Tjänstespecifikation

Underskriftstjänst

INNEHÅLLSFÖRTECKNING

Versionshantering

Version	Datum	Beskrivning	Sign
1.00	2013-10-30	Första fastställda versionen av specifikationen	E-legitimationsnämnden
1.10	2013-08-26	Ändringar i avsnitten 3.2 (språkrättelse), 4.5 (Stöd för SHA-1 borttaget) samt 4.3.1.3 (otillåten tidpunkt för underskrift).	E-legitimationsnämnden
1.20	2015-09-15	Tillägg av krav för hantering av underskriftsmeddelanden.	E-legitimationsnämnden
1.30	2018-08-01	Knytningar till Svensk e-legitimation borttaget och ersatt med eID-systemet där det är lämpligt samt följdändringar med anledning av detta. Uppdatering av standarder för underskriftscertifikat i avsnitt 4.12. Lagring av information i databas är ändrat genom att ordet databas är borttaget. Krav på underskrift enligt PAdES i avsnitt 4.3.1.4 har tillkommit. Beskrivning av hur eIDAS tillitsnivåer hanteras infogat i avsnitt 4.7. Krav på stöd för Signature Activation Protocol i avsnitt 4.7.2. Dessutom har ett antal språkliga justeringar är gjorda.	E-legitimationsnämnden

1 INLEDNING

1.1 TJÄNSTEN I SITT SAMMANHANG

Underskriftstjänsten ger möjlighet att med hög säkerhet genomföra elektronisk underskrift med stöd av e-legitimationer .

Genom att ansluta en underskriftstjänst till en e-tjänst kan e-tjänsten låta en användare skriva under en elektronisk handling. Användarens elektroniska underskrift samt användarens tillhörande underskriftscertifikat skapas av underskriftstjänsten efter det att användaren accepterat att skriva under och genom att legitimera sig i samband med att underskriften genomförs. Endast ett kondensat[1] av handlingen som ska skrivas under sänds till underskriftstjänsten, det vill säga själva handlingen sänds inte till underskriftstjänst.

Underskriftstjänsten som den beskrivs i detta dokument befinner sig inom ramen för ett eID-system där det finns en legitimeringstjänst där användare kan legitimera sig och som ställer ut identitetsintyg. Det tekniska protokoll som tillämpas är direkt anpassat för att legitimering ska kunna utföras av extern leverantör i enlighet med SAML 2.0. Underskriftsfunktionaliteten som den beskrivs kan även användas i andra sammanhang med stöd av lokal anpassning, till exempel där kunden har egna interna mekanismer för att identifiera en användare. Det senare scenariot specificeras inte här.

1.2 OMFATTNING

Detta dokument är en del av den Normativa specifikationen för Underskriftstjänsten vilken sammantaget omfattar de krav som ställs på underskriftstjänsten.

Den Normativa specifikationen för Underskriftstjänsten omfattar följande dokument:

- Normativ specifikation Underskriftstjänst (huvuddokument)
- Policy Underskriftstjänst
- Tjänstespecifikation Underskriftstjänst (detta dokument)
- Icke funktionella krav Underskriftstjänst

1.3 SYFTE

Syftet är att tillhandahålla en underskriftstjänst, en infrastrukturkomponent, som på ett standardiserat sätt kan anropas av e-tjänster för att möjliggöra elektronisk underskrift av elektroniska handlingar.

[1] Termen ”kondensat” används här som en förenklad teknisk beskrivning. Varje signaturstandard har sin egen mängd data som representerar ett dokument samt förutsättningar under vilka dokumentet undertecknas. För vidare detaljer hänvisas till refererade tekniska specifikationer.

1.4 MÅL

Målet med underskriftstjänsten är att den håller hög kvalitet, är säker och att det är enkelt att tillföra ny funktionalitet samt att den kan tillhandahållas kostnadseffektivt. För dem som ska använda underskriftstjänsten ska den vara enkel att integrera mot på ett standardiserat sätt.

1.5 FÖRVÄNTADE EFFEKTER

Att underskriftstjänsten används av alla e-tjänster där det finns behov av underskrift. Det ger en likformning av hur elektroniskt underskrivna handlingar är uppbyggda och ser ut.

1.6 STYRANDE FÖRUTSÄTTNINGAR

Följande styrande förutsättningar ligger till grund för utformning av underskriftstjänsten:

- Att lösningar framtagna med stöd av denna kravspecifikation ska vara tekniskt, funktionellt och säkerhetsmässigt kompatibla till den grad att interoperabilitet kan uppnås mellan organisationer och myndigheter som använder tjänster från olika leverantörer.
- Att handlingar som undertecknas inte ska skickas till underskriftstjänsten.
- Att underskriftstjänsten används i sammanhang där e-tjänsten som begär underskrift säkerställer att användaren kunnat granska och samtycka till det som ska undertecknas samt är införstådd med innebörden av att skriva under handlingen.
- Att underskriftstjänsten i så liten utsträckning som möjligt ska spara och logga information relaterat till utförda underskrifter, utan att sådan information så långt som möjligt ska kunna signeras elektroniskt och överföras till den som begärt underskrift.
- Att underskriftscertifikat utfärdas för varje underskriftstillfälle efter att användaren har legitimerat sig med en giltig e-legitimation för att styrka sin identitet.
- I samband med underskrift legitimeras användaren elektroniskt i enlighet med krav som specificeras vid begäran om underskrift. Vid legitimering bekräftar användaren sin avsikt att skriva under, samt om så begärs, bekräftar information om vad som skrivs under.

1.7 AVGRÄNSNINGAR

Följande ingår inte, eller specificeras inte i denna kravspecifikation:

- Tjänster för validering av elektroniska underskrifter.
- Elektroniska tjänster för att lämna in begäran om revokering av underskriftscertifikat. I det fall detta förekommer förutsätts detta vara en manuell procedur som utförs av lokal administratör hos underskriftstjänsten, och då endast i undantagsfall.
- De delar av den övergripande underskriftsprocessen som hanteras av anslutna e-tjänster som till exempel att föra en dialog med användaren om att göra en underskrift.
- Stödtjänster som används av e-tjänster för att hantera handlingar för att skapa och signera ett meddelande (sign request) som sänds till underskriftstjänsten samt för att ta emot meddelande (sign response) från underskriftstjänsten och sätta ihop det till en undertecknad handling.
- Funktioner för elektronisk legitimering (se nedan).

1.8 ELEKTRONISK LEGITIMERING

I samband med elektronisk underskrift genom underskriftstjänst måste användaren legitimeras samt deklarera sin avsikt att skriva under genom att bekräfta ”jag skriver under” eller motsvarande, med lämplig metod. E-tjänsten som begär underskrift ställer krav på legitimering i det signerade ”sign request” som skickas till underskriftstjänsten som bland annat innefattar:

- Krav på tillitsnivå i enlighet med E-legitimationsnämndens Tillitsramverk [ELN-0700]
- Information som användaren ska bekräfta i samband med legitimering för underskrift.
- Eventuell begäran av Signature Activation Data (SAD) i enlighet med Deployment Profile for the Swedish eID Framework [ELN-0602] avsnitt 7.2.2

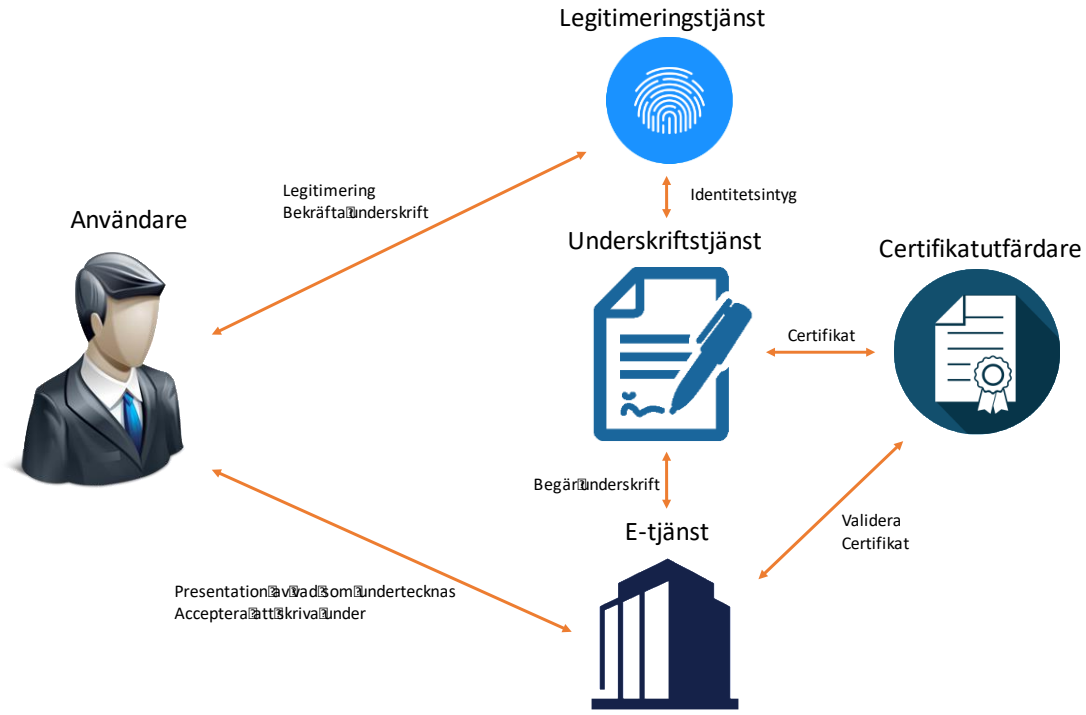
2 FUNKTIONELL BESKRIVNING

2.1 SAMMANFATTNING

Underskriftstjänsten implementeras i anslutning till en e-tjänst genom vilken användare kan skriva under elektroniska handlingar med stöd av en e-legitimation. Underskriftstjänsten är i detta sammanhang en del av det funktionella flöde som inbegriper följande funktioner och aktörer:

Användare	Fysisk person som har e-legitimation och nyttjar tjänst inom ett eID-system. I samband med underskriftstjänsten, specifikt nyttjar e-tjänst i syfte att skriva under elektronisk handling.
E-tjänst	Webbtjänst som användaren besöker och där användaren begär att få underteckna en elektronisk handling, till exempel underskrift av självdeklaration i Skatteverkets e-tjänst.
eID-system	Ett antal tjänster och funktioner som samverkar och kommunicerar med varandra på ett ordnat sätt. Det är tjänster och funktioner som e-tjänster, legitimeringstjänster, utfärdare av e-legitimationer, underskriftstjänster med flera.
Underskriftstjänst	Tjänst genom vilken användaren kan skriva under en elektronisk handling.
Stödtjänst	En tjänst eller funktioner som ingår i, eller anlitas av e-tjänsten för att understödja e-tjänsten med funktioner som krävs för att förbereda underskrift, skriva under med stöd av underskriftstjänsten samt för att kunna kontrollera och hantera underskrivna elektroniska handlingar.
Sign request, **Underskriftsbegäran** samt **Begäran om underskrift**	Ett elektroniskt signerat meddelande som skickas från e-tjänst som begär underskrift, via användarens webbläsare, till en underskriftstjänst.
Sign response samt **Underskriftssvar**	Ett elektroniskt signerat meddelande som returneras från underskriftstjänsten, via användarens webbläsare, till den e-tjänst som begärde underskrift, innehållande resultatinformation för begärd underskrift.

Det grundläggande flödet vid underskrift illustreras enligt följande figur.



Figur 1 Olika delar och aktörer vid underskrift

Användaren är inloggad i en e-tjänst och har nått den punkt där användaren behöver skriva under en elektronisk handling, till exempel en självdeklaration i Skatteverkets e-tjänst.

Användaren skriver under den elektroniska handlingen genom följande förfarande:

- E-tjänsten presenterar den handling som användaren ska skriva under. Detta kan ske genom att e-tjänsten tillhandahåller funktioner genom vilka användaren kan kontrollera samtliga lämnade uppgifter. Användaren väljer att skriva under handlingen.
- E-tjänsten, eventuellt i samverkan med en stödtjänst, skapar och signerar en begäran om underskrift (sign request) enligt protokoll som specificeras i avsnitt 3.1 och överför användaren till underskriftstjänsten med denna begäran bifogad enligt protokoll som specificeras i avsnitt 3.1.
- Underskriftstjänsten kontrollerar inkommen begäran om underskrift.
- Underskriftstjänsten överför användaren till användarens legitimeringstjänst (samma legitimeringstjänst som användaren använde för att logga in till e-tjänsten) för legitimering.
- Användaren legitimerar sig i legitimeringstjänsten med sin e-legitimation (Autentisering) och bekräftar att underskrift görs genom en text motsvarande ”jag skriver under …”. Normalt visas även ett meddelande (sign message) i legitimeringstjänst som anger i vilket sammanhang underskriften görs.

- Legitimeringstjänsten utfärdar ett identitetsintyg och returnerar användaren till underskriftstjänsten med identitetsintyget bifogat.
- Underskriftstjänsten kontrollerar identitetsintygets äkthet samt användarens identitet och avsikt att skriva under som fastställts vid legitimering.
- Underskriftstjänsten skapar användarens elektroniska underskrift samt tillhörande underskriftscertifikat.
- Underskriftstjänsten skapar ett underskriftsvar (sign response) där all relevant information om underskriften ingår enligt protokoll som definieras i avsnitt 3.1 och överför användaren till e-tjänsten med svaret bifogat enligt protokoll som definieras i avsnitt 3.1.
- E-tjänsten, eventuellt med stöd av stödtjänst, tar emot svaret från underskriftstjänsten gör en äkthetskontroll och fogar samman underskriftssvaret med handlingen till en undertecknad elektronisk handling.
- E-tjänsten bekräftar underskriften för användaren.
- Underskriftscertifikatets giltighet kan efter fullbordad underskrift kontrolleras mot spärrlista som tillhandahålls av underskriftstjänsten.

Vid förfarandet ovan skapar underskriftstjänsten ett nyckelpar för användaren samt det underskriftscertifikat som kan användas för att verifiera underskriften. Ett nytt nyckelpar och ett nytt certifikat skapas vid varje underskriftstillfälle. Eftersom underskrift endast kan ske med stöd av ett giltigt identitetsintyg som i sin tur kräver en giltig e-legitimation, så kan underskrift inte ske med stöd av en spärrad e-legitimation eller med stöd av en e-legitimation vars giltighetstid löpt ut. Spärrning av e-legitimation innebär att denna inte längre kan användas vid underskrift. Det finns därför få skäl att spärra ett underskriftscertifikat eftersom underskriftsnyckeln raderas så fort den har använts och underskriftscertifikatet är utställt.

Tekniska lösningar och standarder för verifiering av certifikat kräver dock tillgång till aktuell spärrinformation, även om listan över spärrade certifikat är tom. Vid varje tillfälle en underskrift verifieras måste därför underskriftstjänsten tillhandahålla aktuell spärrinformation.

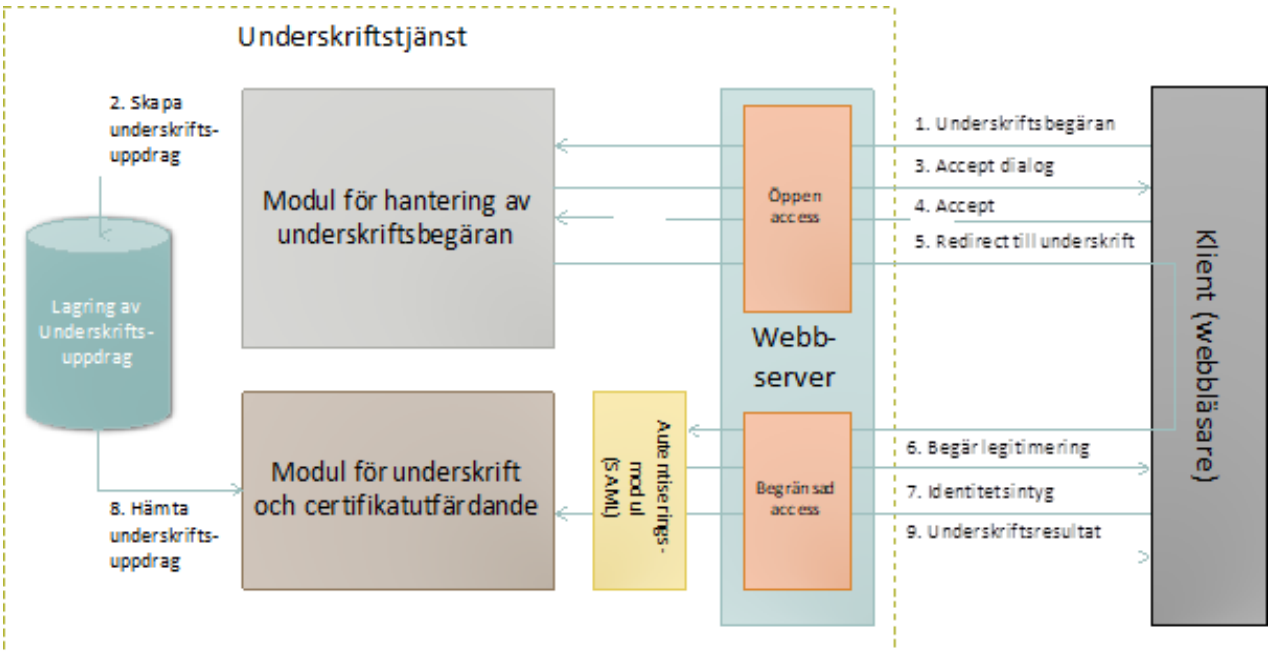
2.2 INGÅENDE FUNKTIONER

Följande funktioner ingår i underskriftstjänsten.

Mottagning och kontroll av underskriftsbegäran	Funktion för att ta emot och kontrollera inkommande begäran om underskrift (sign request).
Kontroll av data som ska undertecknas	Funktion för att kontrollera den data som ska undertecknas för att så långt som möjligt säkerställa att den är korrekt i förhållande till den underskrift som skapas.
Användargränssnitt för underskrift	Funktion för interaktion med användaren via dennes webbläsare för presentation av vissa felmeddelanden.

Överföring av användaren till legitimeringstjänst	Funktion för att överföra användare till legitimeringstjänst med begäran om legitimering samt att säkerställa att användaren bekräftat avsikt att skriva under. Normalt sänds även ett underskriftsmeddelande med till legitimeringstjänsten som beskriver i vilket sammanhang underskriften görs.
Kontroll av identitetsintygets äkthet	Funktion för att kontrollera äktheten i det identitetsintyg som kommer från legitimeringstjänsten.
Kontroll av legitimerad användares identitet	Funktion för att kontrollera användarens identitet efter legitimering i förhållande till den begäran om underskrift som mottagits.
Generering av nycklar	Funktion för generering av privata underskriftsnycklar
Certifikatutfärdande	Funktion för utfärdande av underskriftscertifikat i samband med underskrift.
Underskrift	Funktion för att skapa elektronisk underskrift i enlighet med begäran om underskrift.
Underskriftssvar	Funktion för att skapa underskriftssvar (sign response) samt att överföra användaren med detta svar till den e-tjänst som begärt underskrift.
Lagrad information om uppdraget	Funktioner för lagring av information relaterat till pågående och behandlade underskriftsuppdrag.
Behörighetskontrollfunktion och behörighetsregister	Funktion och tillhörande behörighetsregister över e-tjänster som är behöriga att skicka begäran om underskrift.
Spärrning av underskriftscertifikat	Funktion för att kunna spärra underskriftscertifikat.
Distribution av spärrinformation	Funktion för distribution av spärrinformation för utfärdade underskriftscertifikat.

Funktionernas inbördes relation vid underskrift illustreras av följande skiss:



Figur 2 Funktionella delar i underskriftstjänsten

Ovanstående skiss illustrerar följande steg i en underskriftsprocess sett från underskriftstjänstens perspektiv:

1. Underskriftstjänsten tar emot begäran om underskrift. Begäran om underskrift skickas från användarens webbläsare men har skapats av den e-tjänst som begär underskrift. Överföring av användare med bifogad begäran om underskrift beskrivs närmare i avsnitt 3.1.
2. Inkommen begäran om underskrift kontrolleras. Om begäran om underskrift är OK, skapas ett underskriftsuppdrag. Uppgifter om uppdraget lagras under uppdragets livslängd och den tid efter genomfört uppdrag som krävs för att nödvändiga kontroller, spårning och uppföljning ska kunna genomföras.
3. Användaren överförs till underskriftstjänstens autentiseringsmodul.
4. Autentiseringsmodulen begär legitimering av användaren genom att överföra användaren till den legitimeringstjänst som angetts i mottagen begäran om underskrift.
5. Autentiseringsmodulen tar emot och verifierar äktheten på identitetsintyget från legitimeringstjänsten. Om kontrollen lyckas, överförs användaren till underskriftstjänstens funktioner för underskrift och certifikatutfärdande.
6. Underskriftstjänsten kontrollerar att användarens styrkta identitet överensstämmer med inkommen begäran om underskrift med stöd av den lagrade informationen om uppdraget. Om kontrollen lyckas, skapas nycklar och tillhörande underskriftscertifikat och användarens elektroniska underskrift skapas.
7. Underskriftstjänsten skapar ett underskriftsvar (sign response) och returnerar användaren till e-tjänsten som begärt underskrift med detta svar.

Notera att denna process illustrerar ett exempel på ett felfritt typflöde. Flödet illustrerar inte eventuella felsituationer där någon av kontrollerna ovan leder till att underskriftsprocessen

avbryts. Motsvarande resultat kan uppnås av en systemdesign som på olika sätt avviker från beskrivningen ovan så länge det uppnådda resultatet är detsamma.

2.3 MULTIPLA INSTANSER AV UNDERSKRIFTSTJÄNSTEN

Underskriftstjänsten tillämpar en rollfördelning där e-tjänsten tillhandahåller underskriftstjänsten gentemot användaren och underskriftstjänsten i detta avseende agerar som underleverantör till e-tjänsten. Underskriftstjänsten agerar dock som utfärdare av underskiftscertifikat, med tillhörande funktioner för att tillhandahålla spärrinformation, gentemot förlitande part.

Underskriftstjänsten registreras i metadata som en tjänst som tillhandahålls av e-tjänstens organisation. Detta gör att underskriftstjänstens metadata innehåller information till stöd för grafiska gränssnitt vid legitimering för underskrift som är knutet till e-tjänsten som användaren nyttjar och som presenterar den information som användaren ska underteckna. Den legitimeringstjänst som legitimerar användaren för underskrift kan därmed avgöra, genom underskriftstjänstens metadata, vilken organisations e-tjänst som begär underskrift.

En underskriftstjänst kan betjäna ett flertal e-tjänster genom separata logiska instanser av underskriftstjänsten där varje logisk instans betjänar en organisations e-tjänster. När så sker så representeras underskriftstjänsten med en EntityDescriptor i metadata för varje instans av underskriftstjänsten. Se vidare kraven på logiska instanser i avsnitt 4.2.

2.4 BESKRIVNING AV FUNKTIONER

Detta avsnitt ger en övergripande beskrivning av samtliga ingående funktioner. Krav som dessa funktioner ska uppfylla redovisas i avsnitt 4 samt i tillämpliga delar i avsnitt 5.

2.4.1 Mottagning och kontroll av underskriftsbegäran

Sign request som inkommer till underskriftstjänsten kontrolleras för att säkerställa:

- Att samma underskriftsuppdrag inte betjänas mer än en gång.
- Att begäran om underskrift inkommit från behörig avsändare och är korrekt undertecknad.
- Att begäran om underskrift inkommit inom den tidsperiod då den är giltig.
- Att begäran om underskrift innehåller all nödvändig information i enlighet med ställda krav på innehåll i avsnitt 4.

2.4.2 Kontroll av data som ska undertecknas

De data som ska undertecknas inkommer till underskriftstjänsten i form av underskriftsdata i enlighet med [Eid2-DSS].

Den information som utgör underskriftsdata är utformad i enlighet med det dokument och underskriftsformat som tillämpas för respektive underskrift.

För XML underskrift utgörs dessa data av elementet `<ds:SignedInfo>` och vid PDF underskrifter utgörs detta av ASN.1 kodad data (SignedAttrs) som bl.a. innehåller en hash över dokumentet som ska undertecknas samt uppgift om tidpunkt för underskrift.

Kontroll av data som undertecknas innefattar kontroller av strukturerad information om underskriften om sådan bifogats begäran om underskrift samt att det hashvärde som ska undertecknas har en korrekt struktur och innehåll som är förenligt med de underskriftsalgoritmer som specificeras.

2.4.3 Användargränssnitt för underskrift

Underskriftstjänst enligt denna tjänstespecifikation tillhandahåller inget gränssnitt mot användaren i samband med underskrift.[2]

Underskriftstjänsten tillhandahåller endast gränssnitt gentemot användare i händelse av fel i sign request som gör det omöjligt för underskriftstjänsten att returnera användaren till e-tjänsten som begärt underskrift. Denna situation kan uppstå om underskriftstjänsten inte kan verifiera signaturen på inkommen sign request, eller om denna inte innehåller information om e-tjänst som begärt underskrift samt en retur URL till vilken användaren ska returneras efter underskrift.

2.4.4 Legitimering av användare för underskrift

Användare som ska skriva under överförs till en legitimeringstjänst för legitimering. Legitimeringstjänstens identitet (entityID) hämtas från den sign request som betjänas. Om specifik legitimeringstjänst specificeras så används denna vid legitimering för underskrift.

Om begäran om underskrift innehåller underskriftsmeddelande (sign message) som ska visas för användaren så inkluderas detta i begäran om legitimering till legitimeringstjänsten.

Vid begäran om kvalificerad underskrift, samt i övrigt när underskriftstjänsten anser att detta är befogat, skickas även en begäran om Signature Activation Data (SAD) med i begäran om legitimering.

Identitetsintyg som returneras från legitimeringstjänsten äkthetskontrolleras vid mottagandet. Underskriftstjänsten kontrollerar användarens identitet som säkerställts genom legitimering uppfyller ställda säkerhetskrav samt innehåller nödvändiga uppgifter som krävs för att skapa en underskrift.

Vid begäran om legitimering specificeras krav på legitimeringsprocessen (legitimeringskontext) genom en URI identifierare (`AuthnContextClassRef`) som definierar krav på legitimeringsprocessen i enlighet med [Eid2-Identifiers]. Legitimeringskontext specificerar som minst en tillitsnivå men kan även specificera krav på visning av underskriftsmeddelande i legitimeringsprocessen.

En underskriftstjänst som mottar en begäran om underskrift som innehåller underskriftsmeddelande, kontrollerar om angiven legitimeringstjänst kan visa

[2] Protokollet för begäran om underskrift enligt [Eid2-DSS] ger möjlighet för den tjänst som begär underskrift att skicka med ett meddelande till användaren som underskriftstjänsten kan visa upp i ett användargränssnitt.

underskriftsmeddelande. Om så är fallet så begärs alltid legitimering med krav på visning av underskriftsmeddelande.

2.4.5 Kontroll av legitimerad användares identitet

Den relevanta information om användarens identitet samt avsikt att skriva under som underskriftstjänsten tar emot via autentiseringsmodulen jämförs med information om användaren som ingår i den begäran om underskrift som betjänas.

Underskriften skapas endast om denna information stämmer och unikt identifierar samma användare samt att användaren har godkänt att skriva under i enlighet med begäran om legitimering.

2.4.6 Generering av nycklar

Nycklar för att generera underskrifter skapas och används i en särskild hårdvarumodul, s.k. HSM (Hardware Security Module).

Ett unikt nyckelpar genereras för varje underskriftstillfälle. Detta nyckelpar kan genereras direkt vid underskriftstillfället eller kan vara en förproducerad nyckel som skapats i förväg under perioder då underskriftstjänsten har låg belastning. Användning av förproducerade nycklar möjliggör snabbare svarstider för underskriftstjänsten och möjliggör även en jämnare belastning på hårdvarumodulen vid stora volymer underskrift under kort tid. För att tillgodose behovet av stora volymer av förproducerade nycklar så kan förproducerade nycklar även lagras i krypterad form utanför HSM modulen enligt förfarande som gör att nycklarna endast kan dekrypteras och användas i HSM modulen.

Varje underskriftsnyckel raderas direkt efter att den använts för underskrift och den tillhörande publika nyckeln lästs ut och inkluderats i ett underskriftscertifikat.

2.4.7 Certifikatutfärdande

Underskriftscertifikat utfärdas för varje underskrift och certifierar den publika nyckel som ingår i det nyckelpar som skapas unikt för varje underskrift.

Dessa certifikat tillsammans med de CA-certifikat som krävs för att verifiera underskriftscertifikatet, upp till ett självsignerat rotcertifikat inkluderas i den sign respons som returneras till e-tjänsten som begärt underskrift.

2.4.8 Underskrift

En elektronisk underskrift skapas med stöd av användarens privata nyckel, underskriftscertifikatet, en signeringsalgoritm, samt i enlighet med det signaturformat som begärts.

2.4.9 Underskriftssvar

Underskriftssvar returneras till adress som specificeras i den sign request som betjänas. Detta gäller oavsett om underskriften genomförs eller avbryts.

Undantag för denna regel är om mottagen sign request inte innehåller information om returadress. Om så är fallet, överförs användaren till ett generellt felmeddelande.

2.4.10 Lagrad information om uppdraget

Följande information lagras om uppdraget:

- Information om underskriftsuppdrag lagras minst under den begränsade maximala giltighetstid som konfigurerats för underskriftsuppdrag i underskriftstjänsten. Denna information lagras för att kunna hantera uppdragen under dess giltighetstid men samtidigt för att kontrollera att ett uppdrag inte betjänas två gånger, samt i den mån informationen behövs för att möta kraven på underskriftstjänsten vad gäller lagring av bevismaterial.
- Information om utfärdade certifikat som krävs för att kunna spärra enskilda certifikat under dess giltighetstid.

Uppgift om inkomna och behandlade underskriftsuppdrag lagras minst så länge som krävs för att kunna kontrollera att ett underskriftsuppdrag aldrig betjänas två gånger. Detta är ett viktigt skydd mot återuppspelning av underskriftsuppdrag mot underskriftstjänsten. Den lagrade informationen om underskriftsuppdraget innehåller därför information om det tidsfönster inom vilket underskriftsuppdraget får betjänas samt vilka processteg underskriftsuppdraget slutfört. Den lagrade informationen om underskriftsuppdraget kan tas bort först en tid efter det att giltighetstiden för tillhörande sign request löpt ut. Den lagrade informationen ska skyddas avseende tillgänglighet och integritet.

2.4.11 Behörighetskontrollfunktion och behörighetsregister

Underskriftstjänsten kontrollerar att den som begär underskrift är en behörig e-tjänst.
För detta behöver underskriftstjänsten ett behörighetsregister där alla behöriga e-tjänster är registrerade samt möjlighet att lokalisera den publika nyckel som ska användas för att autentisera behörig e-tjänsts underskrift på mottagen sign request.

Kontroll av att e-tjänst som begär underskrift är registrerad i behörighetsregistret och accepterad av underskriftstjänsten är en viktig kontroll eftersom e-tjänsten tillhandahåller viktiga användargränssnitt för användarens granskning av handling som ska undertecknas samt för användarens acceptans att skriva under. Det är därför viktigt att inte acceptera en sign request från en fientlig webbtjänst som kanske lurar användaren att skriva under information ovetandes eller på felaktiga grunder.

Nyckel som används för att autentisera sign request från e-tjänsten hämtas från metadata om inte en specifik nyckel för e-tjänsten konfigurerats i behörighetsregistret.

2.4.12 Spärrning av certifikat

Spärrning av certifikat antas endast ske i undantagsfall med stöd av manuella processer efter det man kunnat konstatera att ett certifikat måste spärras.

2.4.13 Distribution av spärrinformation

Spärrinformation publiceras alltid som CRL (Certificate Revocation List enligt RFC 5280). Andra protokoll för tillhandahållande av spärrinformation, ex OCSP, eller för validering av certifikat, ex XKMS, får tillhandahållas.

3 BESKRIVNING AV GRÄNSSNITT

3.1 TEKNISKA GRÄNSSNITT

Tekniskt gränssnitt för begäran om underskrift till, samt underskriftssvar från underskriftstjänsten specificeras i [Eid2-DSS-Prof].

Certifikat som utfärdas av underskriftstjänsten i samband med underskrift utformas i enlighet med [Eid2-Cert-Prof].

3.2 GRAFISKA GRÄNSSNITT

Det grafiska gränssnittet designas för att kunna lämna felmeddelande enligt vad som framgår av avsnitt 4.11.

4 FUNKTIONELLA KRAV

I de funktionella kraven som omgärdar behandling av underskriftsuppdrag ingår konfigurerbara parametrar som sammantaget utgör en policy för underskriftstjänsten vilket framgår av dokumentet Policy Underskriftstjänst.

4.1 GRÄNSSNITT

Gränssnitt ska utformas i enlighet med avsnitt 3.

4.2 REPRESENTATION I METADATA

Underskriftstjänsten ska vara representerad i metadata i enlighet med metadatakraven i deployment-profil [Eid2-Depl-Prof] så att den bland annat kan identifieras som underskriftstjänst genom att specificera tjänstekategori ”`http://id.elegnamnden.se/ec/1.0/sigservice`”, samt innefatta alla uppgifter som krävs för att understödja legitimeringstjänsternas grafiska användargränssnitt i samband med legitimering för underskrift.

Underskriftstjänsten ska kunna fungera i multipla logiska instanser där varje logisk instans tillhandahåller underskriftstjänst till en organisations e-tjänster. Varje logisk instans av underskriftstjänsten ska representeras av ett separat EntityDescriptor element i metadata, där varje sådant element anger den organisation som avropat underskriftstjänsten (d.v.s. identifierar den organisation som tillhandahåller de e-tjänster som begär underskrift) och där varje logisk instans innehåller data till stöd för grafiska gränssnitt (mdui element) som kopplar underskriftstjänsten till avropande organisations e-tjänst(er).

Underskriftstjänsten ska kunna hantera begäran om legitimering av användare på ett sådant sätt att det framgår vilken logisk instans av underskriftstjänsten (representerat av unik EntityID i metadata) som begär legitimering för underskrift.

4.3 KONTROLL AV INKOMMANDE SIGN REQUEST

Inkommande sign request ska kontrolleras noggrant i enlighet med följande steg:

1. **Kontroll av unik sign request id**. En unik referens till inkommande sign request ingår som parameter i den http POST som inkommer till underskriftstjänsten där sign request ingår. Denna referens ska kontrolleras mot de underskriftsuppdrag som för närvarande behandlas. Inkommande request ska inte betjänas om den unika referensen redan förekommer i den lagrade informationen om uppdraget. Den unika referensen är inte krypterad eller undertecknad och utgör endast ett första skydd mot ofrivillig upprepning (ex, genom page reload).
2. **Kontroll av underskrift**. Sign request ska vara signerat av behörig e-tjänst och ska kunna verifieras av den nyckel som lokaliseras eller identifieras genom underskriftstjänstens behörighetsregister. Om underskriften inte kan verifieras som giltig och skapad av behörig e-tjänst, får ingen information från denna sign request användas av underskriftstjänsten.
3. **Kontroll av giltighetstid**. Den giltighetstid som anges i sign requesten ska kontrolleras. Sign requesten ska inte behandlas om den inte är inom sin aktuella giltighetstid. Längden på sign requestens giltighetstid ska kontrolleras. Giltighetstiden får inte överstiga konfigurerad maximal giltighetsid. Detta för att sign requesten ska kunna raderas inom rimlig tid utan att detta innebär risk för återuppspelning av gamla request till underskriftstjänsten. Sign request med för lång giltighetstid ska inte betjänas.
4. **Kontroll av signerad sign request id samt status**. Sign requestens unika identitet hämtas från den verifierade sign requesten och jämförs mot underskriftsuppdrag i den lagrade informationen om underskriftsuppdrag. Sign requesten ska inte betjänas om dess unika identitet representerar ett existerande underskriftsuppdrag. Samtidigt ska den unika identiteten kontrolleras med avseende på entropi. Underskriftsuppdraget ska inte accepteras om den unika identiteten representeras av mindre än 64 bitars data.
5. **Kontroll av datainnehåll**. Sign requesten kontrolleras så att den innehåller nödvändig data för att kunna fullfölja underskriftsuppdraget.

Den returadress som specificeras i sign request och som utgör den URL hos begärande e-tjänst till vilken sign response ska returneras, får endast användas om sign requesten klarar kontrollerna 1-4. Om någon av kontrollerna 1-4 misslyckas, så returneras användaren inte tillbaka till e-tjänsten, utan får istället ett felmeddelande direkt från underskriftstjänsten.

4.3.1 Kontroll av data som ska undertecknas

4.3.1.1 XML Signatur enligt XML DSig

Underskrift med XML signatur enligt XML DSig [XML-Dsig] ska stödjas.
Underskriftstjänsten ska kontrollera att samtliga hashvärden över data som ingår i referenser

till signerade objekt, är skapade med samma hash algoritm som underskriftstjänsten använder för att utföra själva underskriften.

4.3.1.2 XAdES Signatur
Underskriftstjänsten ska stödja underskrift enligt XAdES BES [ETSI EN 319 132].
Underskriftstjänsten ska kontrollera att eventuellt bifogat XAdES objekt är kompatibelt med XAdES standardens XML schema.

4.3.1.3 PDF Signatur
Underskriftstjänsten ska stödja underskrift av PDF dokument [PDF].
Underskriftstjänsten ska kontrollera att den tidpunkt för signering som anges i SignedAttrs [CMS] överensstämmer med den tidpunkt då signaturen skapas med acceptans av tidsavvikelse som ska vara konfigurerbar.

4.3.1.4 PAdES Signatur
Underskriftstjänsten ska stödja underskrift av PDF Advanced Electronic Signatures (PAdES) i enlighet med standarden ETSI EN 319 142.

Om tidpunkt för underskrift inte är acceptabel, så ska underskriftstjänsten inte genomföra underskrift av detta dokument utan ska istället returnera ett felmeddelande till e-tjänst som begärt underskrift.

4.4 LAGRING AV ANVÄNDARRELATERAD DATA

4.4.1 Underskriftsuppdrag och sign request

Underskriftstjänsten ska endast lagra information relaterat till användares genomförda underskrifter, och endast under den tid, som krävs för att genomföra underskriften och klara ställda säkerhetskrav.

Information om underskriftsuppdrag inklusive tillhörande sign request som lagras i underskriftstjänsten enligt avsnitten 2.4.10 och 4.3 ska raderas efter det att underskriftsuppdraget inte längre behövs för att skydda mot att gamla sign request skickas om och betjänas mer än en gång. Informationen ska raderas när giltighetstiden löpt ut. Undantag gäller för information relaterat till felaktiga sign request som får sparas i utredningssyfte i säkerhetslogg tills dess att grunden för felet kunnat identifieras.

Specifikation av vilken användarrelaterad information som lagras framgår av dokumentet Policy för Underskriftstjänsten.

4.4.2 Certifikat

Underskriftstjänsten ska lagra uppgifter om utfärdade certifikat som gör det är möjligt med spärrning av certifikat.

Förutom detta ska tjänsten, då underskrift med kvalificerade certifikat erbjuds, lagra information om utfärdade kvalificerade certifikat och uppgifter i övrigt som krävs för att uppfylla eIDAS krav på utfärdande av kvalificerade certifikat.

4.5 SIGNERINGSALGORITMER

Underskriftstjänsten ska kunna stödja signering med de algoritmer som framgår av avsnitt ”Godkända signeringsalgoritmer” i dokumentet ”Policy för Underskriftstjänsten”: Underskriftstjänsten ska kunna konfigureras med avseende på vilka signeringsalgoritmer som får användas.

Om den sign request som ligger till grund för underskrift innehåller uppgift om begärd signeringsalgoritm, så ska denna signeringsalgoritm tillämpas om den stöds av underskriftstjänsten. Om sådan algoritm inte stöds av underskriftstjänsten så ska ingen underskrift skapas utan ett felmeddelande ska istället returneras till e-tjänsten som begärt underskrift.

Om den sign request som ligger till grund för underskrift inte innehåller uppgift om begärd signeringsalgoritm ska den algoritm som framgår att avsnitt ”Standardalgoritmer för underskrift” i dokumentet ”Policy för underskriftstjänsten” användas. Detta förval ska kunna konfigureras som en del av underskriftstjänstens policy.

4.6 ANVÄNDARGRÄNSSNITT

Underskriftstjänsten tillhandahåller inget gränssnitt mot användare förutom i händelser av fel i sign request som gör det omöjligt för underskriftstjänsten att returnera användaren till e-tjänsten som begärt underskrift. Se vidare avsnitt 3.2.

4.7 LEGITIMERING AV ANVÄNDARE

Användare ska legitimeras av den legitimeringstjänst som är angiven i tillhörande sign request.

Underskriftstjänsten ska ha en konfigurerbar policy som anger såväl lägsta som normal tillitsnivå med vilken användare legitimeras vid underskrift.

Legitimering vid underskrift ska ske med normal tillitsnivå om inte annat anges i den sign request som ligger till grund för underskriften.

Legitimering vid underskrift får aldrig ske med tillitsnivå som understiger konfigurerad lägsta tillitsnivå.

Om sign request anger en högre tillitsnivå för legitimering vid underskrift så ska denna högre tillitsnivå tillämpas. Om detta inte är möjligt, så ska underskrift inte genomföras.

Underskriftstjänsten ska endast begära legitimering om den har förutsättningar för att inhämta de identitetsattribut för användaren som e-tjänsten som begärt underskrift krävt i sin sign request. Underskriftstjänsten får använda attributstjänster för att uppfylla kraven på användarattribut.

Om sign request innehåller underlag för att skapa mer än en underskrift så ska det räcka med en legitimering som stöd för att skapa samtliga begärda underskrifter. D.v.s. användaren ska inte legitimeras en gång per begärd underskrift utan endast en gång per sign request.

4.7.1 Underskriftsmeddelande

Om sign request innehåller ett underskriftsmeddelande (sign message) så ska underskriftstjänsten kontrollera om angiven legitimeringstjänst stödjer visning av underskriftsmeddelande. Kontroll ska också göras att begärd tillitsnivå stöds. Om legitimeringstjänsten stödjer detta så ska legitimering begäras med en AuthnContextClassRef URI för begärd tillitsnivå som innefattar krav på visning av underskriftsmeddelandet i enlighet med [Eid2-Identifiers].

Om underskriftsmeddelandet har attributet **`MustShow`** satt till **`true`** ska underskrift endast genomföras om det är säkerställt att användaren förevisats och godkänt meddelandet i samband med legitimering för underskrift. Förfarande för att säkerställa detta vid legitimering enligt SAML 2.0 är specificerat i [Eid2-Depl-prof].

Om legitimeringstjänsten inte stödjer visning av underskriftsmeddelande och underskriftsmeddelandet har attributet **`MustShow`** satt till **`true`**, så ska användaren inte legitimeras. Underskriften ska då istället returnera användaren med ett felmeddelande till e-tjänsten som begärt underskrift.

Legitimering utan visning av underskriftsmeddelande får endast göras i följande fall:

- Sign request saknar `<SignMessage>` element
- Sign request innefattar `<SignMessage>` element med attributet **`MustShow`** satt till **`false`** samt att legitimeringstjänsten som tillämpas saknar funktioner för att visa underskriftsmeddelandet i samband med legitimering.

4.7.2 Signature Activation Protocol

Underskriftstjänsten ska stödja Signature Activation Protocol (SAP) enligt [ELN-0613] samt enligt [ELN-0602] avsnitt 7.2.2.

Underskriftstjänsten ska (in enlighet med [ELN-0602]) skicka begäran om Signature Activation Data (SAD) i begäran om legitimering (AuthnRequest) till legitimeringstjänsten när den underskrift som ska skapas är en kvalificerad underskrift (”QC/SSCD”). Underskriftstjänsten bör dock alltid begära SAD från en legitimeringstjänst som i sin metadata deklarerat stöd för SAP, även om underskriften inte är en kvalificerad underskrift.

4.7.3 Legitimering med utländsk e-legitimation enligt eIDAS

Legitimering ska kunna ske med utländsk e-legitimation via den svenska eDIAS-noden. Detta förfarande skiljer sig från legitimering med svensk e-legitimation enligt följande.

- Andra tillitsnivåer än vad som specificeras i tillitsramverket [ELN-0700] tillämpas. De tillitsnivåer som tillämpas för eIDAS legitimering finns specificerade i [ELN-0603].
- Legitimerad identitet innehåller normalt andra attribut än vad som tillhandahålls av en svensk legitimeringstjänst. Detta gäller speciellt attribut för unik identifierare som anges i sign request.

Vid legitimering med utländsk e-legitimation ska e-tjänsten som begär underskrift specificera vilken tillitsnivå som ska tillämpas för att undvika att underskriftstjänsten tillämpar en ”default” tillitsnivå som inte är avsedd för internationell legitimering.

4.8 KONTROLL AV IDENTITET SAMT AVSIKT ATT SKRIVA UNDER

Användarens identitet som autentiserats genom legitimering ska kontrolleras mot uppgift om användare som specificerats i sign request.

Legitimering av användare accepteras endast om samtliga användarattribut och dess värden som specificerats i sign requesten bekräftats genom legitimering samt att identitetsintyget är utfärdat för den tillitsnivå och legitimeringsprocess som specificerats i begäran om legitimering som `AuthnContextClassRef` URI.

Om SAD begärts från legitimeringstjänsten så ska denna kontrolleras i enlighet med [ELN-0613].

4.9 KONTROLL AV CERTREQUESTPROPERTIES

Om begäran av underskrift angivit en begärd lägsta tillitsnivå så ska underskriftstjänsten kontrollera om detta är förenligt med konfigurerad policy. Om så inte är fallet, ska underskrift inte skapas.

Underskriftstjänsten ska inte utföra legitimering med lägre tillitsnivå än vad som begärts i underskriftsbegäran.

Övriga parametrar kontrolleras i enlighet med [Eid2-DSS-Prof]

4.10 UNDERSKRIFT

Underskriftstjänsten ska stödja underskrift enligt vad som framgår av avsnitt 4.3.1.

Underskrift ska ske genom signering av de data som tillhandahålls i begäran om underskrift i enlighet med [Eid2-DSS-Prof].

Om underskriften är av typen XAdES ska elementet <ds:SignedInfo> uppdateras med referens till signed attributes i det XAdES object som innehåller en hash över underskriftscertifikatet. Såväl signatur, som <ds:SignedInfo> som XAdES objekt innehållande hash över användarens underskriftscertifikat, ska returneras i sign response.

Underskriftstjänsten ska stödja sign request som innehåller begäran om en eller flera underskrifter. Om mer än en underskrift begärs i sign request, så ska samtliga begärda underskrifterna om möjligt returneras i sign response. Om en eller flera underskrifter inte kan skapas enligt begäran i sign request, så ska inget underskriftscertifikat utfärdas och inga underskrifter ska returneras i sign response. Samtliga returnerade underskrifter ska kunna verifieras med det underskriftscertifikat som returneras i sign response.

4.11 FELMEDDELANDEN

Om underskrift inte kan genomföras som begärts ska om möjligt en sign response returneras med lämpligt felmeddelande i enlighet med [Eid2-DSS-Prof].

Felmeddelande som lämnas av underskriftstjänsten direkt till användare ska vara begränsat till ett generellt felmeddelande om att begäran om underskrift misslyckades utan närmare precisering av orsak (för att ge så lite information som möjligt till någon som attackerar systemet).

En användare ska inte få ett felmeddelande direkt från underskriftstjänsten om samtliga följande krav är uppfyllda:

- Sign request är utställt av behörig e-tjänst som angett en retur URL i enlighet med [Eid2-DSS-Prof].
- Sign request är unik och har aldrig behandlats tidigare av underskriftstjänsten.
- Tidsangivelser samt giltighetstid för sign request överensstämmer med uppställda regler och krav.
- Sign request är avsett för och adresserat till den aktuella underskriftstjänsten.

Om dessa krav är uppfyllda ska användaren returneras till e-tjänsten med sign response som innehåller relevanta felkoder och felmeddelanden.

4.12 UTFÄRDANDE AV CERTIFIKAT

Underskriftscertifikat ska utfärdas i enlighet med [Eid2-Cert-Prof].

Underskriftstjänsten ska erbjuda underskriftscertifikat i form av PKC (public key certificate) enligt [Eid2-Cert-Prof], d.v.s. icke kvalificerade certifikat. Underskriftstjänsten kan erbjuda kvalificerade certifikat som option.

Oberoende av vilken instans som används för att skapa underskrift, så kan certifikaten utfärdas av samma certifikatutfärdare under en gemensam utfärdaridentitet. Dock ska kvalificerade och icke kvalificerade certifikat utfärdas med olika utfärdarnycklar under olika utfärdaridentiteter. Underskriftstjänsten ska svara för den certifikatutfärdarfunktion som utfärdar underskriftscertifikat. Underskriftscertifikatens utfärdarfält (issuer field) ska identifiera antingen den organisation som levererar underskriftstjänsten eller en organisation som utfärdar certifikat på uppdrag av den organisation som levererar underskriftstjänsten.

4.12.1 Utfärdarrutiner

Underskriftscertifikat som utfärdas som kvalificerade certifikat ska uppfylla certifikatpolicyn EN 319 411-2 [EN319411-2] enligt profilen QCP-n-qscd (certificate policy for EU qualified certificates issued to natural persons with private key related to the certified, public key in a QSCD) enligt vad som framgår av Policy Underskriftstjänst.

Underskriftscertifikat som utfärdas som icke kvalificerade certifikat ska uppfylla certifikatpolicyn EN 319 411-1 [EN319411-1] enligt profilen NCP (Normalized Certificate Policy), enligt vad som framgår av Policy Underskriftstjänst.

4.13 CERTIFIKATHIERARKI

Utfärdade certifikat ska kunna verifieras av ett CA-certifikat som ingår i en certifikathierarki, d.v.s. CA-certifikatet som medföljer underskriften får inte vara självsignerat utan måste i sin tur vara utfärdat av en annan CA som i sin tur antingen är självsignerat (rotcertifikat) eller signerat av annan CA.

4.14 SIGN RESPONSE

Efter fullgjord underskrift, eller för det fall underskrift inte fullföljts trots mottagandet av en autentiserad sign request från behörig e-tjänst, ska underskriftstjänsten returnera en sign response i enlighet med [Eid2-DSS-Prof].

4.15 SPÄRRNING AV CERTIFIKAT

Underskriftstjänsten ska tillhandahålla administratörsgränssnitt för spärrning av certifikat.

Spärrning av certifikat ska kunna ske baserat på de uppgifter som lagras om certifikatet i underskriftstjänsten.

4.16 DISTRIBUTION AV SPÄRRINFORMATION

Certifikatutfärdarfunktionen ska tillhandahålla spärrinformation. Minimikravet är att tillhandahålla en spärrlista (CRL) i enlighet med RFC 5280 [RFC5280].

Spärrlistan som är relevant för ett certifikat ska göras tillgänglig i enlighet med information i underskriftscertifikatets CRL Distribution Point extension (RFC 5280).

Spärrlistan får inte utfärdas som en delta CRL eller som en indirekt CRL utan ska vara undertecknad med samma nyckel som används för att signera de certifikat som kontrolleras genom spärrlistan.

Spärrlistan ska innehålla en Issuing distribution point extension som anger samma publicerings URL som anges i en CRL Distribution point extension som ingår i de underskriftscertifikat som kontrolleras genom spärrlistan.

4.17 ALGORITMER

Detta avsnitt gäller all tillämpning av krypteringsalgoritmer inom ramen för denna tjänstespecifikation.

Undantag från algoritmer specificerade i enlighet med detta avsnitt får dock göras vid val av algoritmer för underskrift i enlighet med avsnitt 4.5, under förutsättning att detta är förenligt med den policy som upprättats för tjänsten.

Val av algoritmer och nyckellängder för autentisering, kryptering och signering ska följa NIST SP 800-131 [SP800-131] samt ETSI TS 119 312 version 1.1.1 [ETSI-Algo].

Följande algoritmer tillhandahåller minsta acceptabla säkerhetsnivå och uppfyller ovanstående standarder och rekommendationer:

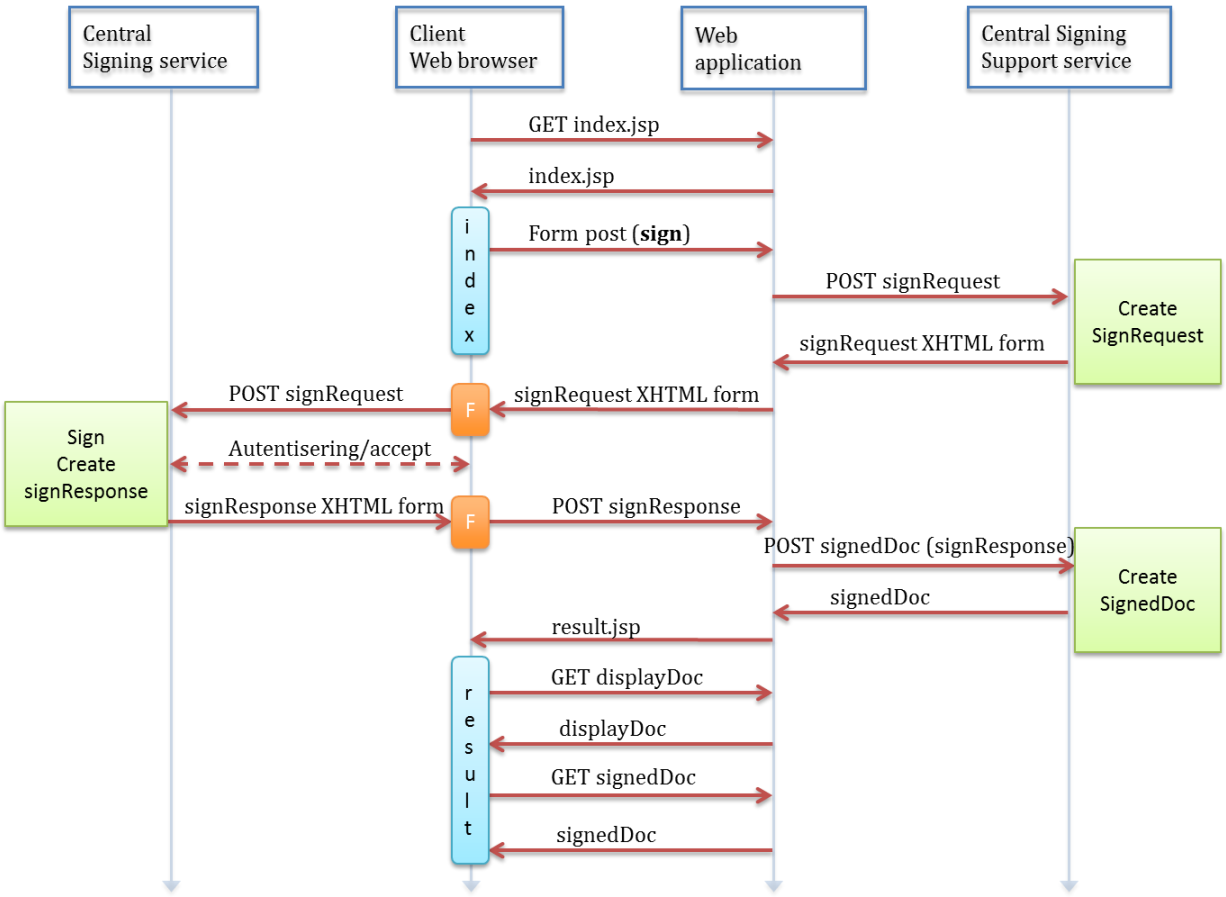
Användningsområde	Algoritm
Symetrisk kryptering	AES-128
Hash algoritm	SHA-256
Publik nyckel algoritm för signering och autentisering	RSA med 2048 bitars modulus.
Publik nyckel algoritm för skapande av symmetrisk sessionsnyckel (Key agreement)	Diffie Hellman, p=2048 bitar
Publik nyckel kryptering med Elliptic Curve (ECC)	ECDSA baserat på NIST kurva P-256

5 ICKE FUNKTIONELLA KRAV

Icke funktionella krav framgår av dokumentet ”Icke funktionella krav Underskriftstjänst”.

6 ANVÄNDNINGSFALL OCH SEKVENSDIAGRAM

Följande sekvensdiagram illustrerar ett typexempel på användning av underskriftstjänsten:



Figur 3 Sekvensdiagram användning av underskriftstjänst

Följande steg illustreras:

- Användaren (Client web browser) hämtar en webbsida (index.jsp) från e-tjänsten (Web application).
- Webbsidan returneras till användarens webbläsare.
- Webbläsaren visar webbsidan som innehåller funktioner för att skriva under en elektronisk handling.
- Användaren accepterar att skriva under vilket i detta exempel resulterar i en form POST till e-tjänsten med innebörden att användaren vill skriva under.
- E-tjänsten har i exemplet knutit till sig en stödtjänst för underskrift (Central signing support service) och skickar handlingen som ska skrivas under till stödtjänsten tillsammans med nödvändiga uppgifter som krävs för att skapa en sign request.
- Stödtjänsten skapar en sign request som returneras till e-tjänsten i form av en XHTML sida i enlighet med [Eid2-DSS-Prof] och returnerar denna till e-tjänsten.
- E-tjänsten returnerar XHTML sidan till användarens webbläsare.

- Användarens webbläsare renderar XHTML sidan. Denna innehåller ett JavaScript som skickar sign requesten genom en html form POST till underskriftstjänsten (Central signing service).
- Underskriftstjänsten betjänar mottagen sign request, legitimerar användaren och skapar därefter underskrift och underskriftscertifikat.
- Underskriftstjänsten skapar en sign respons som returneras till användaren inbakat i en XHTML sida.
- Användarens webbläsare renderar XHTML sidan. Denna innehåller ett JavaScript som skickar sign responsen genom en html form POST till e-tjänsten.
- E-tjänsten vidarebefordrar sign responsen till stödtjänsten.
- Stödtjänsten fogar samman ett underskrivet dokument utifrån sign responsen i kombination med data som mottogs vid skapandet av tillhörande sign request.
- Det undertecknade dokumentet returneras till e-tjänsten.
- En webbsida med bekräftelseinformation returneras till användaren
- Användaren använder eventuella funktioner i bekräftelsesidan för att få tillgång till undertecknad handling, visuell representation av den undertecknade handlingen, information om underskriftens giltighet mm.

7 REFERENSER

7.1 NORMATIVA REFERENSER

Normativa referenser innehåller information som utgör krav för att kunna uppfylla specificerade krav i tjänstespecifikationen. Kraven i denna tjänstespecifikation styr vilka delar i dessa normativa dokument som måste tillämpas.

Om ett krav i denna tjänstespecifikation i något avseende avviker från något av nedanstående normativa dokument, är kravet i denna tjänstespecifikation överordnat.

Referens	Dokument
[CMS]	R. Housley Cryptographic Message Syntax (CMS), IETF (Internet Engineering Task Force) RFC 5652, September 2009
[Eid2-Cert-Prof]	Certificate profile for certificates issued by Central Signing services
[Eid2-Identifiers]	Registry for identifiers assigned by the Swedish e- identification board
[Eid2-Depl-prof]	Deployment Profile for the Swedish eID Framework
[Eid2-DSS]	DSS Extension for Federated Central Signing Services.
[Eid2-DSS-Prof]	Implementation profile for using OASIS DSS in Central Signing services
[ELN-0602]	Deployment Profile for the Swedish eID Framework
[ELN-0603-v1.5]	Registry for identifiers assigned by the Swedish e-identification board
[ELN-0613]	Signature Activation Protocol for Federated Signing
[ELN-0700]	Tillitsramverk för Svensk e-legitimation
[EN319411-1]	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements – Latest published version
[EN319411-2]	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates – Latest published version
[ETSI Algo]	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites. (http://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.01.01_60/ts_119312v010101p.pdf)
[ETSI EN319132]	Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures
[ETSI EN319142]	Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures
[PDF]	Document management -- Portable document format -- Part 1: PDF 1.7, ISO 32000-1:2008
[RFC5280]	Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008

[SP800-131]	NIST Special Publication 800-131A Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths. (http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf)
[XML-Dsig]	D. Eastlake et al, XML-Signature Syntax and Processing, W3C Recommendation, February 2002.