAdES är en kumulativ format, det vill säga, de olika variationerna av XAdES bygger på varandra. Grundformatet för en XAdES måste antingen vara BES, EPES, T eller C.

XAdES-BES (XAdES Basic Electronic Signature)

Det grundläggande formatet för XAdES måste innehålla **1(2)** den digitala signaturen som omsluter data och signeringsattributen (XMLDSIG), samt **2(2)** en hänvisning till nyckelns certifikat och dess hashvärde.

Formatet får eventuellt även innehålla en uppsättning av **(A)** signerade och **(B)** osignerade egenskaper.

Formatet är det minsta som krävs för en elektronisk signatur, och uppfyller EU:s krav på ”elektroniska signaturer”, men har inte tillräckligt med information för att kunna valideras efter lång tid.

XAdES-EPES (XAdES Explicit Policy based Electronic Signature)

XAdES-EPES kan utgå direkt från XMLDSIG eller från BES.

Formatet uppställer ett obligatoriskt element; ett särskilt signerat element som anger att en policy ska tillämpas vid validering, men behöver inte explicit ange vilken policy som ska tillämpas.

Figuren till vänster illustrerar tillägget av elementet utifrån XAdES-BES. Den röda rutan markerar den element som tillkommer jämfört med BES.

XAdES-T (XAdES with Time-stamp)

XAdES-T associerar en tillförlitlig tid till den elektroniska signaturen, vilket är det första steget till en långtidsvalidering av elektroniska signaturer.

Den tillförlitliga tiden kan antingen anges som en tidstämpel i osignerat element, eller ett tidmärke, inte angiven i något element, utan hanterad av en betrodd tjänstetillhandahållare, med ansvar att vid behov tillhandahålla bevis på den tillförlitliga tiden.

Figuren till vänster illustrerar tillägget av elementet utifrån XAdES-BES eller XAdES-EPES.

XAdES-C (XAdES Complete validation data)

XAdES-C lägger till XAdES-T två osignerade element som anger hänvisningar till alla certifikat och CRL och/eller OCSP gensvar som används för att verifiera signaturen, och, om attributcertifikat används i signaturen, två osignerade element för hänvisningar till alla attributcertfikat.

Bevarande av hänvisningar till information, istället för omslutning av information, möjliggör reducering av formats storlek.

Figuren till vänster illustrerar XAdES-C utifrån XAdES-BES eller XAdES-EPES och XAdES-T.

3.3.6.5. Utökade format

ETSI TS 101 903 V1.4.2 (2010-12), b. B
Figurer i detta avsnitt är direkt hämtade från ETSI TS 101 903 V1.4.2 (2010-12), b. B

XAdES-X, XAdES-X-L, och XAdES-A utökar XAdES genom att tillåta särskilda osignerade egenskaper i syfte att möjliggöra verifikation efter en mycket lång tid, och förhindra vissa ”katastrofala situationer”.[36]

[36] Ingen direkt hänvisning till vad som menas, utan en generell hänvisning till dokumentets ”normativa del”, men jfr not 17: Verkar åsyfta att förhindra att någon kan använda ett falskt certifikat när nycklarna för en certifikatutfärdare äventyras (ETSI TS 101 733 V2.2.1 (2013-04) b. C, a. C.4).

XAdES-X (XAdES eXtended validation data eller Extended signatures with time forms)[37]

XAdES-X bygger på XAdES-C, och finns i två variationer: Type 1 och Type 2.

XAdES-X Type 1 tidstämplar följande element: signaturen, signaturens tidstämpel om den finns, och alla hänvisningar till certifikat och återkallelsestatus.

XAdES-X Type 2 tidstämplar följande element: alla hänvisningar till certifikat och återkallelsestatus.

[37] Förklaring skiljer sig från a. 3.2 Abbreviations och b. B a. B.1.

XAdES-X-L (XAdES eXtended validation data eller Extended signatures with time forms)[38]

XAdES-X-L bygger på XAdES-X Type 1 eller Type 2 och tillägger två element för att omsluta alla certifikat och återkallelsestatus.

[38] Förklaring skiljer sig från a. 3.2 Abbreviations och b. B a. B.2.

XAdES-A (XAdES Archiving validation data eller Archival electronic signatures)[39]

XAdES-A tillägger två element för att omsluta alla certifikat och återkallelsestatus, samt element för successiva tidstämplar, särskilt avseende valideringsdata.

Successiva tidstämplar skyddar all material mot svaga hash algoritmer eller mot nedbrutna krypteringsmaterial eller -algoritmer.

[39] Förklaring skiljer sig från a. 3.2 Abbreviations och b. B a. B.3.

3.3.6.6. Exempel på hur XAdES variationerna kan byggas på varandra

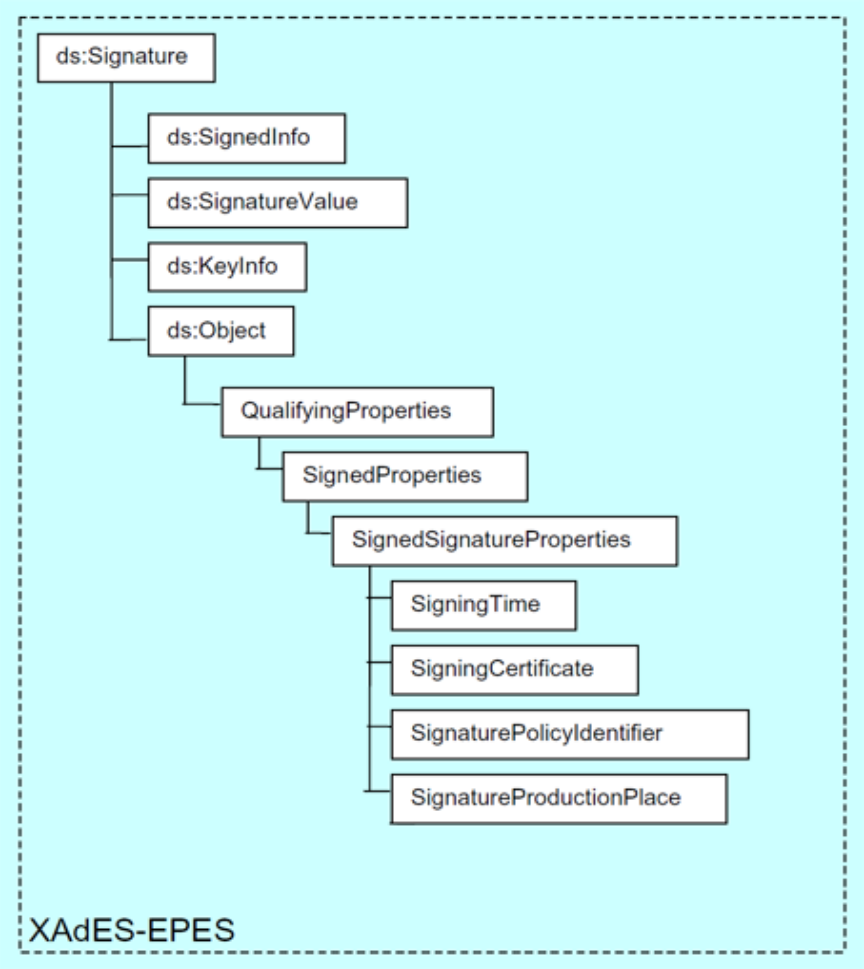
ETSI TS 101 903 V1.4.2 (2010-12) b. G
Figurer i detta avsnitt är direkt hämtade från ETSI TS 101 903 V1.4.2 (2010-12), b. G

Valideringsprocessen av XAdES, om signaturen accepteras eller avvisas, är beroende av tekniska och icke-tekniska bedömningar, samt i det sammanhang signaturen ska användas, vilket kan variera från fall till fall. Dokumentation för XAdES har därför inte normerat valideringsprocessen, och istället ges i bilaga G informativa exempel på vilka tekniska steg valideringsprocessen kan ta form, vilket sannolikt är gemensamt för de flesta sammanhang som signaturer används, och som verifieraren därför bör utföra vid validering av signaturer.

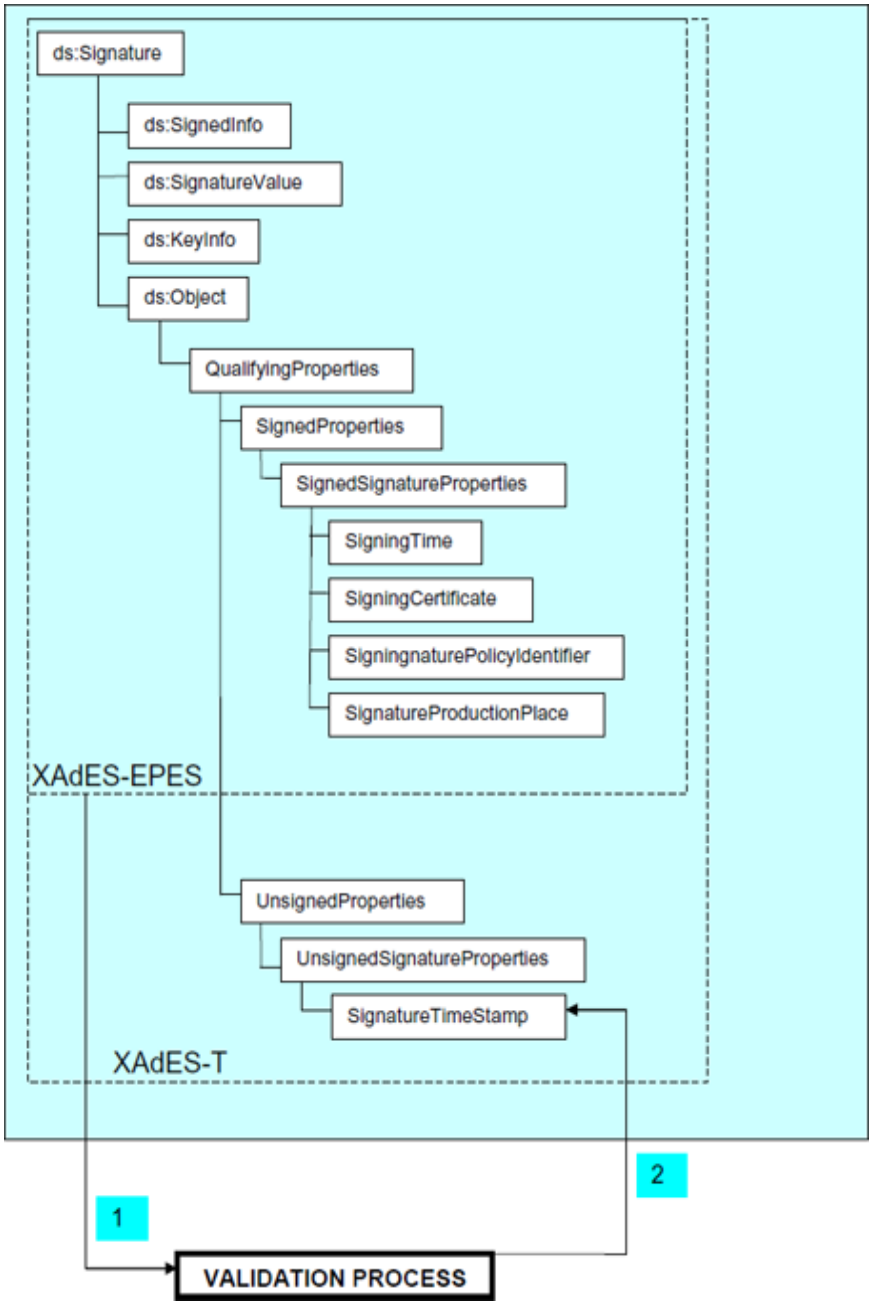
Exemplen visar hur en XAdES-EPES signatur kan, under valideringsprocessen, byggas ut till mer avancerade XAdES -former: XAdES-T till XAdES-C till XAdES-X till XAdES-X-L till XAdES-A. Detta är inte en nödvändig successiv process; andra konstruktioner kan också byggas fram beroende av behov och sammanhang.

Valideringsprocessen beaktas från verifierarens perspektiv. Medan signaturprocessen kan sammanställa XAdES -formen upp till C så är det mer troligt att i de flesta fall så kommer signaturprocesser inte att tillägga valideringsdata.

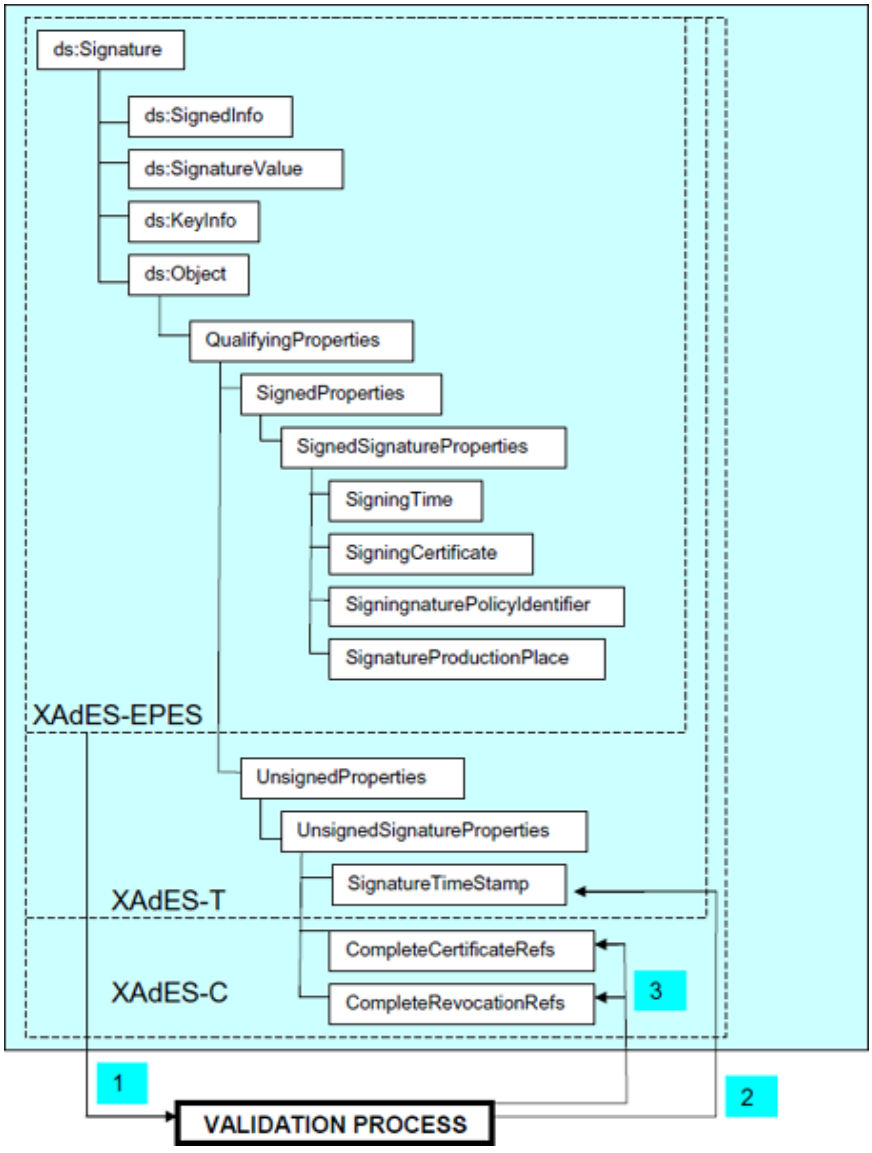
Utgångspunkten för exemplen är en signatur i formatet XAdES-EPES som verifieraren har tagit emot.



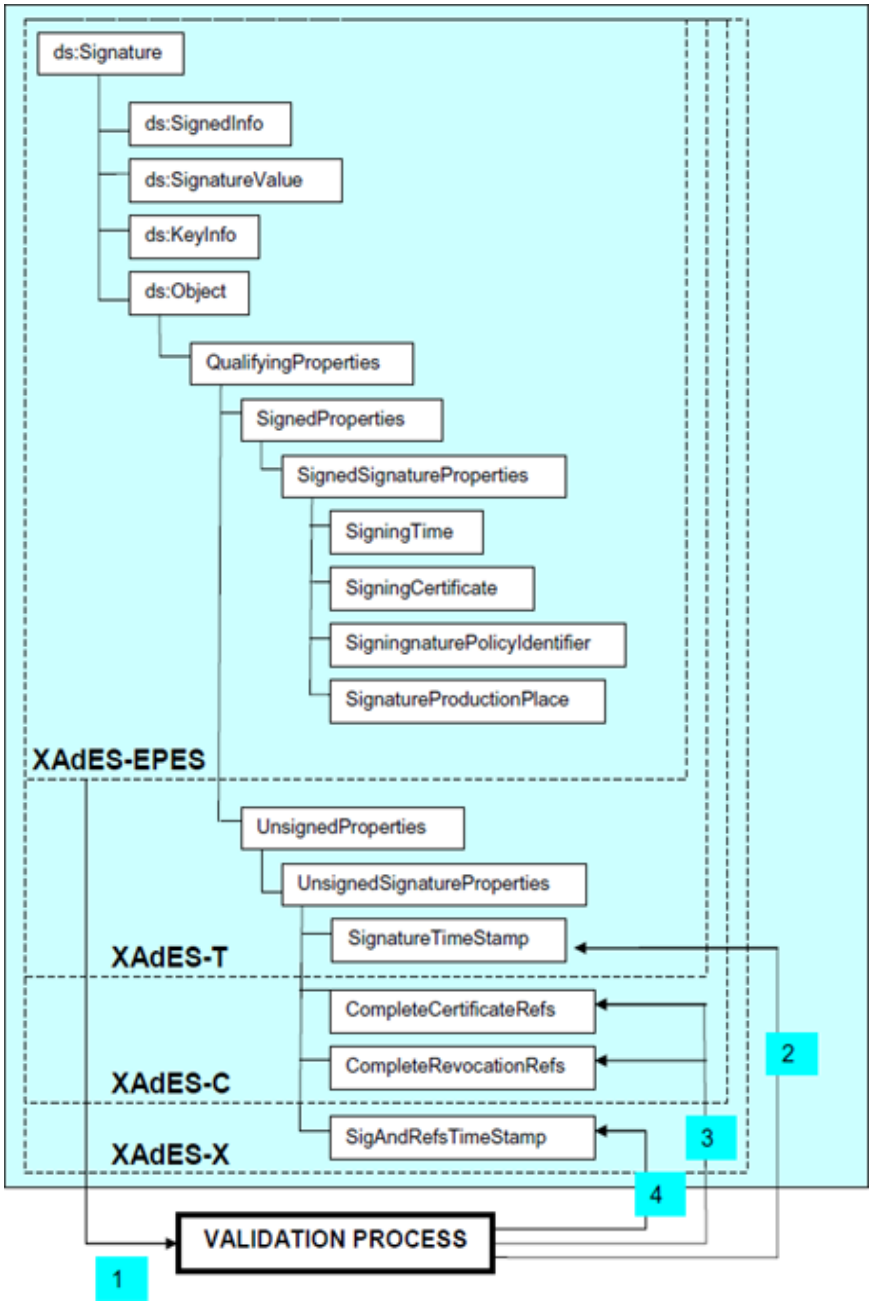
Verifieraren kan **(1)** kontrollera själva signaturen, och sedan **(2)** tidstämpla signaturen, vilket gör att formatet XAdES-EPES övergår till XAdES-T.



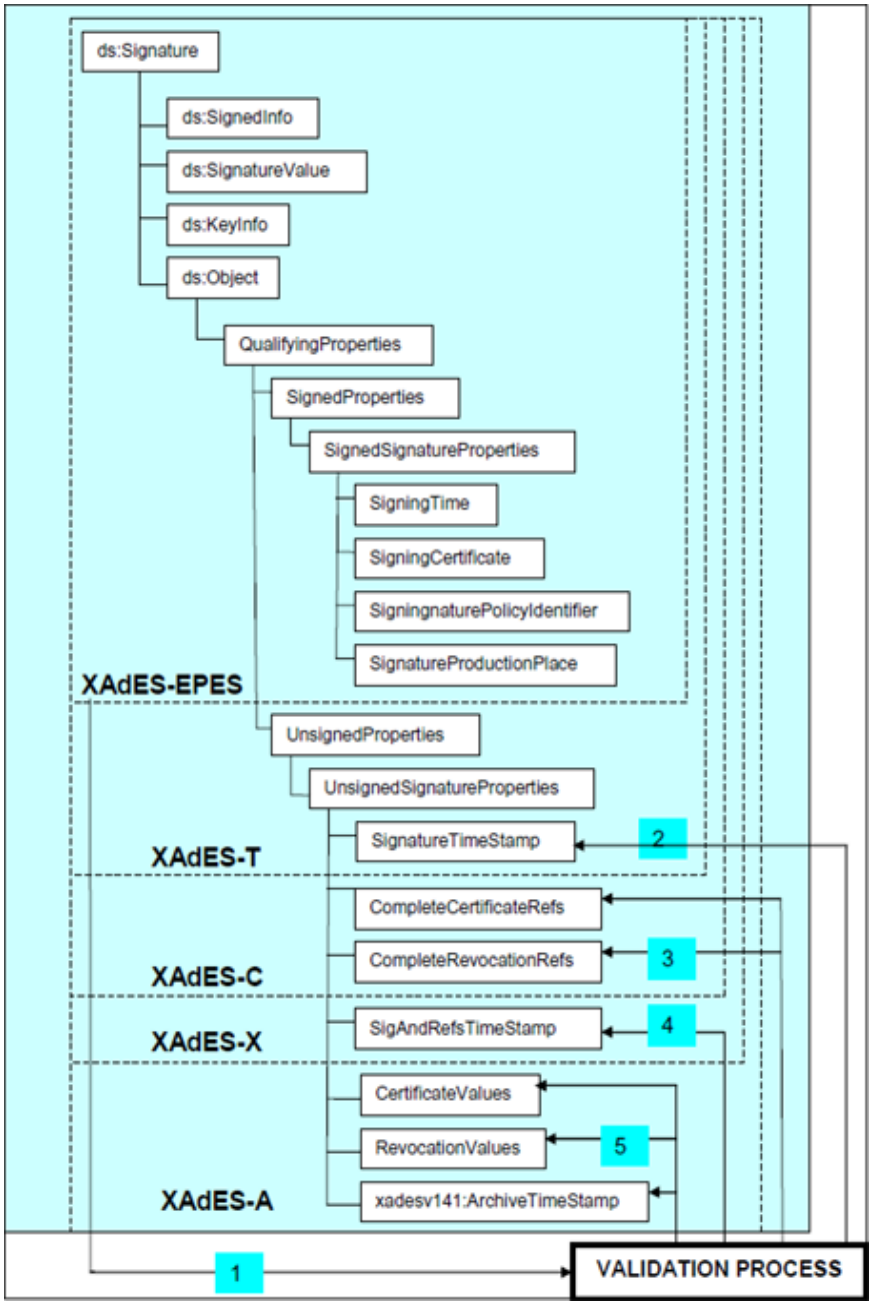
När verifieraren får tillgång till all valideringsdata, däribland certifikat och återkallelsestatus, går det att göra en fullständig validering och **(3)** generera en XAdES-C.



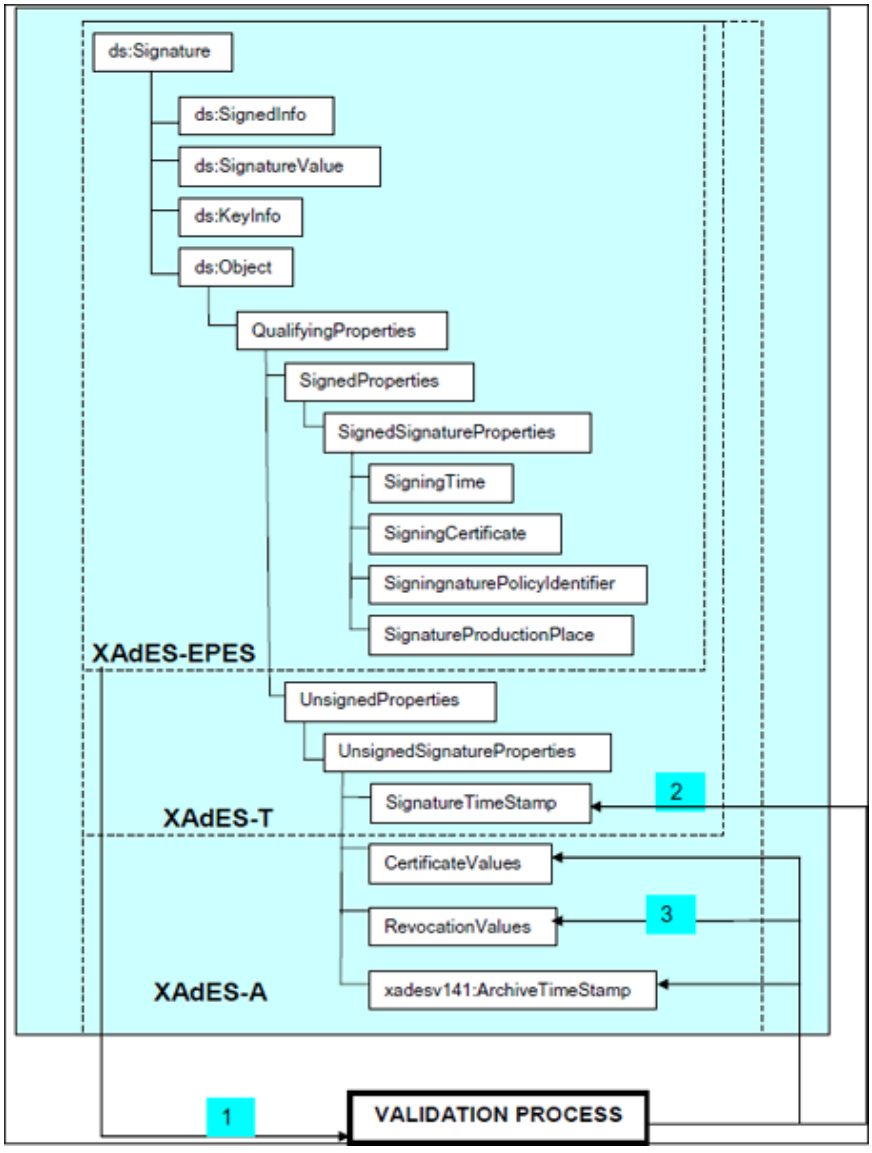
I samband med XAdES-C är det möjligt att **(4)** generera utökade format för valideringsdata som XAdES-X Type 1 eller Type 2.



Innan algoritmerna som användes för exempelvis signaturen, tidstämplar, och certifikat, blir eller riskerar att bli sårbara, så kan det bli nödvändigt att **(5)** insamla och omsluta all data och tidstämpla allt, vilket resulterar i XAdES-A.



Det är möjligt att direkt övergå från XAdES-EPES direkt till XAdES-A, genom XAdES-T och omslutning av all valideringsdata.



3.3.7. XML Dsig (XML Signature Syntax)

3.3.7.1. Funktion

XML Signature Syntax and Processing beskriver en syntax och regler för integritet (kondensat), och autenticitet för meddelanden (signaturer) och signatärer (certifikat) för data i XML med signaturen eller utanför. Informationen behandlas inte i binär form utan i ”textform”.

3.3.7.2. Historik

Fyra versioner av dokumentationen för standarden har påträffats. De två första versionerna saknar numrering. Den första var publicerade den 12 februari 2012,[40] och den andra utgåvan av den versionen är daterat till 10 juni 2008. Den tredje versionen, och nu gällande, utgiven 11 april 2013, är numrerad som version 1.1.[41] Samtliga versioner är W3C rekommendationer.

Den sista versionen, 2.0, utgiven 11 april 2013 är inte en W3C rekommendation utan en informativ ”Working Group Note”.[42]

[40] http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/
[41] http://www.w3.org/standards/techs/xmlsig/
[42] http://www.w3.org/TR/2013/NOTE-xmldsig-core2-20130411/

4. Infrastruktur

Detta avsnitt beskriver den infrastruktur som tillämpas [2013] för att distribuera och använda ett elektroniskt signerat dataobjekt; de tekniska, juridiska och organisatoriska processer som tillsammans skapar ett system som säkerställer att den elektroniska signaturen uppfyller de krav som uppställs på autenticitet.

4.1. Juridisk reglering

Svenska certifikatutfärdare som utfärdar ”kvalificerade” certifikat ”till allmänheten” [i ”öppna system”] omfattas av LKES (§ 1:2), och ställs under viss tillsyn och har skadeståndsansvar för utfärdade certifikat.

4.1.1. Förvaringsskyldighet

En certifikatutfärdare har en skyldighet att ”bevara all relevant information om certifikaten under den tid som är motiverad med hänsyn till typen av certifikat och övriga omständligheter.” (LKES § 11:1). Relevant information åsyftar underlag för bevis vid rättsliga förfaranden, och inte signaturframställningsdata (prop. 1999/2000:117, s. 43:3, 74). Det framgår emellertid inte av förarbetet vad som är ”motiverad tid”.

En certifikatutfärdare får inte bevara, lagra eller kopiera signaturframställningsdata (LKES § 11:2, prop. 1999/2000:117 s. 43:3, 74, jfr s. 29:7, från DES: ”Vidare är utfärdaren förbjuden att lagra eller kopiera uppgifter för skapande av signaturer.”; jfr LKES § 3 p. 1, ”[en anordning för signaturframställningsdata ska säkerställa att signaturframställningsdata] i praktiken kan förekomma endast en gång”) eftersom ”… det är väsentligt för tilltron till elektroniska signaturer att det bara är undertecknaren som har tillgång till signaturframställningsdata” (prop. 1999/2000:117 s. 43:3,74; jfr a. 4.1.6.10, Certifikat: Hemliga nycklar,). En certifikatutfärdare får emellertid generera signaturframställningsdata förutsatt att det sker konfidentiellt (LKES § 9 p. 7, prop. 1999/2000:117 s. 73; jfr 4.1.6.14, Certifikat: ”Roaming Credentials”,).

4.1.2. Kvalificerade certifikat

Ett kvalificerat certifikat måste uppfylla kraven i LKES § 6. Certifikatet måste:

- vara utfärdat av en certifikatutfärdare som är anmäld hos tillsynsmyndigheten (LKES § 8), och som uppfyller kraven i
  - LKES § 9-12, 1:2 (svenska certifikatutfärdare) eller § 7 (utländska certifikatutfärdare),
  - eventuella meddelade föreskrifter med stöd av LKES § 13,
- vara utfärdad för viss tid,
- uppfylla kraven på innehåll i LKES § 6:1 p. 1-9, och
- eventuella meddelade föreskrifter med stöd av LKES § 6:2.

4.1.3. Sekretess

Sekretess gäller, för signaturframställningsdata förvarad hos myndighet, i syfte att förhindra missbruk genom insyn enligt offentlighetsprincipen (OSL 18:9, tidigare 5:2 Sekretesslagen; se vidare prop. 1999/2000:117 a. 9, Sekretessfrågor).

4.1.4. Tillsyn

En tillsynsmyndighet, Post- och telestyrelsen, säkerställer bland annat att kvalificerade certifikat uppfyller de i LKES uppställda kraven för kvalificerade certifikat, och ingriper mot missbruk (se vidare prop. 1999/2000:117 a. 6.12, Tillsyn).

4.1.5. Öppna och slutna system

Från ett juridiskt perspektiv, genom LKES, ser man på ett system för elektroniska signaturer antingen som ”öppet” [”till allmänheten”] eller ”slutet”. Tillämpningsområdet för LKES, och det bakomliggande direktivet DES, är öppna system.

Det finns tre faktorer som påverkar bedömningen om ett system är öppet: certifikatutfärdare, undertecknare och mottagare. Ju mer sammanvävd dessa faktorer är genom civilrättsliga avtal desto slutnare betraktas systemet. Det kan exempelvis röra sig om en signatur som ska användas inom samma organisation eller tjänst, såsom bankernas Internettjänster. Ett öppet system blir motsatsvis öppnare när faktorerna blir mer löst sammanhållna. Detta kan exempelvis vara när mottagaren måste förlita sig på en signatur eller certifikat utanför ett civilrättsligt avtalsförhållande (prop. 1999/2000:117 a. 5.2:1, s. 35:4-36:2). Öppna system tillåter i princip att vem som helst kan bli en certifikatutfärdare, undertecknare och mottagare i systemet utan att behöva i förhand ingå avtal med någon annan i systemet.

Det framgår av DES en strävan efter teknikneutralitet och ett förbud mot att införa förhandstillstånd för kvalificerade certifikat. Detta förhindrar möjligheten att organisera en tillitsmodell för certifikat där staten fungerar som den absoluta rot-certifikatutställare [”toppnod”] och utfärdar certifikat för övriga certifikatutställare. Fördelen med en sådan modell skulle vara effektiv tillsyn över alla certifikat i omlopp. Detta innebär också emellertid att i syfte operera på marknaden måste övriga utfärdare av kvalificerade certifikat ansluta sig och anpassa sina tekniska lösningar till den statliga rot-certifikatutställaren [slutet system], vilket inte är förenligt med DES (prop. 1999/2000:117 s. 61:2-3 jfr 4.1.6.16, Tillitsmodeller för certifikat: Bro-certifikatutfärdare; jfr 4.5.5 Öppet eller slutet system?,).

4.1.6. Certifikat

Syftet med certifikat är att sammankoppla en identitet med signaturen; från vem en hemlig nyckel och dess offentliga nyckel härrör. Den elektroniska signaturen må vara unik men är inte sammankopplad med någon särskild identitet. Den elektroniska signaturen kan enbart skapas med en hemlig nyckel, men mottagaren vet inte med säkerhet att signaturen tillhör den som är utställt i signaturen. Vem som helst med en hemlig nyckel kan framställa en elektronisk signatur och hävda att signaturen tillhör den som är utställt i signaturen. Mottagaren behöver således verifiera att signaturen tillhör rätt utställare; vems privata nyckel har använts?

Det följer att lösningen inte kan vara uteslutande teknisk och kräver administrativ, juridisk och organisatorisk stöd.

Certifikatsystemet introducerar en [betrodd] tredje part eller ”TTP” (Trusted Third Party), en så kallad ”certifikatutfärdare” eller ”CA” (”Certification Authority”),[43] som understödjer transaktionen mellan utställaren och mottagaren. Certifikatutfärdaren har ansvar att utfärda, hantera och upphäva certifikat.

Ett certifikat intygar att en offentlig nyckel härrör från en särskild identitet. Certifikatet är antingen elektroniskt signerat med certifikatutfärdarens hemliga nyckel, det vill säga, ”självsignerat” (”self-certification” eller ”self-signed certificate”) eller en annan certifikatutfärdares hemliga nyckel (Digital Signatures [2002] s. 61:2; jfr LKES § 6 p. 8; enligt LKES § 6 p. 5 måste den offentliga nyckeln inkluderas i ett kvalificerat certifikat).

Systemet förutsätter att den hemliga nyckeln inte obehörigen kopierats eller använts.

4.1.6.1. Anslutning till ett certifikatstatusprotokoll eller ”OCSP” (”Online Certificate Status Protocol”)

En begäran om ett certifikats tillstånd genom OSCP ger en respons om certifikatets status. Statusmeddelanden arkiveras inte av någon aktör så det faller på verifieraren av en signatur att statusmeddelanden lagras korrekt (ETSI TS 101 733 V2.2.1 (2013-04) b. C, a. C.4.1.2).

Informationen från OSCP används för att säkerställa att certifikatet för signaturen var giltig vid tidpunkten för signeringen (s.ä. a. 4.1.6.7, Förteckning över återkallade certifikat eller ”CRL” (”Certificate Revocation List”)).

4.1.6.2. Arkivering och återskapande av nycklar

Ett certifieringsorgan kan erbjuda arkivering[44] av nycklar i syfte att återställa förlorade nycklar. En nyckel som används för elektronisk signering bör emellertid aldrig arkiveras (Digital Signatures [2002] s. 74:4).

4.1.6.3. Attributauktoritet eller ”AA” (”Attribute Authority”)

En attributauktoritet utställer attributcertifikat som binder en eller flera attribut till en identitet. Attributen certifierar identitetens behörighet. Detta kan exempelvis vara den funktion eller roll som identiteten har i en organisation med den juridiska behörighet som tillåter att en juridisk handling eller åtgärd kan vidtas, såsom fullmakt att binda organisation till ett avtal. Attributsauktoriteter upprättas vanligtvis inom organisationer, vilka bäst vet varje individs behörighet inom organisationen. Attributscertifikat kan också ha korta giltighetsperioder, exempelvis

[43] LKES § 2:12, ”certifikatutfärdare: den som utfärdar certifikat eller som garanterar att någon annans certifikat uppfyller vissa krav.”.
[44] Begreppet ”arkivering” används inte i juridisk betydelse här utan i certifikatstjänstsammanhang.

vara giltig endast för en dag (ETSI TS 101 733 V2.2.1 (2013-04) b. C, a. C.3.4; ETSI TS 101 903 V1.4.2 (2010-12) a. 7.2.8).

4.1.6.4. Certifikatpolicy

En omfattande och principiell beskrivning av hur certifikatutfärdaren arbetar och de åtgärder som tas för att säkra och skapa tillit till sina certifikat (Statskontorets rapport 2003:13 s. 21, 90).

4.1.6.5. Certifikatets livscykel

Ett certifikat måste ha en begränsad livstid,[45] vilket föranleder följande möjliga steg i certifikatets livscykel efter utfärdande: förnyande, förfallande eller upphävande (Digital Signatures [2002] s. 65:3-2).

4.1.6.6. ”CPS” (”Certification Practice Statement”)

En beskrivning av hur certifikatutfärdaren praktiskt gör för att tillämpa och uppfylla sin certifikatpolicy (Statskontorets rapport 2003:13 s. 21, 90).

4.1.6.7. Förteckning över återkallade certifikat eller ”CRL” (”Certificate Revocation List”)

En förteckning över återkallade certifikat upprätthålls av en certifikatutfärdare efter att certifikatet antingen markerats som ogiltigt i eller borttagits från platsen där certifikaten förvaras. Problemet är att förteckningarna publiceras inom specifika intervaller, och en hemlig nyckel som inte är tillförlitlig är fortfarande i bruk tills förteckningen uppdaterats (Digital Signatures [2002] s. 82:3; protokoll har föreslagits för att möjliggöra förfrågningar om ett certifikats status: OCSP (Online Certificate Status Protocol) i RFC 2560, se a. 4.1.6.1, och SCVP (Simple Certificate Validation Protocol); jfr LKES § 10 p. 1-2; s.ä, ETSI TS 101 733 V2.2.1 (2013-04) b. C, a. C.4.1.1).

Informationen från en CRL används för att säkerställa att certifikatet för signaturen var giltig vid tidpunkten för signeringen (ETSI TS 101 733 V2.2.1 (2013-04) b. C, a. C.4.1-C.4.1.1).

4.1.6.8. Förteckning över återkallade certifieringsutfärdare eller CARL (”Certificate Authority Revocation List”)

En förteckning över återkallade certifikatutfärdare. Informationen från en CARL används för att säkerställa att alla certifikatutfärdare för signaturen var giltiga vid tidpunkten för signeringen (ETSI TS 101 733 V2.2.1 (2013-04) b. C, a. C.4.2).

4.1.6.9. Förvaring av certifikat eller ”Certificate Repository”

Certifikatförvaringen åsyftar en ”plats”, exempelvis en databas, där alla certifikat utfärdad av certifikatutfärdaren sparats eller lagrats. Förvaringen kan fungera som en central lagrings-

[45] Jfr LKES § 6:1, rekvisit för kvalificerad certifikat: ”utfärdat för viss tid”.

plats för alla offentliga nycklar, och även alla upphävda certifikat (Digital Signatures [2002] s. 65; jfr a. 4.1.1, Förvaringsskyldighet,).

4.1.6.10. Hemliga nycklar

En certifikatutfärdare kan utfärda hemliga nycklar (jfr LKES § 10 p. 3, prop. 1999/2000:117 s. 73), men dessa bör inte användas för signaturer, utan möjligtvis för kryptering av innehåll [konfidentialitet]; hemliga nycklar bör alltid genereras på klient-sidan och inte på server-sidan (Digital Signatures [2002] s. 74:3-4; jfr 4.1.6.14, Certifikat: ”Roaming Credentials”; jfr a. 4.1.1, Förvaringsskyldighet).

4.1.6.11. Hårda och mjuka certifikat

Med hårda certifikat åsyftas ett certifikat utfärdat för en hemlig nyckel som är bundet till ett fysiskt objekt, exempelvis ett ”kort”, vilket ska förhindra kopiering av nyckeln. Med mjuka certifikat åsyftas ett certifikat utfärdat för en hemlig nyckel som är förvarad, exempelvis, som en ”datafil” på en hårddisk, vilket kan kopieras.

4.1.6.12. Hårda och mjuka nycklar

Med hårda nycklar åsyftas en hemlig nyckel som är bunden till ett fysiskt objekt, tillverkad enligt strikta metoder, exempelvis ”smarta kort”, vilket ska skydda mot olika former av attacker. Med mjuka nycklar åsyftas en hemlig nyckel som är förvarad, exempelvis, som en ”datafil” på en hårddisk (Prop. 1999/2000:117 s. 23).

4.1.6.13. Registreringsorgan eller ”RA” (”Registration Authority”)

Ett registreringsorgan kan definieras som ansvarig för att autentisera och validera inkommande begäran om certifikat. Ett registreringsorgan kan uppställas som en fysisk resurs för att hantera en logisk fördelning av arbetsuppgifter som annars sköts av certifikatutfärdaren, vilket avlastar certifikatutfärdarens arbetsbörda. En certifikatutfärdare kan således uppställa en eller flera registreringsorgan som hanterar själva certifikatsprocessen mot allmänheten (Digital Signatures [2002] s. 64).

4.1.6.14. ”Roaming Credentials”

”Roaming Credentials” åsyftar att både den hemliga nyckeln och certifikatet lagras krypterad på en central server och hämtas säkert av användaren till den lokala klienten vid exempelvis signering eller kryptering/dekryptering av data (Digital Signatures [2002] s. 75:1).

4.1.6.15. Tidstämpelsauktoritet eller ”TSA” (”Time-Stamping Authority”)

En tidstämpelsauktoritet är en pålitlig källa som kan förse ett givet hashvärde med en tidstämpel. En tidstämpel består av ett signerat dokument med det hashvärdet som signerats [stämplats], vem som har utfört signeringen [tidstämplingen] av hashvärdet, och tidpunkten för stämpeln. Detta bevisar att det tidstämplade informationen existerade *före* tidpunkten för

stämpling (ETSI TS 101 733 V2.2.1 (2013-04) b. C, a. C.4.3; ETSI TS 101 903 v1.4.2 (2010-12) a. 7.1.4).

4.1.6.16. Tillitsmodeller för certifikat

Certifikat bygger på den tillit användarna har hos certifikatutfärdaren, och följaktligen, för dess utfärdade certifikat. Fråga om det tillit en certifikatutfärdare åtnjuter kan omfatta en annan certifikatutfärdare. Anledningen till att man vill använda flera certifikatutfärdare för att hantera certifikat kan vara allt från de dataresurser som krävs, till de administrativa problem som uppstår, för att hantera större antal certifikat. En lösning är att sprida ut hantering av certifikat mellan olika certifikatutfärdare.

Ett certifikat kan antingen vara själv-signerat av en certifikatutfärdare eller signerat av en annan certifikatutfärdare.

Det finns alltid ett ursprungligt certifikat, ”rot-certifikatet”, som antingen utgör ”huvudcertifikatet” mellan certifikatutfärdaren och användarna eller utgör grunden för mer komplicerade certifikatstrukturer mellan flera certifikatutfärdare. Rot-certifikatet är, som andra certifikat, antingen själv-signerat eller signerat av en annan certifikatutfärdare.

I ett hierarkiskt certifikat-struktur utgör ett rot-certifikat grunden för andra certifikatutfärdare som använder rot-certifikatet, eller certifikat härledda från rot-certifikatet, för att utfärda ytterligare certifikat istället för att ”själv-signera” certifikat. Inom denna hierarki kan användarens tillit knytas till en gemensam grund; rot-certifikatet.

Frågan är hur man kan koppla ihop flera certifikat från olika rot-certifikat. En användare kan alltid medge tillit till varje certifikat eller rot-certifikat. Det kan emellertid bli betungande för användaren att hantera alla certifikat.

Det finns tre metoder till förfogande för att utvidga tillit från en certifikatutfärdare till en annan eller andra certifikatutfärdare, och där den senare metoden försöker hantera problemen som uppstår med den tidigare metoden: kors-certifikation, mesh-certifikat, bro-certifikatutfärdare.

Kors-certifikation (”cross-certification”) innebär att en certifikatutfärdare (X) utfärdar ett certifikat för en annan certifikatutfärdares (Y) certifikat eller rot-certifikat, samtidigt som den certifikatutfärdaren (Y) utfärdar motsvarande certifikat eller rot-certifikat till den första certifikatutfärdaren (X).

Problemet med denna metod är att det utfärdade certifikatet kan fortsätta ”kors-certifieras” mellan flera certifikatutfärdare, bortom vad som ursprungligen var tänkt av den första certifikatutfärdaren, samtidigt som användaren förväntas lita på att alla certifikat som inkluderats genom denna kors-certifiering är pålitliga. Det vill säga, om två certifikatutfärdare certifierar varandra kan den ena certifikatutfärdaren certifiera ytterligare en certifikatutfärdare som det andra certifikatutfärdares användare kommer att acceptera som en pålitlig certifikatutfärdare.

Det anses inte vara praktiskt att uppställa regler mellan certifikatutfärdarna i syfte att enbart ”vidare- kors-certifiera” under vissa omständigheter.

De andra två metoderna, mesh-certifikat och bro-certifikatutfärdare, försöker hantera problemet som uppstår med den första metoden, kors-certifikation.

Mesh-certifikat innebär att samtliga certifikatutfärdare måste certifiera varandra. Om två certifikatutfärdare certifierar varandra får den ena certifikatutfärdaren inte certifiera en ny certifikatutfärdare förrän den andra certifikatutfärdaren också certifierat den nya certifikatutfärdaren, och den nya certifikatutfärdaren måste i sin tur certifiera de andra två certifikatutfärdarna. Det betyder att det samtliga certifikatutfärdare måste certifiera alla andra certifikatutfärdare innan de släpps in i certifikatsnätverket. Problemet är att dessa typer av mesh-nätverk snabbt blir svårhanterliga eftersom certifikaten växer geometriskt när antalet certifikatutfärdare växer linjärt.

Den tredje metoden, bro-certifikatutfärdare, försöker hantera problemet med de två första metoderna, kors-certifikation och mesh-certifikat.

”Bro-certifikatutfärdare” (”Bridge CA”) är en central anknytningspunkt för samtliga certifikatutfärdare att certifiera sig mot genom att följa bro- certifikatutfärdarens regler. Bro-certifikatutfärdaren är inte en certifikatutfärdare som vänder sig mot användarna utan organiserar enbart certifikatutfärdarna (Digital Signatures [2002] s. 75-78; jfr a. 4.1.5, Öppna och slutna system„ juridiska hinder mot centrala lösningar).

4.2. Notarius publicus eller “Notary” [service]

En “notarius publicus” är en offentlig befattningshavare med bland annat uppgiften att bestyrka äktheten i avskrifter. Detta koncept kan omvandlas till digitala dataobjekt där en betrodd tredje part, vilket kan vara privat såväl som offentlig, kan ”stämpla”, logga, kvittera, verifiera och annars intyga att ett dataobjekt mellan en avsändare och mottagare är original och/eller inte har förändrats (Statskontorets rapport 2003:13 a. 3.9).

4.3. PKI

PKI (Public Key Infrastructure) eller “öppna nyckelsystemet” är ett system som inte har en klar definition men vissa kännetecken:

- utfärdandet av certifikatet är viktigt,
- distribution av certifikatet genom antingen en öppen katalogtjänst eller individuella utskick,
- möjlighet att spärra certifikat,
- kontrollmöjligheter av certifikatets status, exempelvis, kontrollera om den är spärrad,
- bestämt certifikatformat (Prop. 1999/2000:117 s. 22), samt,
- användarnas tillit till certifikatutfärdaren (Digital Signatures [2002] s. 53:1).

Infrastrukturen namnges efter metoden att organisera certifikatutfärdare, exempelvis, ”hierarkisk PKI”, ”kors-certifikation PKI”, och ”mesh PKI” (jfr a. 4.1.6.16, Tillitsmodeller för certifikat„).

Den grundläggande principen är att en fysisk eller juridisk person, genom certifikat, sammanbinds med ett ”nyckelpar” [hemlig och offentlig nyckel]. Infrastrukturen konstitueras i princip av certifikaten och certifikatutfärdarna, och den tillit användarna har för dessa.

En kontroll av att en elektronisk signatur härrör från rätt person innebär, förutsatt att signaturen validerades korrekt, att mottagaren eller den förlitande parten måste lita på att certifikatet som medföljde den offentliga nyckeln är giltigt. Certifikatet kan kontrolleras mot exempelvis spärrlistor, men i grunden handlar det om en tillit till att certifikaten utfärdats korrekt och säkert i syfte att den offentliga nyckeln hör ihop med en hemlig nyckel som tillhör den person som avses.

4.4. OpenPGP

http://openpgp.org/

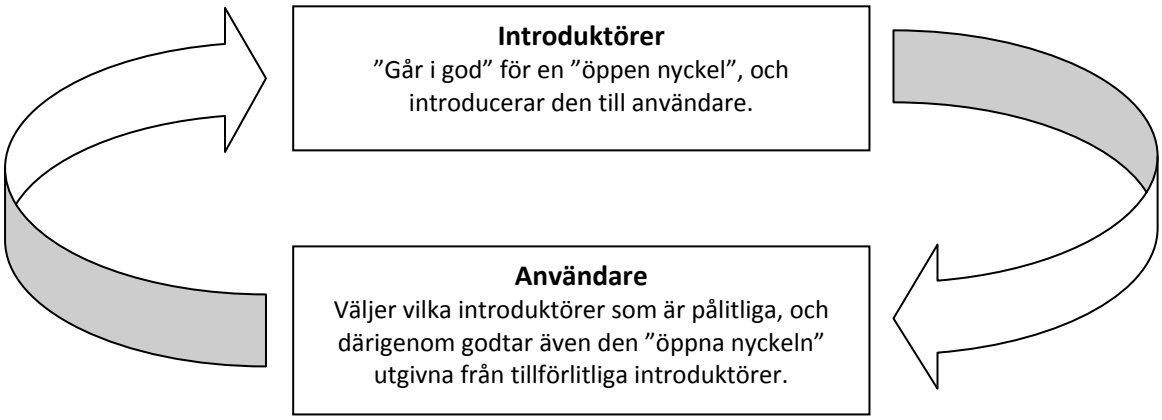
OpenPGP (Open Pretty Good Privacy) är en icke-proprietär krypteringsstandard som anger ett protokoll för kryptering av e-post-kommunikation, vilket omfattar format för krypterade meddelanden, signaturer och certifikat. Standarden är definierad i ”Förslag till standard RFC 4880” och utarbetat av ”OpenPGP” -arbetsgruppen i IETF (Internet Engineering Task Force).

OpenPGP ska inte sammanblandas med ”PGP” som är ett företags tillämpning av OpenPGP.

Tekniskt bygger standarden på asymmetrisk kryptering, och PKI eller “öppna nyckelsystemet (se a. 4.3, PKI), men under benämningen ”OpenPGP PKI” (istället för ”Certifikat PKI”) eftersom den tillämpar en ”web of trust” -arkitektur, istället för ”X.509” -formatet och centrala certifikatutfärdare; infrastrukturen är decentraliserad.

”Web of trust” är en tillitsmodell som PGP införde för att säkerställa att utställaren av en öppen nyckel faktisk är knuten till den som är utställt i signaturen (jfr a. 4.1.6.16, Tillitsmodeller för certifikat). Modellen bygger på konceptet av ”introduktörer” (eng. ”introducers”) som fungerar som ”certifikatutfärdare” i ”Certifikat PKI”.

En introduktör kan vara ”pålitlig” eller ”okänd”. En introduktör kan introducera en öppen nyckel, knutet till en specifik person, till sin bekantskapskrets. De i bekantskapskretsen som uppfattar introduktören som pålitlig kan acceptera att den öppna nyckeln tillhör den specifika personen som introduktören accepterat att nyckeln tillhör. En och samma öppna nyckel kan introduceras av flera olika introduktörer. Ju fler introduktörer som anses ”pålitliga” och introducerar nyckeln desto tillförlitligare blir den nyckeln. Olika användare kan ha tillit för olika introduktörer, och får avväga antalet pålitliga och okända introduktörer för att avgöra om nyckeln är tillförlitligt.



4.5. Federation

Vid framställningens skrivande [2013] var [är] utvecklingen av Federation i den planerade slutfasen. Detta avsnitt grundar sig i, och utgår från, det material som var [nu är] tillgängligt.

Federation, identitetsfederation, eller en federativ arkitektur, är en infrastruktur för teknisk, juridisk, och administrativ samordning och fördelning av ”funktioner” i ett ”system” (jfr Svensk e-legitimation s. 5). Federationsinfrastrukturen har lagts som grunden för ”Svensk e-legitimation” [systemet]. Funktionerna i federationen kan särskiljas som ”roller” och ”tjänster”. Rollerna är användare, arbetsgivare, attributsintygsutfärdare, attributssamordnare, [federations-] operatör, e-legitimationsutfärdare, leverantörer av eID-tjänster, tillhandahållare av e-tjänster. Tjänsterna är anvisningstjänst, tjänst för metadata, och underskriftstjänst (PM: Marknadsundersökning [2012] a. 5.2, Tjänster som är föremål för upphandling) samt attributstjänst.

Hela infrastrukturen för Svensk e-legitimation [”federationen”] består av en eller flera ”federationer” som opererar på en gemensam [offentlig] ”basstruktur”. En federation utgörs av en federationsoperatör och dess ”anslutande medlemmar”, det vill säga, de aktörer som har rollen som tillhandahållare av e-tjänster. Gentemot federationen opererar övriga aktörer i sina roller. Interaktionen mellan dessa aktörer samordnas tekniskt, juridiskt, och administrativt, dels genom basstrukturen och dels genom respektive federations operatör.

Det kan finnas flera federationer inom den privata sektorn, men den offentliga sektorn representeras av en federation. Den offentliga federationsoperatören har även ansvar för den gemensamma [offentliga] basstrukturen (Svensk e-legitimation, s. 10).

Syftet med federationen är *identifikation*; signering eller underteckning är en kompletterande funktion i federationen. Denna framställning kommer i huvudsak att avgränsa sig till funktionen som berör elektroniska signaturer, det vill säga, ”signatur- eller underskriftstjänsten” (se a. 4.5.3, Signeringstjänst, signaturtjänst och underskriftstjänst).

4.5.1. Federation i jämförelse med PKI

En federation kan ses som en organisatorisk infrastruktur, det vill säga, den samordnar och fördelar resurser i en specifik konfiguration, eller ett abstrakt lager för att förtydliga relationen mellan resurser. Det ”bakomliggande maskineriet” är avgränsad till varje funktion inom federationen. PKI i jämförelse kan ses som en teknisk infrastruktur som bygger på nyckelpar och där den organisatoriska infrastrukturen, det vill säga tillitsmodellerna, understödjer den tekniska grunden. Från detta perspektiv så kan en ”funktion” i en federation tillämpa PKI i det ”bakomliggande maskineriet”.

I en federation kan det exempelvis finnas en funktion som intygar identiteten av en undertecknare [identitetsutfärdare]. Hur denna identifikation hanteras internt av funktionen är en annan fråga; det kan exempelvis vara genom en ”PKI-lösning”. Funktionen som hanterar identifikationen av användare kan sedan anropas av andra funktioner inom federationen, exempelvis tjänstetillhandahållaren eller signeringstjänsten. En tjänstetillhandahållare kan exempelvis begära att användaren identifierar sig mot sin identitetsutfärdare, och från identitetsutfärdaren får ett identitetsintyg som bekräftar att användaren är den person som användaren påstår sig vara.

Likheterna mellan federation och PKI är att den part som ska förlita sig [förlitande part] på identifikationen måste i båda fallen lita på funktionen i federationen respektive att ett certifikat är giltigt och säkert. Skillnaden är att i federationssystemet gör inte den förlitande parten själv ett beslut om användarens identitet är korrekt, genom exempelvis en teknisk kontroll av certifikatet, utan istället förhåller sig till tillförlitligheten hos identifikationsfunktionen och antingen accepterar eller avvisar intyget från identifikationsfunktionen (jfr SOU 2009:86 s110).

Från ett juridiskt perspektiv uppstår vissa andra divergerade och sammanfallande punkter. Medan den rättsliga regleringen på området elektroniska signaturer omfattar PKI och inte ”federationer”, skulle en funktion inom federationen som hanterar elektroniska signaturer möjligtvis omfattas av samma regelverk (jfr SOU 2010:104 a. 3.7:3, ”Det är centralt för en svensk lösning att signaturlagens krav uppfylls.” jfr a. 2.1, Elektronisk och digital signering samt elektronisk underskrift.).

4.5.2. Identitetsintyg

Ett identifikationsintyg innehåller uppgifter om en användares identitet och juridiska behörighet, organisatoriska roll eller andra egenskaper [attribut]. Identitetsintyget levereras av eID-tjänsten i elektronisk form (Svensk e-legitimation s. 5-6; jfr a. 4.1.6.3, Attributauktoritet eller ”AA” (”Attribute Authority”)).

4.5.3. Signeringstjänst, signaturtjänst och underskriftstjänst

Medan ”underskriftstjänst” används i E-legitimationsnämndens arbeten kommer denna framställning att fortsätta använda ”signeringstjänsten” som i tidigare förarbeten. Denna term bör lämpligen vara mer korrekt eftersom en ”underskriftstjänst” inte är tänkt att vara begränsad till att enbart framställa ”elektroniska underskrifter”.

Tjänst för signering, signatur eller underskrifter är en kompletterande central-e-tjänst, men fråga om det är en nödvändig funktion i en offentlig federation (Svensk e-legitimation a. 7.1:1, ”Underskriftstjänsten bör närmast betraktas som en kompletterande e-tjänst snarare än en central komponent i federationen.”, jfr 7.2:1, jfr dock SOU 2010:104 a. 3.7:1, ”För att den beskrivna infrastrukturen ska bli fullständig behövs även en central tjänst för elektroniska underskrifter (signeringstjänst)”, och a. 5.5.3.).

Infrastrukturen för Svensk e-legitimation ska möjliggöra användandet av andra typer av e-legitimering i syfte att underteckna ett dataobjekt. Legitimationer som inte är ”PKI-orienterad”, exempelvis ”koddosor”, kan inte användas för att förse ett dataobjekt med en avancerad elektronisk signatur, och kan ha format som inte är vanligt förekommande eller accepterad (SOU 2010:104 a. 3.7:2). Idén är tillsynes att olika typer av e-legitimationer [”det bakomliggande maskineriet”] kan kanaliseras genom signaturtjänsten [”funktionen”] som kan framställa alla typer av elektroniska signaturer.

Mot bakgrund av a. 4.1.1 Förvaringsskyldighet,, 3.1 Program,, och diskussionen i SOU 2010:104 s. 72:3-4, rättsläget är oklart kring frågan om ”logisk kontroll” avseende förbud mot lagring och kopiering av signaturframställningsdata samt kontroll över den hemliga nyckeln uppfyller kraven i LKES och DES (jfr SOU 2010:104 b. 17 a. 4:4-5 jfr a. 4.1, om en signeringstjänst kan uppfylla kraven genom jämförelse med en lokal [fysisk] kontroll; jfr a. 4.1.6.10, Certifikat: Hemliga nycklar,, jfr a. 4.1.6.14, Certifikat: ”Roaming Credentials”,).

4.5.3.1. Certifikat

Signeringstjänstens certifikatfunktion ska utfärda ”kvalificerade certifikat”. Dessa certifikat utfärdas för *varje nyckelpar* och för *varje enskild signering*. Certifikatet får en särskild viktig betydelse eftersom den privata nyckeln från nyckelparet raderas efter signering; certifikatet är det enda som binder, och kan binda, användaren till signeringen genom identitetsintyget (se SOU 2010:104 b. 17 a. 12.2 Identitetsattribut).

Signeringstjänstens certifikatfunktion ska tillhandahålla allmän tillgänglig spärrinformation. Minimikravet är att upprätthålla en CRL (SOU 2010:104 b. 17 a. 12.3.1).

Signeringstjänstens certifikatfunktion kan tillhandahålla en certifikatverifieringsfunktion, via SAML (”Security Assertion Markup Language”), som en attributtjänst. Verifiering av ett certifikat sker genom en attributsförfrågan, tillsammans med användarens certifikat som ska verifieras, till certifikatfunktionen som svarar, om certifikatet är giltigt, med ett attributsintyg med användarens identitetsattribut (SOU 2010:104 b. 17 a. 12.3.2).

4.5.3.2. Möjliga tillvägagångssätt

I bilaga 17 till SOU 2010:104 beskrivs tre möjliga tillvägagångssätt för att tillämpa signeringstjänster som en funktion eller flera funktioner i federationen. Presentationen är hypotetisk och antar att signeringstjänsterna kan konkretiseras på ett liknande sätt.

Den gemensamma utgångspunkten är bland annat att signeringstjänsten ska fungera genom sedvanliga och allmänna system; dator, operativsystem, webbläsare (se vidare SOU 2010:104 b. 17 a. 5).

Alternativ 1 (central tjänst)

1. Användaren ”loggar in” med sin e-legitimation till e-tjänsten, och använder en tjänst som kräver en ”underskrift”.
2. Användaren dirigeras av e-tjänsten till signeringstjänsten.
3. Signeringstjänsten hämtar dataobjektet som ska signeras från e-tjänsten.
4. Signeringstjänsten presenterar dataobjektet som ska signeras, och att e-tjänsten vill att dataobjektet ska signeras.
5. Användaren kan bekräfta eller avbryta underskrift av dataobjektet.
6. Om användaren bekräftar att acceptera underskrift av dataobjektet:
    a. användaren dirigeras till tjänsten för legitimering hos sin identitetsutfärdare,
    b. genom att legitimera sig godkänner användaren samtidigt underskrift av dataobjektet.
7. Signeringstjänsten får ett identitetsintyg från identitetsutfärdaren.
8. Dataobjektet får en elektronisk underskrift av signeringstjänsten.
9. Användaren dirigeras tillbaka till e-tjänsten med bekräftelse att dataobjektet har signerats.
10. E-tjänsten hämtar det elektroniskt signerade dataobjektet från signeringstjänsten.

Alternativ 1 innebär att dataobjektet måste hanteras av tredje part, det vill säga, signeringstjänsten. Detta förutsätter **1(2)** att e-tjänsten får lämna ut dataobjektet till tredje part, samt **2(2)** att tredje part kan hantera och meningsfullt presentera dataobjektet för användaren endast med stöd av användarens webbläsare.

Alternativ 2 (central tjänst)

1. Användaren ”loggar in” med sin e-legitimation till e-tjänsten, och använder en tjänst som kräver en ”underskrift”.
2. E-tjänsten presenterar dataobjektet som ska signeras, och att e-tjänsten vill att dataobjektet ska signeras.
3. Användaren kan bekräfta eller avbryta underskrift av dataobjektet.
4. Om användaren bekräftar att acceptera underskrift av dataobjektet, e-tjänsten:
    a. beräknar dataobjektets hashvärde,
    b. skickar hashvärdet till signeringstjänsten, och
    c. dirigerar användaren till signeringstjänsten.
5. Signeringstjänsten dirigerar användare till identitetsutfärdaren för legitimering,
    a. genom att legitimera sig godkänner användaren samtidigt underskrift av dataobjektet.
    b. Användaren dirigeras tillbaka till signeringstjänsten.
6. Signeringstjänsten får ett identitetsintyg från identitetsutfärdaren.

7. Den elektroniska underskriften genereras med hashvärdet från e-tjänsten.
8. Användaren dirigeras tillbaka till e-tjänsten med bekräftelse att dataobjektet har signerats.
9. E-tjänsten sammanfogar dataobjektet tillsammans med underskriften och presenterar resultatet till användaren och bekräftar att dataobjektet har signerats.

Alternativ 2 innebär att signaturtjänsten krypterar hashvärdet [”signeringen”] och varken användaren eller e-tjänsten kan kontrollera hashvärdet *innan* krypteringen. Kontroll *efter* signering är möjlig förutsatt att signeringen kan verifieras. En hotbild är att, en bedräglig signaturtjänst krypterar ett annat hashvärde. Vidare innebär metoden att signeringstjänsten inte kan tidstämpla det signerade dataobjektet eftersom signeringstjänsten inte får tillgång till dataobjektet.

Alternativ 3 (lokal tjänst)

1. Användaren ”loggar in” med sin e-legitimation till e-tjänsten, och använder en tjänst som kräver en ”underskrift”.
2. Användaren dirigeras av e-tjänsten till signeringstjänsten.
3. Signeringstjänsten hämtar dataobjektet som ska signeras från e-tjänsten och överför den till användaren [lokala dator].
4. Användaren signerar dataobjektet med sin e-legitimation och en särskild applikation installerat på sin lokala dator.
5. Signeringstjänsten kontrollerar användarens identitet mot identitetsutfärdaren.
6. Användaren dirigeras tillbaka till e-tjänsten tillsammans med det signerade dataobjektet.

Alternativ 3 innebär **1(2)** att e-legitimationen måste vara baserad på certifikat, och **2(2)** verifiering av signatur är inte möjligt utan tillgång till svensk infrastruktur för identifiering, vilket försvårar för utländska aktörer.

Jämförelse mellan alternativ 1, 2 och 3 av vart funktionerna exekveras

FUNKTION	ALTERNATIV 1	ALTERNATIV 2	ALTERNATIV 3
Identifiering av användaren	e-tjänsten	e-tjänsten	e-tjänsten
Presentation av dataobjektet som ska signeras	signeringstjänst	e-tjänsten	lokalt
Beräkning av dataobjektets hashvärde	signeringstjänst	e-tjänsten	lokalt
Användare bekräftar att granskad dataobjektet ska signeras	signeringstjänst	e-tjänsten	lokalt
Identifiering av användaren inför signering	signeringstjänst	signeringstjänst	lokalt
Framställning av nyckelpar och utfärdande av nyckelcertifikat; radering av hemlig nyckel	signeringstjänst	signeringstjänst	-
Framställande av nyckelcertifikatutfärdarens certifikat	signeringstjänst	signeringstjänst	-
Generering av den elektroniska under-	signeringstjänst	signeringstjänst	lokalt

skriften [kryptering av hashvärdet]			
Tidstämpling av dataobjektet [vid begäran] 1. Beräkning av eller tillgång till hashvärdet av det dataobjekt som ska tidstämplas. 2. Generering av tidsinformation. 3. Signering av (1) och (2).	signeringstjänst / e-tjänsten / ”tidstämpelstjänst”	e-tjänsten / ”tidstämpelstjänst” / signeringstjänst (behöver i så fall tillgång till dataobjektet)	e-tjänsten / ”tidstämpelstjänst”
Sammanställning av slutprodukt: sammanfogning av dataobjektet och den elektroniska signeringen, tillsammans med certifikat och eventuell tidstämpel	signeringstjänst	e-tjänsten	signeringstjänst / e-tjänsten

4.5.3.3. Logg

Signaturtjänsten ska spara följande information.

- Samtliga begäran (”request”) och gensvar (”response”) som berör signeringen (se SOU 2010:104, b. 17, a. 10.4 Signing request och response).
- Hashvärdet av dataobjektet som har signerats.
- Signaturen [det krypterade hashvärdet].
- Certifikatet som skapades för det nyckelpar som signerade dataobjektet, samt certifikatet för de certifikatutfärdare som krävs för att verifiera nyckelcertifikatet (jfr SOU 2010:104, b. 17, a. 10.4 och 11:3 p. 3 och 11:6).
- Identitetsintyget från användarens accept av signering.

Däremot, ”[dataobjektet] som signerats och det signerade [dataobjektet] bör inte loggas” (SOU 2010:104, b. 17, 10.7).

Loggar ska förses med tillförlitlig och spårbar information om tiden kring händelseförloppen. Formatet ska vara ”UTC(SP)”.

4.5.3.4. Tillit

Frågan om tilliten till e-tjänster kräver en mer djupgående diskussion, men några faktorer som kan nämnas är följande.

Den huvudsakliga frågan bör vara vem man vill, bör och får, samt respektive negation, ta del av dataobjektet som signeras. Lokala kontra centrala tjänster konkurrerar.

Tjänster kan tillhandahållas av såväl offentliga som privata aktörer. Vem som är mer tillförlitlig för en privatperson kan grunda sig i exempelvis ekonomiska, politiska eller kunskapsmässiga faktorer, medan en myndighet kan förhålla sig till andra myndigheter och företag på andra grunder, såsom rättssäkerhet, förvaltningsrättsliga regler och offentlighetsprincipen.

Tillitsnivån påverkar huruvida man ”släpper in” en tjänstetillhandahållare till sin lokala miljö eller om man ”släpper ifrån” sig sin information.

4.5.4. Svensk e-legitimation

Svensk e-legitimation åsyftar dels ”själva legitimationen”, men begreppet inkluderar även andra koncept såsom Svensk e-legitimation som ett ”certifikat” eller ”stämpel” (Svensk e-legitimation, s. 6).

4.5.5. Öppet eller slutet system?

Fråga om federation utgör ett öppet eller slutet system har betydelse i förhållande till DES vilket uppsätter förbud mot system som är ”slutna” (a. 4.1.5, Juridisk reglering: Öppna och slutna system).

Utgångspunkten bör lämpligen vara att ”Federationen” som ett identifieringssystem faller utanför tillämpningsområdet för de lagar som reglerar elektroniska signaturer (jfr SOU 2009:86, s. 91:4-92:1).

Fråga om signeringstjänstens rättsliga betydelse som en tjänst inom federationen. I och med **1(3)** att signeringstjänsten omfattar elektroniska underskrifter, **2(3)** att elektroniska underskrifter inte är kvalificerade elektroniska signaturer, **3(3)** förbudet mot slutna system omfattar enbart kvalificerade certifikat [för kvalificerade elektroniska signaturer], bör lämpligen slutsatsen vara att frågan saknar vidare betydelse för denna framställning (jfr SOU 2010:104 a. 3.7:1, ambitionen är att de elektroniska underskrifterna *kan anses* kvalificerade).

5. Bevarande av elektroniska signaturer för en obestämd framtid

Det finns ett antal, och det kan tillkomma nya, metoder för att säkerställa att en elektronisk signatur bevaras för en obestämd framtid.[46] Detta avsnitt redovisar endast metoder som standardiserats, och inte teoretiska eller annars praktiska tillämpade metoder.[47] Avsnittet inkluderar även faktorer som kan äventyra elektroniska signaturers tillstånd för långtidsbevaring.

Bevarande av digitala objekt handlar i allmänhet om att bevara alla komponenter som datorn använt för att tolkat och omvandlat kod till det representerade dataobjektet, och tillgång till rätt hårdvara om dataobjektet är maskinberoende. Detta innebär att man kan återställa det digitala objektet i dess ursprungliga skick och mening, vilket förutsätter att komponenternas integritet inte äventyrats.

För elektroniska signaturer handlar emellertid det även om att bevara signaturens giltighet, det vill säga, att man kan validera inte bara integriteten av innehållet som signeringen avser, utan även vem som signerat innehållet.

Problemet med långtidsvalidering av elektroniska signaturer är att de komponenter som krävs för att validera signaturen dels inte är tillgängliga, eller tillgängliga mot en kostnad av tid eller pengar, och dels så småningom utgår med tiden (ETSI TS 102 778-4 V1.1.1 (2009-07), b. A, a. A.1; jfr Statskontorets rapport 2003:13 s. 44, giltighetstiden av nycklar och certifikat uppskattas till ungefär 20 år).

En elektronisk signatur är bevarad om och när dess autenticitet inte kan ifrågasättas eller äventyras. Det bör emellertid inte vara acceptabelt att anse en signatur som ogiltig även om dess nycklar och certifikat, efter en giltig tidpunkt, senare äventyrades. Det bör således vara tillräckligt att man kan visa att en signatur var giltig en gång i tiden [vid dess framställande] innan den återkallades eller upphörde att gälla (ETSI TS 101 733 V2.2.1 (2013-04) b. C, a. C.4.3; ETSI TS 101 903 V1.4.2 (2010-12) a. 7.3M; jfr Statskontorets rapport 2003:13 s. 40, ”En signatur som skapats med ett spärrat eller för gammalt certifikat går inte att lita på och har inget värde.”).

---

[46] Begreppet obestämd framtid används i samma mening som definierad i teoretisk PDF/A.

[47] Se exempelvis

- *Efficient long-term validation of digital signatures*, av Arne Ansper, Ahto Buldas, Meelis Roos, Jan Willemson, publiceringsdatum okänt men det digitala dokumentet var framställt 2001-05-16 <http://home.cyber.ee/~ahtbu/article/ABRW01.pdf > hämtat december 2013;
- Ds 2003:29 (*Formel Formkrav och elektronisk kommunikation*), a. 2.3.2, Långtidslagring av signaturer, man får förlita sig på säkerhetsrutiner och systemsäkerhetsåtgärder, t.ex. säker förvaring; jfr SOU 2002:78 (*Arkiv för alla – nu och i framtiden*), b. 2 (*Långsiktigt bevarande av digital arkivinformation*), s. 197, Riksarkivets tidiga digitala bevarandestrategi: konverteringsstrategi/migrationsstrategi; informationens äkthet säkerställde genom: standarder, hög datasäkerhet, rutiner för parallella bevarande linjer och av dataformat i original.

Signatären, verifieraren, eller båda, måste kunna bevisa

- att signaturen var skapad eller validerad under giltighetsperioden av alla certifikat som användes för signaturen, vilket kräver,
- att signatärens certifikat och certifikatutfärdarens certifikat som användes för att förse giltiga certifikat för signaturen, var giltiga (ETSI TS 101 733 V2.2.1 (2013-04) b. C, a. C.4.3; jfr ETSI TS 101 903 V1.4.2 (2010-12) a. 7.4; ETSI TS 102 778-4 V1.1.1 (2009-07) a. 4).

I likhet med bevarande av digitala objekt i allmänhet så måste alla komponenter som utgör den elektroniska signaturen bevaras, antingen genom omslutning eller hos en pålitlig källa (jfr ETSI TS 101 733 V2.2.1 (2013-04) b. C, a. C.4.6; jfr ETSI TS 102 778-4 V1.1.1 (2009-07), b. A, a. A.1).

Den elektroniska signaturen är avhängig två komponenter: den hemliga nyckeln och ”algoritmerna” [för beräkning av kondensat och kryptering]. Den hemliga nyckeln måste skyddas och får inte under några omständigheter riskera hamna i obehörig besittning, medan algoritmerna, som kan försvagas över tid, måste kunna ”uppdateras” (ETSI TS 101 733 V2.2.1 (2013-04) b. E, a. E).

5.1. Faktorer som kan påverka långtidsbevarandet av elektroniska signaturer

5.1.1. Beräkning av innehållets hashvärde

Fråga om vad hashvärdet representerar. Det kan vara binärdata och/eller teckenkaraktärer. Om hashvärdet genereras från teckenkaraktärer så är värdet beroende av teckenkodningen. Om teckenkaraktärerna vid signering använder en viss teckenkodning, så måste samma teckenkodning användas vid validering för att säkerställa att hashvärdet även förblir detsamma (jfr Statskontorets rapport 2003:13 a. 4.2, och s. 43).

5.1.2. Policy

ETSI TS 101 733 V2.2.1 (2013-04) b. C, a. C.1 Jfr ETSI TS 101 903 V1.4.2 (2010-12), a. 4.2 ETSI TS 101 903 V1.4.2 (2010-12), a. 7.2.3

En policy för signering kan ange de tekniska och/eller formella förutsättningar som krävs för att en signatur och/eller validering av en signatur ska vara giltig. Policyn underlättar att utfallet av valideringen förblir konsistent.

Policyn kan vara explicit definierad, exempelvis i formatet (jfr EPES -formaten), eller framkomma implicit i, exempelvis, innehållet av det som signeras eller externa hänvisningar till lagar, kontrakt eller avtalsvillkor.

En policy är bunden till signaturen och måste vara tillgänglig. Om policyn avser tekniska regler, såsom regler för framställande och validering av signatur, så måste den vara i en databehandlingsbar format. Om policyn avser formella regler så måste den vara i en mänskligt läsbart format.

Om ingen policy är definierad så kan man anta att signaturen framställdes utan några begränsningar, och i det sammanhanget saknar juridisk betydelse (ETSI TS 101 903 V1.4.2 (2010-12), a. 7.2.3).

5.1.3. Utbytningsattacker eller "substitution attacks"

ETSI TS 101 733 V2.2.1 (2013-04) b. C, a. C.3.3 ETSI TS 101 903 V1.4.2 (2010-12) a. 7.2.2

Utbytningsattacker mot certifikat kan uppkomma när ett antal olika certifikat är associerade med en och samma publika nyckel. Certifikaten kan gälla i olika sammanhang, exempelvis, ett certifikat intygar att den publika nyckeln tillhör en viss person i en organisation, medan ett annat certifikat intygar att den publika nyckeln tillhör samma person, men i privat egenskap. Det kan vara praktiskt att använda samma hemliga nyckel för olika funktioner.

Om certifikaten enbart bifogas en signatur så finns det en risk att certifikatet kan utbytas mot ett annat certifikat som anger att den publika nyckeln tillhör någon annan. Därför måste en "identifikation" om att certifikatet tillhör signatären omslutas i signaturen.

5.2. [Rekursiv] tidstämpling

En metod för att bevisa att information existerade före en viss tidpunkt är att tidstämpla informationen (ETSI TS 102 778-4 V1.1.1 (2009-07), b. A, a. A.1; Statskontorets rapport 2003:13 s. 45). Ju tidigare informationen tidstämplas desto bättre, eftersom tidstämplar på information efter giltighetsperioden för information har inget bevisvärde (ETSI TS 101 733 V2.2.1 (2013-04) b. C, a. C.4.3). Tidstämplar bör framställas med starkare algoritmer eller längre nyckellängder än den ursprungliga signaturen eller tidstämpeln [vid förnyelse av tidstämpel] (ETSI TS 101 733 V2.2.1 (2013-04) b. B, a. B.3, B.4).

Det ska betonas att den typ av tidstämplar som åsyftas här använder samma typ av teknologi som "vanliga signaturer", och dessa tidstämplar kräver i sin tur valideringsdata, vilka kommer så småningom även att utgå med tiden; därav behovet av rekursiv tidstämpling (ETSI TS 102 778-4 V1.1.1 (2009-07), b. A, a. A.1).

För en elektronisk signatur finns det två huvudsakliga komponenter som behöver tidstämplas:

- signaturen (att signaturen existerade vid en viss tidpunkt), samt
- certifikat och återkallelsedata, antingen omsluten eller genom hänvisning till dem (informationen som låg till grund för signaturen existerade vid en viss tidpunkt,[48] det vill säga, var giltig vid signering men sedermera kan ha blivit återkallad eller upphört

[48] CRL eller OCSP, och CARL -information (ETSI TS 101 733 V2.2.1 (2013-04) b. C, a. C.4.1, C.4.2).

att gälla) (ETSI TS 101 733 V2.2.1 (2013-04) b. C, a. 4.3-4.5; ETSI TS 101 903 V1.4.2 (2010-12) a. 7.4, 7.6.2).

Tidstämpeln kan avse var komponent för sig och, ytterligare tidstämpel för, allt tillsammans (att all information existerade samtidigt vid en viss tidpunkt). Rekursiv tidstämpling av alla komponenter kan utföras successivt efter behov för att säkerställa att informationen har förblivit oförändrat genom tiden.

5.2.1. CAdES

CAdES tillämpar två metoder för tidstämpling för långtidsbevarande,

- CAdES-X[49] tidstämpel av hela CAdES-C eller endast av alla hänvisningar till certifikat och återkallelsestatus, där i båda fallen alla certifikat och återkallelsestatus kan vara omslutna.
- CAdES-A[50] [rekursiv] tidstämpling av alla komponenter (se a. 5.2.2, Arkiv valideringsdata (CAdES-A, XAdES-A)).

5.2.2. PAdES

PAdES tillämpar en metod för långtidsbevarande,

- PAdES-LTV, omsluter all valideringsdata, och [rekursiv] tidstämpling av alla komponenter.

5.2.3. XAdES

XAdES tillämpar tre metoder för tidstämpling för långtidsbevarande,

- XAdES-X[51] tidstämpel av antingen signaturen, alla hänvisningar till certifikat och återkallelsestatus eller endast av alla hänvisningar till certifikat och återkallelsestatus,
- XAdES-X-L[52] omsluter alla certifikat och återkallelsedata,
- XAdES-A[53] [rekursiv] tidstämpling av alla komponenter (se a. 5.2.2, Arkiv valideringsdata (CAdES-A, XAdES-A)).

5.2.4. Arkiv valideringsdata (CAdES-A, XAdES-A)

ETSI TS 101 733 V2.2.1 (2013-04) b. C, a. C.4.5 ETSI TS 101 903 V1.4.2 (2010-12) a. 8.2

CAdES-A och XAdES-A är tilltänkt att tillämpa en enda metod för att bemöta samtliga scenarier av säkerhetshot, vilket underlättar hanteringen av alla eventuella säkerhetshot. Metoden kallas för ”Arkiv valideringsdata” (”Archive validation data”).

[49] CAdES-X bygger på CAdES-C.
[50] CAdES-A kan bygga på CAdES-BES, CAdES-EPES, CAdES-T, CAdES-C, CAdES-X.
[51] XAdES-X bygger på XAdES-C.
[52] XAdES-X bygger på XAdES-X Type 1 eller Type 2.
[53] XAdES-A bygger på XAdES-X-L.

Arkiv valideringsdata består av valideringsdata och fullständig certifikat och återkallelsedata tidstämplad tillsammans med signaturen. Detta är nödvändigt om algoritmen för hashvärdet och krypteringen äventyras. Om algoritmerna för tidstämplingen misstänks eller riskeras bli äventyrad så kan man tidstämpla rekursivt. Detta måste göras innan algoritmerna äventyras.

En säkerhetsåtgärd är att inte använda samma TSA för tidstämpling vid CAdES-A, som för tidstämplingen vid CAdES-T och CAdES-C; en säkrare TSA kan [bör] användas vid CAdES-A (ETSI TS 101 733 V2.2.1 (2013-04) b. C, a. C.4.8).

6. Riksarkivets perspektiv

Kommer att publiceras vid en senare tidpunkt.

7. Förteckning över källor

Förteckningen är upprättad efter alfabetisk ordning.

Departementspromemoria

Ds 1998:14, Digitala signaturer - en teknisk och juridisk översikt
Ds 2003:29, Formel Formkrav och elektronisk kommunikation

Näringsdepartementets promemoria av den 15/19 november 2012 (Myndigheternas tillgång till tjänster för elektronisk identifiering)

E-delegationen

Elektroniska original, kopior och avskrifter (2012-06-07)

PM – Marknadsundersökning, Marknadsundersökning avseende centrala tjänster för Svensk e-legitimation (2012-10-15)

E-legitimationsnämnden

Svensk e-legitimation, Modellbeskrivning, Version 2012-04-09

IETF

Information från http://tools.ietf.org/

ETSI

ETSI SR 003 232 V1.1.1 (2011-02), Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles (PAdES); Printable Representations of Electronic Signatures

ETSI TS 101 733 V2.2.1 (2013-04), Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)

ETSI TS 101 903 V1.4.2 (2010-12), Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)

ETSI TS 102 778-1 V1.1.1 (2009-07), Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES

ETSI TS 102 778-2 V1.2.1 (2009-07), Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1

ETSI TS 102 778-3 V1.1.1 (2009-07), Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles

ETSI TS 102 778-4 V1.1.1 (2009-07), Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES-LTV Profile

ETSI TS 102 778-5 V1.1.1 (2009-07), Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 5: PAdES for XML Content - Profiles for XAdES signatures

EU-kommissionen

Kommissionens Beslut (2009/767/EG) av den 16 oktober 2009

OpenPGP

Information från http://openpgp.org/

Proposition

Proposition 1999/2000:117, Lag om kvalificerade elektroniska signaturer, m.m.

Riksarkivet

ArkivE, Val av format för elektroniska kontorsdokument
Rapport 1999:1, Om gallring - från utredning till beslut
Rapport 2000:1, Elektronisk dokumenthantering [Lagerlöf & Leman]
Rapport 2006:1, Elektroniskt underskrivna handlingar

RSA

Information från http://www.emc.com/emc-plus/rsa-labs/

Mohan Atreya, Benjamin Hammond, Stephen Paine, Paul Starrett, Stephen Wu, *Digital Signatures*, RSA Press, 2002

Skatteverket

Information från http://skatteverket.se/

RSV M 2003:24, Grundläggande riktlinjer för myndigheternas användning av e-legitimationer och elektroniska underskrifter

Statens offentliga utredningar

SOU 1996:40, Elektronisk dokumenthantering
SOU 2002:78, Arkiv för alla – nu och i framtiden
SOU 2009:86, Strategi för myndigheternas arbete med e-förvaltning
SOU 2010:104, E-legitimationsnämnden och Svensk e-legitimation

Statskontoret

Rapport 2003:13, Elektroniska urkunder

W3C

Information från http://www.w3.org/

Wikipedia

Artikel ”Digital signature”
Artikel ”Electronic signature”
Artikel ”PKCS”

Övrig litteratur

Arne Ansper, Ahto Buldas, Meelis Roos, Jan Willemson, *Efficient long-term validation of digital signatures*, publiceringsdatum okänt men det digitala dokumentet var framställt 2001-05-16