Riksarkivet

Rapport

Författare	Avdelning	Telefon	Datum	Version	Sida
Benjamin Yousefi	DOI	010-476 72 98	2015-05-29	1.0	1 (22)
Projekt *Arkiv E - Delprojekt 3: Framställning och bevarande av elektroniska signaturer (avsnitt 6)*	Noteringar Direktiv DOI 2013:1 Dnr RA 20-2013-1154				

Arkiv E - Delprojekt 3: Framställning och bevarande av elektroniska signaturer (avsnitt 6)

Riksarkivet

Rapport

Författare	Avdelning	Telefon	Datum	Version	Sida
Benjamin Yousefi	DOI	010-476 72 98	2015-05-29	1.0	2 (22)
Projekt *Arkiv E - Delprojekt 3: Framställning och bevarande av elektroniska signaturer (avsnitt 6)*	Noteringar Direktiv DOI 2013:1 Dnr RA 20-2013-1154				

Innehållsförteckning

1. Inledning

Denna framställning är det ”sjätte avsnittet” i det tidigare utgivna dokumentet Framställning och bevarande av elektroniska signaturer publicerad 7 oktober 2014 (version 1.3) [huvudframställningen], vilket denna framställning utgår från, kompletterar, och ska läsas i anslutning till.

1.1. Avgränsning

Detta avsnitt utgår från och grundar sig i huvudframställningens fem första huvudavsnitt. Direkta hänvisningar i detta avsnitt till huvudavsnitten kommer enbart att göras i undantagsfall. Begrepp och förkortningar definierade i huvudavsnitten kommer inte att åter definieras i denna framställning. Diskussioner och problemformuleringar i detta avsnitt görs mot bakgrund av bland annat frågor och praktiska problem som presenterats eller tagits upp vid möten eller samtal med olika myndigheter, och under konferenser, seminarium och i workshops.

1.2. Definitioner

1.2.1. Digital

Med ”digital” åsyftas specifikt hur data representeras och lagras i binär form [representerad av ”ettor och nollor”]. Användandet av ”digital” syftar till att lyfta fram att informationen är i centrum, och inte, tillskillnad från ”elektroniskt”, ett medium eller förfarandesätt.[1] Bevarande av digitala objekt avser bevarandet av binär data, vilka kan bearbetas och lagras elektroniskt eller med andra teknologier.

Med en ”digital allmän handling” åsyftas alltså en allmän handling som är representerad i binär form.

1.2.2. Digital signatur och elektronisk signatur

Uttrycket ”elektronisk signatur”[2] är den formella benämningen i svensk och EU-rätt till motsvarigheten av ”egenhändig underskrift” i digital miljö.

Rättsligt innebär en elektronisk signatur helt enkelt ”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” (LKES § 2).[3] En elektronisk

1 Jfr Svenska Datatermgruppen, c/o TNC. Ordlisteartikel 243. <datatermgruppen.se> 20140410.

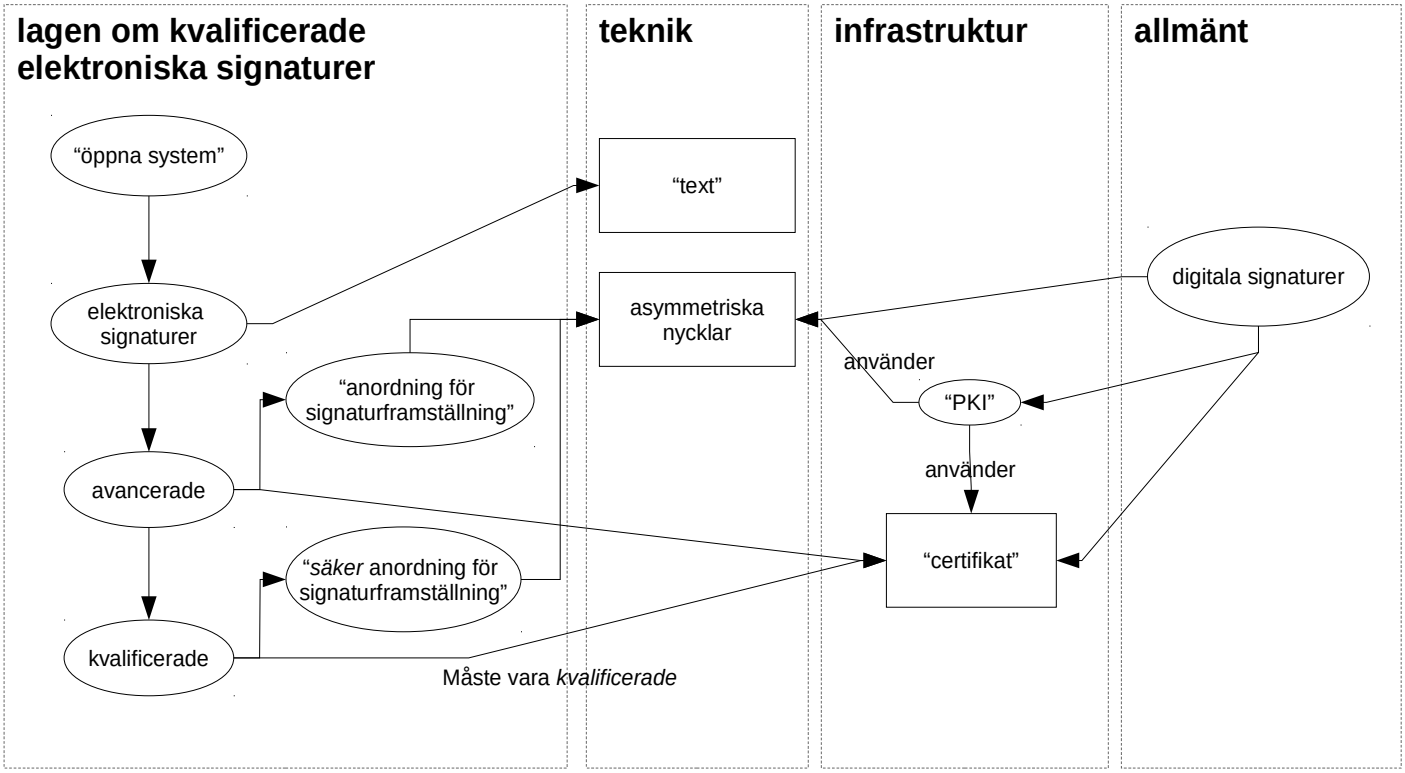
2 Förordning 910/2014 (EU) använder numera uttrycket ”underskrifter” istället för ”signaturer”, men begreppsinnehållet verkar vara detsamma, se vanliga frågor och svar om elektroniska signaturer på riksarkivet.se/elektroniskasignaturer.

3 Jfr Förordning 910/2014 (EU) artikel 3.10 ”[E]lektronisk underskrift: uppgifter i elektronisk form som är fogade till eller logiskt knutna till andra uppgifter i elektronisk form och som används av undertecknaren för att skriva under.”

signatur har tolkats omfatta allt från att skriva sitt namn i anslutning till en text såsom ett e-postmeddelande eller annat dokument, till att använda kryptografiska teknologier såsom asymmetriska nycklar.

Hur en elektronisk signatur framställs tekniskt har betydelse för bedömningen av hur signaturen ska kvalificeras i ett rättsligt förfarande. Eftersom elektroniska signaturer kan framställas på olika sätt används olika uttryck för tekniska implementeringar av elektroniska signaturer för att uppfylla olika rättsliga krav. Elektroniska signaturer kan förenklat sägas var det mest grundläggande sättet att signera ett dataobjekt. Det finns två rättsligt definierade metoder för att framställa mer tillförlitliga typer av elektroniska signaturer: ”avancerade elektroniska signaturer” och ”kvalificerade elektroniska signaturer”. Dessa metoder kan förenklat sägas grunda sig i användandet av PKI. Vad som utgör en elektronisk signatur är därmed rättsligt reglerat, men det tekniska förfarandet är emellertid inte reglerat, det vill säga, dels att lagen är tänkt att vara teknikneutral, dels att samma teknologi som används för elektroniska signaturer kan användas i andra sammanhang för andra syften utan att lagen om elektroniska signaturer blir tillämplig.

Illustrationen nedan åsyftar att belysa skillnaden mellan tekniken och begreppen; samma teknologi kan ligga till grund för såväl elektroniska som digitala signaturer, asymmetriskt krypterade kondensat-värden kopplade till certifikat, men för elektroniska signaturer finns närmare krav på *hur* man framställer signaturen och certifikaten.



extremt förenklat: syftet är att visa skillnaden mellan tekniken och begreppen

Problemet är emellertid att genom att använda uttrycket ”elektroniska signaturer”, särskilt inom myndighetsverksamheter, kan en diskussion om teknologin sammanblandas med den rättsliga regleringen. En skillnad måste därför göras mellan elektroniska signaturer och den teknologi som kan användas för att skapa elektroniska signaturer. Detta kan förstås som en skillnad mellan vad som kvalificeras som en elektronisk signatur och hur man framställer en sådan signatur.

Uttrycket ”digitala signaturer” åsyftar vanligtvis användningen av asymmetriska nycklar för att kontrollera att information omanipulerat härstammar från en hemlig nyckel. Tillsammans med certifikat eller kvalificerade certifikat kan digitala signaturer ses som ett sätt att framställa avancerade respektive kvalificerade elektroniska signaturer. En elektronisk signatur har med andra ord att göra med den rättsverkan en åtgärd i digital miljö medför, medan en digital signatur är en metod att säkerställa utställare och integritet. Det är därför viktigt att tydliggöra vad som åsyftas med [elektroniska eller digitala] ”signaturer” vid en diskussion.

2. Bevarande av elektroniska signaturer

Bevarandet av elektroniska signaturer innebär i princip detsamma som bevarandet av dataobjekt i allmänhet; bevara alla komponenter som behövs för att en dator ska tolka och återge ”informationen” som ett dataobjekt ursprungligen representerade i syfte att man vid en senare obestämd tidpunkt ska kunna återställa dataobjektets information i dess ursprungliga skick och mening, vilket förutsätter att komponenternas dataintegritet inte har äventyrats, det vill säga, att alla komponenter som utgör den elektroniskt signerade allmänna handlingen är i ursprungligt skick, och därav är den elektroniskt signerade allmänna handlingen i ursprungligt skick.

Bevarandet av elektroniska signaturer innebär alltså förenklat att det elektroniskt signerade dataobjektet såväl som signaturen ska bevaras.

3. Bevarande av elektroniska signaturers giltighet

En skillnad måste göras mellan att bevara en signatur som den var och att bevara att signaturen var/är giltig. Det innebär alltså att bevarandet av en elektronisk signatur i ursprungligt skick inte innebär att signaturens giltighet har bevarats, det vill säga, att signaturen var giltig.

Problemformulering kan utgå från ett antagande att ett dataobjekt är bevarat i ursprungligt skick, det vill säga, att dataobjektet inte på något sätt har förändrats eller förvanskats. Ett dataobjekt består av en konstellation av ”ettor och nollor” [binär data]. Ettor och nollor skapade eller ändrade från/vid en tidpunkt skiljer sig inte från ettor och nollor skapade eller ändrade till/vid en annan tidpunkt. Det följer av detta att bevis på att dataobjektet inte har förändrats eller förvanskats kräver någon form av oberoende referensstruktur som validerar antagandet att dataobjektet inte på något sätt har förändrats eller förvanskats.

Valideringen av en elektronisk signatur, det vill säga kontrollen att signaturen är giltig, är således

beroende av en ”yttre legitimitet”. En bristande liknelse är att jämföra med en handskriven underskrift som kan kontrolleras med någon typ av identitetshandling såsom ett ID-kort eller pass, och där andra faktorer kan påverka kontrollen, såsom särskilda markeringar i dokumentet eller pappret.

Bevarandet av den elektroniska signaturens giltighet utgår därför från samma principer som bevarande av den elektroniska signaturen, men därutöver ska även signaturens giltighet eller ”äkthet” i rättslig mening bevaras, det vill säga, att signaturen omanipulerad härrör från den som framstår som utställare. Detta innebär förenklat att bevara all information och alla komponenter, det vill säga *valideringsdata*, som kan bevisa att den elektroniska signaturen är giltig, det vill säga *validerar* den elektroniska signaturen.

Två tillvägagångssätt har observerats för att bevara giltigheten av en elektronisk signatur. Den ena metoden är ”rekursiv tidsstämpling”, medan den andra metoden kan förenklat beskrivas som ”systemberoende”. Oavsett vilken metod man tillämpar uppstår två för båda metoderna gemensamma frågor: **(1)** vilka är komponenterna man måste bevara för giltigheten?, och **(2)** hur bevarar man komponenterna?

3.1. Komponenter

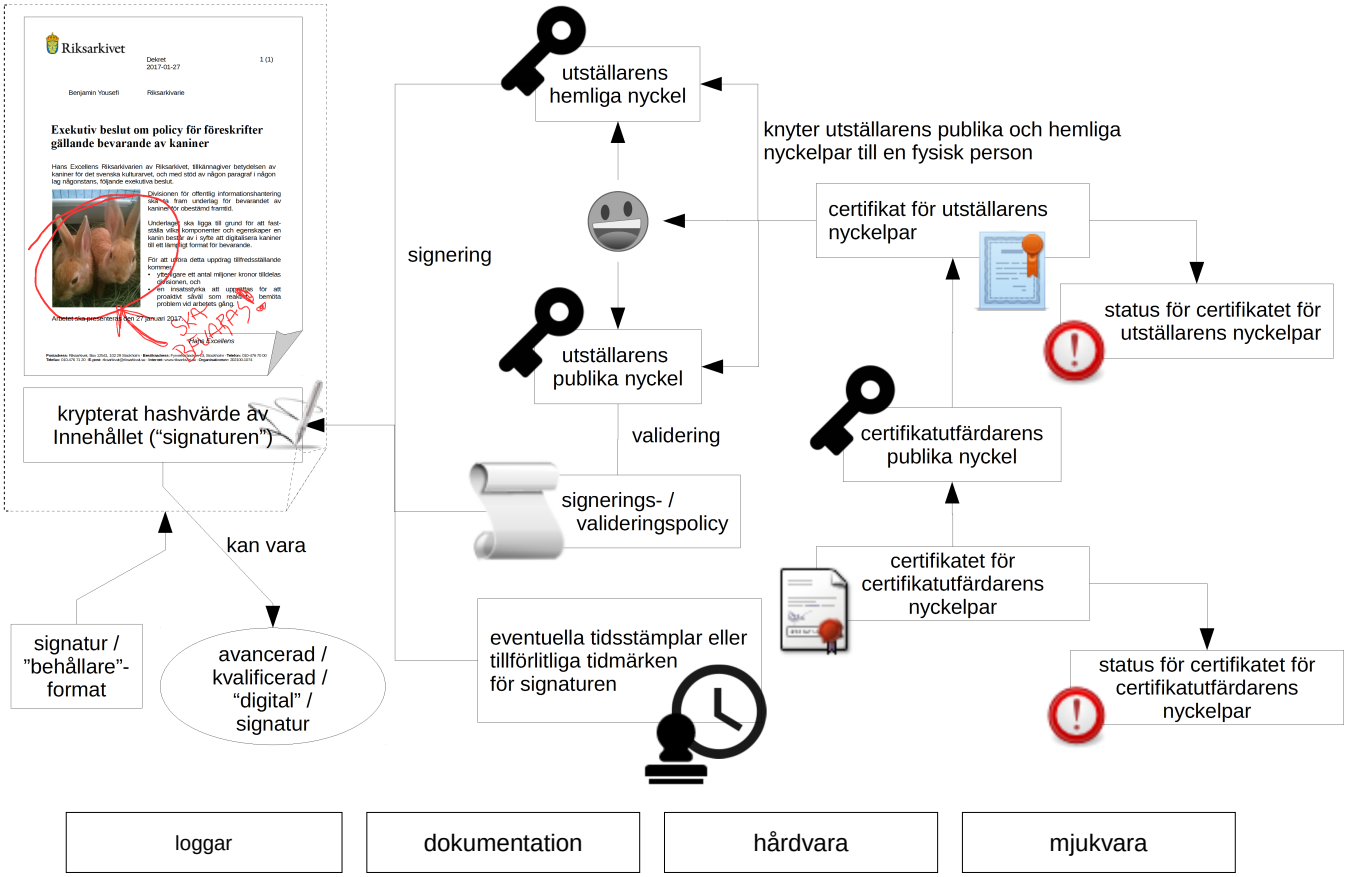
De komponenter som kan aktualiseras enligt ETSI -standarden för långtidsbevarande av giltigheten av en signatur är följande:

- utställarens publika nyckel (korresponderar med utställarens privata nyckel)
- certifikatet för den publika nyckeln som knyter utställarens hemliga nyckel till en fysisk eller juridisk person,
- status om certifikatet för den publika nyckeln var giltigt vid signeringstidpunkten, det vill säga, att den inte var upphävd eller återkallad,
- certifikatet för certifikatutfärdarens certifikat som knyter certifikatutfärdaren till den publika och hemliga nyckeln som användes för att certifiera [signera] certifikatet för utställarens certifikat,[4]
- status om certifikatet för certifikatutfärdarens certifikat var giltigt vid signeringstidpunkten, det vill säga, att den inte var upphävd eller återkallad,
- tillförlitlig tidsstämpel eller tidmärke för signaturen, och,

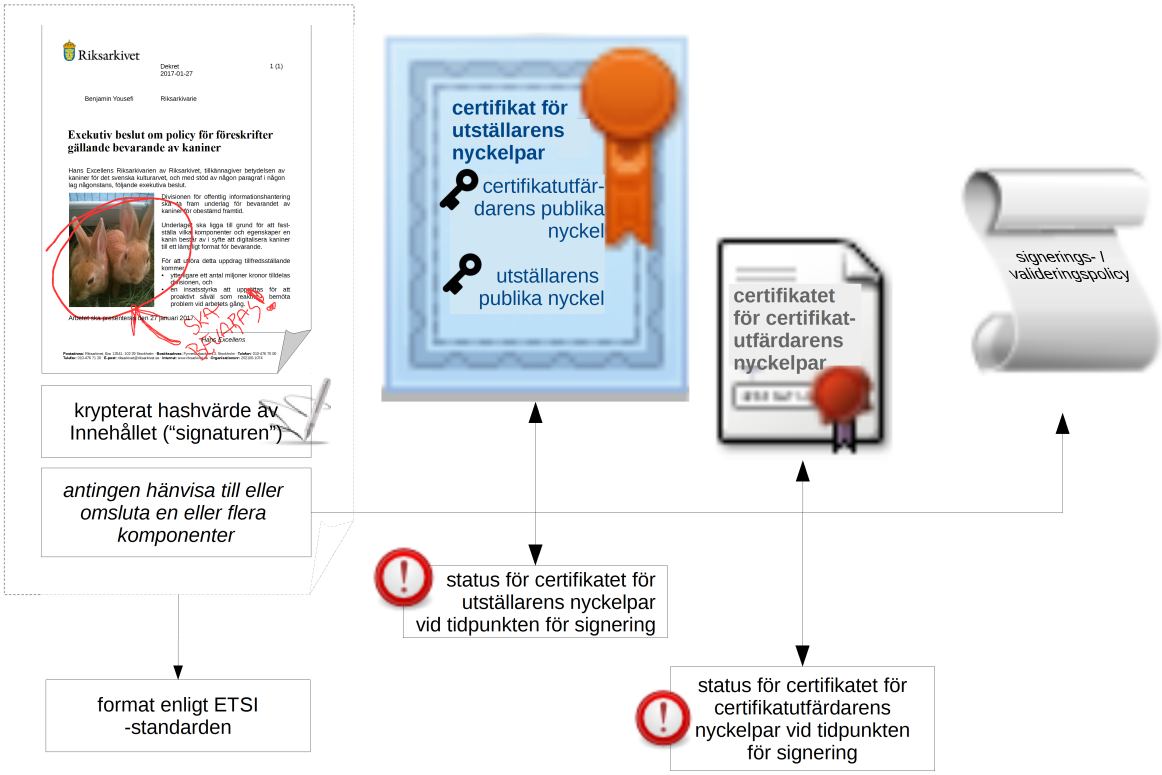
4 Det ska noteras att det kan finnas fler certifikatutfärdare i denna kedja, det vill säga, att för varje certifikat finns en certifikatutfärdare, och om certifikatutfärdaren inte använder ett ”rot-certifikat” utan förlitar sig på en annan certifikatutfärdares certifikat, kan den certifikatutfärdarens certifikat vara erforderlig (se tillitsmodeller för certifikat i huvudframställningen).

- policyn, om tillämpligt, för valideringsprocessen av signaturen.

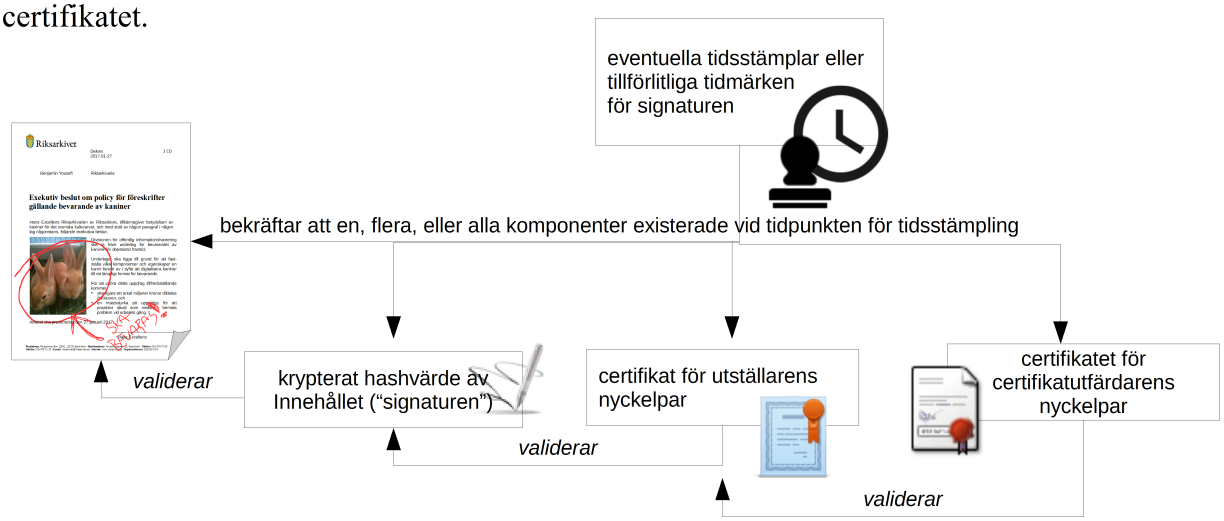
Nedan illustreras ett förenklad flödesschema över hur komponenterna förhåller sig till varandra.



Nedan illustrera vilka komponenter som måste bevaras, antingen genom att omslutas eller hänvisas till, för långtidsbevarandet av signaturens giltighet.



Förenklat handlar det om att komponenterna kan visa **(1)** att signaturen tillhörde den fysiska eller juridiska person som är angiven som utställare, och **(2)** att den som certifierat att signaturen tillhörde den fysiska eller juridiska person som är angiven som utställare var behörig att utfärda certifikatet.

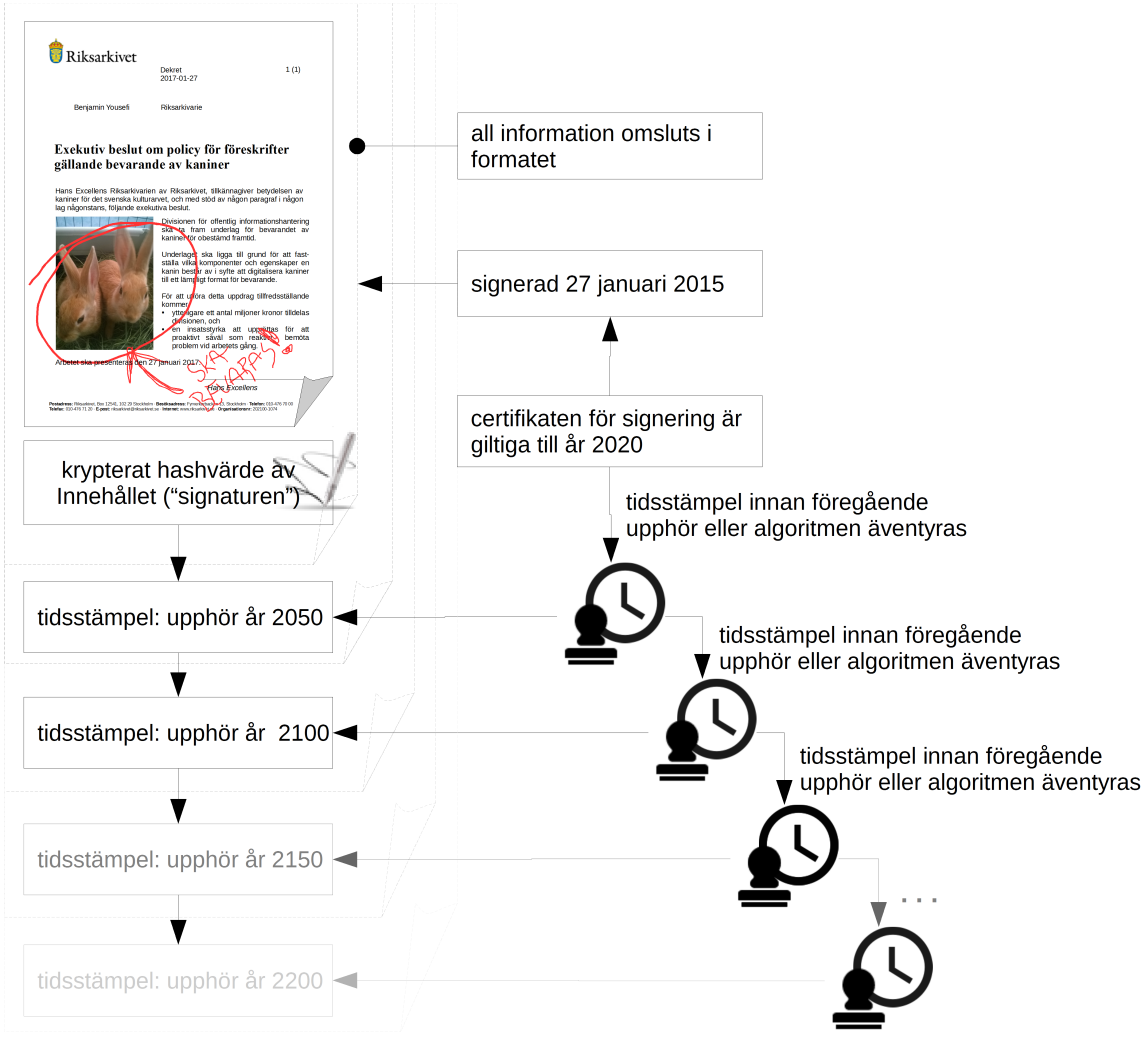


3.2. *Rekursiv tidsstämpling*

Rekursiv tidsstämpling redovisas i huvudframställningens avsnitt 3 och 5, här kommer enbart tankar kring metoden för långtidsbevarandet av en signaturs giltighet att diskuteras.

Metoden innebär förenklat att man kan visa att en signatur var giltig en gång i tiden, innan den upphörde att vara giltig, genom att bevara signaturen och alla komponenter som användes för validera signaturen (se a. 3.1, *Komponenter*). Detta kräver att man även kan visa att alla komponenter var giltiga en gång i tiden, innan de upphörde att vara giltiga, vilket uppnås genom att tidsstämpla [”signera”] alla komponenter.

Tidsstämpeln, vilken i princip använder samma teknologi som signaturer, lider emellertid av samma problem – den är giltig för en viss period och kommer med tiden att upphöra att vara pålitlig. Detta kräver att tidsstämpeln i sin tur måste ”omstämplas” med jämna mellanrum, det vill säga, rekursiv tidsstämpling. Slutresultatet är en ”kedja” av tidsstämplar som man kan följa för att utreda om en signatur var giltig en gång i tiden.



Tidsstämpeln kan avse var komponent för sig och/eller, ytterligare tidsstämpel för, alla komponenter tillsammans i syfte att visa att alla komponenter existerade samtidigt vid tidpunkten för signering.

Fördelen med rekursiv tidsstämpling, från ett bevarandeperspektiv, är att det är möjligt, även om inte nödvändigt, att omsluta alla komponenter som används vid valideringen av signaturen i ett och samma dataobjekt. Från ett rättsligt och tekniskt perspektiv är fördelen att det finns en standardiserad process för format för användandet av rekursiv tidsstämpling, ETSI -standarden, vilken dels är ett europeiskt initiativ, dels syftar till att uppfylla kraven i gällande rätt för elektroniska signaturer.

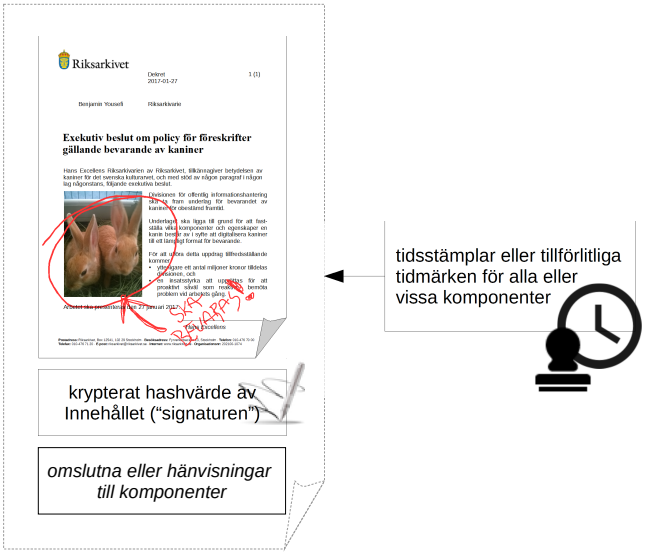
Nackdelar med rekursiv tidsstämpling har inte påträffats, men det bör tillsynes röra sig om administrativa och organisatoriska problem som kan uppstå, som exempelvis,

- det krävs att det finns rutiner för tidsstämplingen med jämna mellanrum, och särskilt innan en tidigare tidsstämplings säkerhet äventyras,

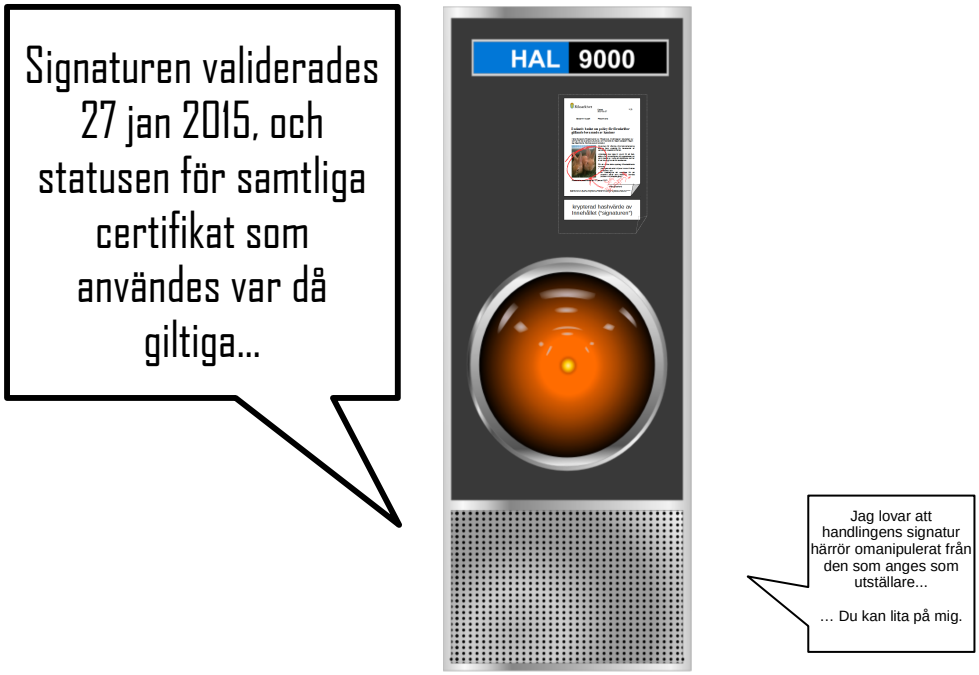
- en rekursiv tidsstämpling kommer troligtvis att växa i storlek, och om alla komponenter ska bevaras för varje handling, och det rör sig om ett stort antal handlingar, kan lagringen ta en betydande plats,

- ska komponenter som används för flera handlingar, såsom certifikatutfärdarens certifikat, bevaras separat och länkas till samtliga handlingar så gäller det att dessa kan tillgängliggöras för de handlingar som behöver dem när exempelvis handlingen ska lämnas ut. Problemet här är att i allmänhet när komponenter separeras så finns det en risk för att sambandet mellan komponenterna äventyras, med följd att det inte senare går att återförena alla komponenter.

Det finns även andra frågor som kan vara av intresse att närmare diskutera, såsom fråga om hur man bedömer ett fall där ”kedjan” bryts efter en viss tid, exempelvis 50 år, eller med andra ord, hur länge behöver man tidsstämpla?



3.3. Systemberoende



Systemberoende metoder har inte redovisats i huvudframställningen utan utgår från befintliga metoder som används för att i allmänhet säkerställa att ett dataobjekt inte otillåtet förändrats. Med ”systemberoende” åsyftas exempelvis tekniska[5] och/eller systematiska åtgärder[6] som tillsammans skapar ett system som kan validera ett dataobjekt genom att säkerställa att det dataobjektet inte har förändrats och att dataobjektet isolerats sedan omhändertagande.[7] Detta kan exempelvis vara att man arkiverar ett elektroniskt signerat dokument i ett system för bevarande [”e-arkiv”].

En signaturs tillförlitlighet är beroende av de komponenter som redovisats i a. 3.1, *Komponenter*. Två frågor som blir aktuella avseende systemberoende åtgärder är: **(1)** kan dessa komponenter säkras för lång tid genom ett system?, och **(2)** kan informationen ersättas och/eller representeras på annat sätt genom att man använder ett system?

Den första frågan avser att istället för att använda rekursiva tidsstämplar så bevarar man alla komponenter i ett system som exempelvis har behörighetskontroll, säkerhetskopior, och loggar/spårbarhet. Frågan är emellertid vilka åtgärder som är nödvändiga för att ett sådant system ska anses som mer eller mindre tillförlitligt; är exempelvis hashkontroller nödvändiga?

5 Såsom behörighetskontroll, hashkontroller, loggar.
6 Med systematiska åtgärder åsyftas en konsekvent kvalitetssäkring av information, exempelvis, planlagda åtgärder, arbetsrutiner, säkerhetskontroller.
7 För att exempelvis förhindra utbytningsattacker eller andra typer av attacker.

Fördelen med en systemberoende lösning är att den möjligtvis kan vara mer lätthanterlig än tillämpningen av rekursiva tidsstämplar.

Från ett långtidsperspektiv finns emellertid andra problem. För att bevara dataobjektet så måste man bevara allt det kringliggande och alla de understödjande delarna som utgör systemet; bevarandet av dataobjektet innebär rent faktiskt att man även måste bevara systemet. För att återställa dataobjektet måste hela systemet fungera i ursprungligt skick. Under en längre tid kan det hända att insikten i systemet med tiden faller i glömska, exempelvis på grund av dåligt underhåll eller nedläggning av myndigheten. Detta innebär att för att bedöma tillförlitligheten i systemet kan det behövas en genomgång av dokumentation och kod; någon måste se över och tolka systemet för att förstå hur man återställer och validerar dataobjekten i systemet.

Ett systemberoende tillvägagångssätt kan möjligtvis även göra det svårt att leverera ett signerat dataobjekt om dess giltighet är uteslutande beroende av systemet, det vill säga, att signaturen kan inte valideras utanför systemet.

Den andra frågan avser problemen med att försöka bevara alla komponenter som är nödvändiga för långtidsbevarandet av elektroniska signaturer. I praktiken kan det vara svårt att exempelvis inhämta och bevara status om certifikatets säkerhetstillstånd. Det finns två aspekter av denna fråga. Den ena är om det är möjligt att exempelvis notera i dataobjektets metadata att alla komponenter var giltiga vid validering eller att myndigheten ”stämplar” dataobjektet efter att ha validerat den elektroniska signaturen, medan den andra handlar om det är möjligt att efter att man har validerat en signatur en gång kan bevara och hänvisa till den bedömningen i framtiden.

Båda aspekterna är diskutabla. Den andra aspekten är emellertid problematisk. Frågan är om det går att bevara en *bedömning* om att något var äkta? Antagandet är att en bedömning är en värdering som görs vid varje tillfälle. Slutsatsen av en bedömning kan bevaras, men den slutsatsen måste bedömas vara tillförlitlig vid ett annat tillfälle. Det handlar inte bara om själva slutsatsen är ”äkta”, det vill säga att den inte är exempelvis förfalskad, men även om samma slutsats skulle dras vid ett senare tillfälle. Om grunden för den bevarade slutsatsen har gallrats eller inte längre är tillgänglig så kan man inte göra några nya bedömningar mot bakgrund av att någon ifrågasätter den ”godkända slutsatsen”.

I slutändan innebär ett systemberoende tillvägagångssätt att det är myndigheten som ”går i god” för att signaturen och dess komponenter är äkta, vilket under vissa omständigheter kan uppställa frågor om rättssäkerhet.

3.4. Notariatssystem

Det ska kort nämnas något om idén att etablera ett ”informationsvalv” eller ”archivum” i romersk mening, det vill säga, ”*pålitliga* digitala arkiv som, i likhet med gamla tiders arkiv, kan garantera informationsinnehållet utan krav på sigill och signaturer.” (betoning i original) (Statskontorets

rapport 2003:13 a. 6.2).

Riksarkivet skulle i detta sammanhang, förenklat beskrivet, kunna fungera som exempelvis en databas som allmänheten och andra myndigheter kan verifiera kondensatet av allmänna digitala handlingar, genom exempelvis ett webbgränssnitt.

4. Modell för analys och värdering

Från Riksarkivets perspektiv är bevarandet av den digitala allmänna handlingens dataintegritet[8] av väsentlig betydelse, det vill säga, att den digitala allmänna handlingen har bibehållit sitt ursprungliga skick.

4.1. Bakgrund

Riksarkivet har yttrat sig i remiss över betänkandet SOU 2010:104 (E-legitimationsnämnden och Svensk e-legitimation) och Näringsdepartementets promemoria av den 15/19 november 2012 (Myndigheternas tillgång till tjänster för elektronisk identifiering) om upprättandet av en svensk Federation.

De problem Riksarkivet uppmärksammat i sina yttranden, relevant för denna framställning, kan sammanfattas som följande.

- Fråga om vad som utgör allmänna handlingar.
- Fråga om att säkerställa, juridiskt och praktiskt, långsiktigt bevarande av allmänna handlingar.
- Fråga om ansvaret för allmänna handlingar och gallring.

Riksarkivets uppfattning är att för att besvara frågeställningarna som uppstår måste först utredas en kartläggning av handlingsflödet och ansvaret för handlingar i infrastrukturen.

4.2. Frågeställningar

Fyra frågeställningar har uppställts, i förslagsvis ordning, för att bryta ner den övergripande problematiken vid bedömning av bevarandet av en elektronisk signatur.

1. Vilka komponenter avgränsar och fixerar samt kan autentisera, eller validera, den elektroniska signaturen?
2. Vilka komponenter är relevanta; nödvändiga, tillräckliga eller önskvärda för signaturen och giltigheten av signaturen?

8 Uttrycket dataintegritet har införts och används istället för uttrycket autenticitet, men med samma begreppsinnehåll; i ett arkivrättsligt sammanhang åsyftar vanligtvis autenticitet att en handling har bibehållit sitt ursprungliga skick, exempelvis, i Riksarkivets föreskrifter används uttrycket ”autenticitet” i nämnda bemärkelse. Syftet med att använda dataintegritet istället för autenticitet är att undvika begreppsförväxling med autenticitet i ett rättsligt sammanhang.

3. Vilka komponenter är allmänna handlingar; om komponenten är en allmän handling: fråga om gallring; om komponenten inte är allmän handling: fråga om åtgärder för att säkerställa komponenten.

4. Hur ska komponenterna bevaras?

4.3. Exempel på tillämpning av modellen

Se även *Framställning och bevarande av elektroniska signaturer – en praktisk vägledning*.

Mot bakgrund av framställningens huvudsakliga behandlingsområde konkretiseras kartläggningen av elektroniskt signerade dataobjekt med i kontexten ”federationen”.[9]

Medan federation inte nödvändigtvis behöver vara begränsat till användandet av PKI eller ett certifikatsystem, så har förarbetet till federation (SOU 2010:104) utgått både från exempel och en teknisk utgångspunkt som närmast berör ett hemligt/publikt nyckelsystem (jfr nedan, rekommenderade format). Detta avsnitt kommer således att utgå från asymmetrisk krypterade kondensat-värden kopplade till certifikat i en PKI.

Följande format för signaturtjänsten rekommenderas i bilagan till förarbetet för federation (SOU 2010:104 b. 17 a. 11.1; om formaten se vidare huvudframställningen a. 3.3, Format).

Format	Profil	Förutsättning (rekommenderas)
CAdES	BES	För redan signerade digitala objekt utan tidsstämpel.
CMS		För redan signerade digitala objekt utan tidsstämpel.
CMS	T	För redan tidsstämplade digitala objekt.
PDF		Vid signering av digitala objekt som inte ska tidsstämplas.
PAdES	BES	För redan signerade digitala objekt utan tidsstämpel.
PAdES	T	Vid signering av digitala objekt som ska tidsstämplas.
XML Dsig		Vid signering av digitala objekt som inte ska tidsstämplas.
XAdES	BES	För redan signerade digitala objekt utan tidsstämpel.
XAdES	T	Vid signering av digitala objekt som ska tidsstämplas.

De rekommenderade formaten utgörs av de grundläggande formaten i CAdES, PAdES och XAdES. Det krävs således att dessa format utökas för att uppnå långtidsgiltighet om man ska tillämpa rekursiv tidsstämpling.[10]

9 Se a. 4.5.3, Signeringstjänst, signaturtjänst och underskriftstjänst.

10 Jfr 3:5 (tekniska krav för elektroniskt underskrivna handlingar) i RA-FS 2009:2 (Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling)): tillåtna format är antingen CMS (IETF RFC 2315 PKCS #7: CMS 1.5) eller XML-signatures.

4.3.1. Det första ledet

Det första ledet är att identifiera alla komponenter som är relevanta vid bevarandet av den elektroniska signaturen och dess giltighet.[11] Rättsligt är dessa komponenter att ses som handlingar. Nedan följer ett urval av komponenter som kan aktualiseras.[12]

Det framgår av a. 3.1 (*Komponenter*) vilka komponenter som kan vara relevanta för bevarandet av elektroniska signaturers giltighet enligt ETSI -standarden. Av diskussionen i a. 3.3 (*Systemberoende*) skulle det emellertid vara möjligt att andra metoder kan aktualisera andra komponenter. Det är i detta sammanhang svårt att närmare diskutera vilka dessa komponenter skulle vara, eftersom det är beroende av hur systemet är konstruerat. Det är rimligt att anta att det rör sig ytterst om fyra led: **(1)** validering av innehållet (signaturen), **(2)** validering av signaturen (certifikatet), och **(3)** validering av certifikatet (certifikatutfärdarens certifikat), samt **(4)** validering av en, flera eller samtliga föregående led (jfr illustrationerna i a. 3.1, jfr även a. 4.3.2, *Det andra ledet*).

Det kan i anslutning till det här ledet vara nödvändigt att göra en rättslig bedömning av komponenternas betydelse för den digitala allmänna handlingens äkthet, i detta sammanhang från ett juridiskt perspektiv, exempelvis i enlighet med BrB, och/eller FL § 10:3.

Komponent	**Syfte**
Utställarens publika nyckel	Validera utställarens signering, det vill säga, att utställarens hemliga nyckel användes för att signera dataobjektet.
Certifikat för utställarens nyckelpar	Knyter en fysisk eller juridisk person till utställarens hemliga nyckel och därmed till utställarens publika nyckel; validerar att utställaren vid tidpunkten för signering var den person som certifikatet var utfärdat för.
Status för certifikatet för utställarens nyckelpar	Validera att certifikatet för utställarens nyckelpar var giltigt vid signeringstidpunkten, det vill säga, att nyckelparet inte var upphävt eller återkallat; att den fysiska eller juridiska person utställt i certifikatet var den som använde den hemliga nyckeln vid signering.
Certifikatutfärdarens publika nyckel	Validera certifikatutfärdarens signering, det vill säga, att certifikatutfärdarens hemliga nyckel användes för att signera certifikatet för utställarens nyckelpar.
Certifikatet för certifikatutfärdarens nyckelpar	Knyter en fysisk eller juridisk person till certifikatutfärdarens hemliga nyckel och därmed till certifikatutfärdarens publika nyckel; validerar att certifikatutfärdaren vid tidpunkten var den fysiska eller juridiska person som fick utfärda ett certifikat för utställarens nyckelpar.
Status för certifikatet för certifikatutfärdarens nyckelpar	Validera att certifikatet för certifikatutfärdarens nyckelpar var giltigt vid tidpunkten för utfärdandet av certifikatet för utställarens nyckelpar, det vill säga, att certifikatutfärdarens nyckelpar inte var upphävt eller återkallat.
Eventuella tidsstämplar eller tillförlitliga tidmärken för signaturen	Validerar att information existerade innan den tidsstämplade eller tidmarkerade tidpunkten.

11 I SOU 20010:104, s. 204-205, p. 1.81-1.85, bevarade av handlingar, exemplifieras de handlingar som anses vara relevant för utfärdaren av Svensk e-legitimation.

12 För en diskussion om komponenter som i allmänhet kan bli aktuella och varför de är viktiga, se SOU 2002:78 (Arkiv för alla – nu och i framtiden), b. 2 (Långsiktigt bevarande av digital arkivinformation), a. 1, Bakgrund.

Signeringspolicy	Formella och/eller tekniska regler för hur signering och/eller validering av signatur ska gå till.
Dataobjektets krypterade hashvärde ["signaturen"]	Till grund för att beräkna hashvärdet av "innehållet" som signerats av utställaren.
Dataobjektets hashvärde	Till grund för att jämföra med det krypterade [signerade] hashvärdet.[13] Tillgång till själva dataobjektet är dock att föredra.
Dataobjektet	För att beräkna hashvärdet i syfte att jämföra med det krypterade [signerade] hashvärdet.
Request and Response headers [RRH]	HTTP-huvudfält svars- och gensvars- meddelanden vid begäran av en HTTP-transaktion.[14]
Dokumentation	Information som kan vara nödvändig för att säkerställa att hårdvara och mjukvara konfigureras rätt och fungerar som det ska, se exempelvis, docs.eid2.se, SOU 2010:104 b. 17, a. 14.
Hårdvara	För att exekvera nödvändig mjukvara [operativsystemet och webbläsare-teknologierna]. Kan även vara "hårda" nycklar eller certifikat.
Operativsystem	Kan exekvera de nödvändiga webbläsare-teknologierna och för att dataobjektet ska presenteras som avsett. Detta kan inkludera, exempelvis, kodbibliotek, drivrutiner och teckensnitt.
Webbläsarteknologier	För att dataobjektet ska presenteras som avsett i webbläsaren. Detta kan inkludera: interpretatorn eller programtolken för JavaScript, renderingsmotorn för HTML och/eller CSS, externa resurser, såsom programkodsbibliotek till exempelvis JavaScript, instickningsmoduler eller "plug-ins" till webbläsaren.

4.3.2. Det andra ledet

Av de komponenter som har kartlagts måste myndigheten bedöma, i det andra ledet, vilka som har relevans för bevarandet av den elektroniska signaturen.

Utgångspunkten bör vara LKES § 2 där förutsättningen är att grundläggande och mer avancerade eller kvalificerade elektroniska signaturer är "… 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 [de] inte har förvanskats…". Det följer av lagen att per rättslig definition så är en elektronisk signatur, grundläggande, avancerad såväl som kvalificerad, en del av handlingen (Jfr prop. Prop. 1999/2000:117 s. 70).

Signaturen [det krypterade hashvärdet] ska därmed ses som en del av "dataobjektet". I anslutning till detta krävs den offentliga nyckeln för att dekryptera det krypterade hashvärdet [signaturen], vilket annars är tillsynes, en slumpmässig sekvens av alfanumeriska tecken. Detta bör ses som det minimala för att bevara själva signaturen, men vars utställare då inte med säkerhet kan kopplas till den fysiska eller juridiska person som är utställd i signaturen (jfr RA-FS 2009:2 3:5 vilket föreskriver om bevarandeformatet för själva signaturen).

13 Se a. 4.5.3.3, Logg.
14 Se a. 4.5.3.3, Logg.

Nästa steg är alltså att verifiera att utställaren är den fysiska eller juridiska person som utställarens signatur hävdar. Certifikatet för utställarens nyckelpar ämnar till att knyta den hemliga nyckeln till en faktisk fysisk eller juridisk person. Detta förutsätter att certifikatet är ”äkta”, det vill säga att certifikatutfärdaren var behörig att utfärda certifikatet. För båda certifikaten gäller att vid tidpunkten för signering att certifikaten inte var återkallade eller upphävda. Tillsynes verkar samtliga komponenter vara nödvändiga för att säkert koppla utställaren till en fysisk eller juridisk person.

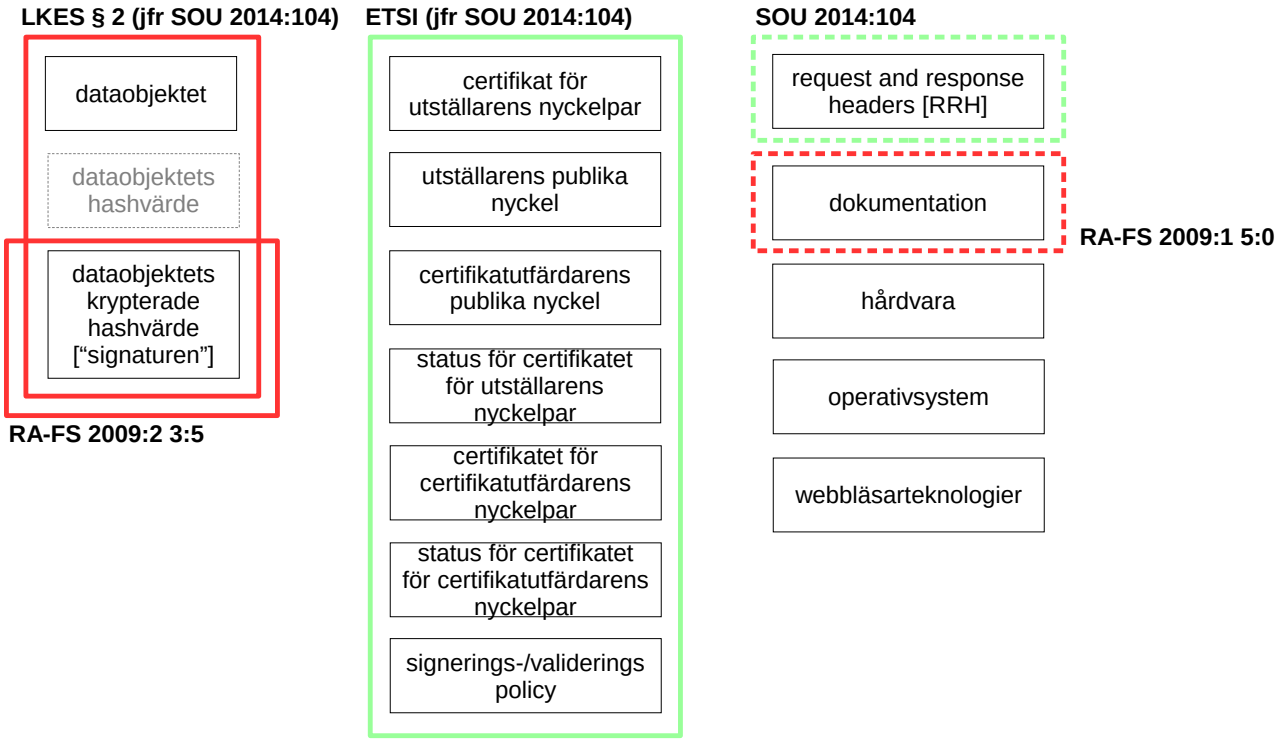
För att signeringsprocessen, och efterföljande valideringsprocesser, ska utföras korrekt behövs eventuellt utfärdad signerings- och/eller valideringspolicy. Detta är emellertid inte nödvändigt för att själva signaturen ska vara giltig, men för att bekräfta att signaturen är giltig. Av liknande skäl kan ”dokumentation” vara relevant för giltigheten, det vill säga, att hård- och mjukvara konfigureras korrekt i syfte att bevarande-, signerings- och valideringsprocessen utförs korrekt (jfr RA-FS 2009:1 5:0, vilket uppställer krav på att ”[m]yndigheten ska dokumentera sina elektroniska handlingar för att handlingarna ska kunna framställas, överföras, hanteras, förvaras och vårdas på ett tillfredsställande sätt under den tid som de ska bevaras.”).

Att bevara signaturen, kopplingen till en fysisk eller juridisk person, och valideringsunderlaget kan endast, så länge alla komponenter är giltiga, bevisa att signaturen är giltig. Det sista steget är alltså bevarandet av giltigheten av komponenterna, det vill säga, att man kan bevisa att samtliga komponenter vid valideringstidpunkten var giltiga.

En myndighet måste själv avgöra vilken eller vilka steg som är mer eller mindre viktiga att säkerställa beroende på omständigheterna, såsom syftet med den elektroniska signaturen för att myndigheten ska efterleva sina rättsliga skyldigheter, däribland medborgarnas rätt att ta del av allmänna handlingar, rättskipningen och förvaltningen, samt forskningens behov.[15]

Nedan illustreras vilka komponenter som är rättsligt reglerade (rött), och vilka komponenter som kan vara relevanta för bevarandet av den elektroniska signaturens giltighet (grönt).

15 Se vidare *Framställning och bevarande av elektroniska signaturer – en praktisk vägledning*.



4.3.3. Det tredje ledet

Av de komponenter [handlingar] som har kartlagts bör myndigheten, i det tredje ledet, klargöra vilka som är allmänna. Tillkomna [inkomna eller upprättade, och förvarade] handlingar i enlighet med TF är allmänna. Frågor som kan aktualiseras är exempelvis om en komponent är handling eller uppgift, eller om den faller under undantagen i TF, såsom led i teknisk bearbetning, eller tillhör en privat aktör.

De handlingar som är allmänna ska bevaras i ursprungligt skick oavsett om de är relevanta eller inte för bevarandet av den elektroniska signaturen. Anses den allmänna handlingen inte vara relevant för bevarandet av den elektroniska signaturen och eventuellt dess giltighet kan myndigheten gallra den med stöd av författning eller beslut från Riksarkivet.

Medan detta led framträder som något självklart ämnar den att hjälpa myndigheten att uppmärksamma *vilka handlingar som inte är allmänna men som är relevanta*. Problemet är att vissa komponenter som är av särskild betydelse för bevarandet av den elektroniska signaturen kan mycket väl aldrig inkomma till myndigheten, eller upprättas hos myndigheten, eller till och med aldrig vara tillgänglig för myndigheten. Det kan röra sig om valideringsdata såsom certifikat eller spärrlistor som finns hos en eller flera tjänstetillhandahållare. Det är särskilt viktigt att betona att myndigheten måste i dessa fall, i ett tidigt skede, ta ställning till om man ska hämta in och säkra särskild information

innan informationen antingen ”försvinner” eller utgår.

Det ska här lyftas fram att Riksarkivet kan i detta sammanhang med stöd av sista stycket arkivförordningen § 3 föreskriva om förutsättningarna för när en handling [elektronisk signatur] ska anses vara arkiverad.

4.3.4. Det fjärde ledet

Är en komponent en allmän handling, så ska den bevaras i ursprungligt skick. Komponenterna kan emellertid återges med en ny representation. En sådan förändring kan leda till informationsförändring. Om en myndighet vill konvertera, omvandla eller organisera en elektronisk signatur eller valideringsdata som är en allmän handling från en representationsform till en annan, uppstår som huvudregel en informationsförändring, och fråga om gallring aktualiseras, vilket kräver stöd i författning eller beslut från Riksarkivet; det måste alltså ske en sedvanlig arkivrättslig gallringsutredning.

Det kan exempelvis röra sig om att man vill konvertera en komponent från ett format till ett annat, exempelvis från CMS till CAdES, eller från CAdES till PAdES. Ett annat tänkbart fall är att en myndighet vill omorganisera certifikatet för en signatur, exempelvis från omslutning/hänvisning till hänvisning/omslutning. Ett mer långtgående exempel är att myndigheten vill omvandla all information om den elektroniska signaturen och dess giltighet till metadata eller annan form och föra in det i handlingen, ärendehanteringssystemet eller ett system för bevarande.

I a. 3.3, *Systemberoende*, diskuterades andra tillvägagångssätt för att bevara en elektronisk signatur, och eventuellt dess giltighet. En myndighet som vill tillämpa alternativa tillvägagångssätt som den anser är lämpliga måste beakta syftet med den elektroniska signaturen för att myndigheten ska efterleva sina rättsliga skyldigheter, däribland medborgarnas rätt att ta del av allmänna handlingar, rättskipningen och förvaltningen, samt forskningens behov. Uppstår det en informationsförändring måste myndigheten utföra en sedvanlig gallringsutredning, och finna stöd för åtgärden i författning eller beslut från Riksarkivet.

5. Förteckning över källor

5.1. Bilder

Samtliga bilder inhämtade under perioden oktober-december 2014 från iconfinder.com, om inte annat är angivet.

Key icon
Creative Commons (Attribution-Share Alike 3.0 Unported)
creativecommons.org/licenses/by-sa/3.0/

Certificate, stock icon
GPL
gnu.org/copyleft/gpl.html

Award, certificate, diploma, license icon
Free for commercial use (Include link to authors website)
pixel-mixer.com

Certificate icon
Free for commercial use (Do not resell)

Priority, status icon
GPL
gnu.org/copyleft/gpl.html

Access, clock, time, icon
Free for commercial use

Stamp icon
Creative Commons (Attribution 3.0 Unported)
creativecommons.org/licenses/by/3.0/

Porcher, signature icon
Creative Commons (Attribution-NonCommercial-NoDerivs 2.5 Generic)
creativecommons.org/licenses/by-nc-nd/2.5/

lol.gif
Benjamin Yousefi
Public Domain

HAL 9000
openclipart.org/detail/189247/hal-9000-by-charner1963-189247
openclipart.org/share
creativecommons.org/publicdomain/zero/1.0/

Riksarkivet

Rapport

Författare	Avdelning	Telefon	Datum	Version	Sida
Benjamin Yousefi	DOI	010-476 72 98	2015-05-29	1.0	22 (22)
Projekt *Arkiv E - Delprojekt 3: Framställning och bevarande av elektroniska signaturer (avsnitt 6)*	Noteringar Direktiv DOI 2013:1 Dnr RA 20-2013-1154				