Tjänstespecifikation

Underskriftstjänst

som del av Svensk e-legitimation

INNEHÅLLSFÖRTECKNING

1 INLEDNING

1.1 TJÄNSTEN I SITT SAMMANHANG

E-legitimationsnämnden arbetar med att införa en ny infrastruktur för elektronisk legitimering i Sverige som bygger på federerad teknik enligt SAML standarden. En av de många fördelarna med en sådan infrastruktur är att användare autentiseras i e-tjänster med ett identitetsintyg (SAML authentication assertion, d.v.s. en SAML assertion med authentication och attribute statements) enligt en gemensam standard oberoende av vilken teknik som används i användarens e-legitimation. Detta gör det möjligt att använda olika typer av e-legitimationer (ex. mobila lösningar, smarta kort, kod dosor mm) så länge de uppfyller ställda säkerhetskrav.

Den nya infrastrukturen gör det även möjligt att använda e-legitimationer som medger säker autentisering, men där e-legitimationen inte längre behöver innehålla en privat nyckel och tillhörande certifikat enligt x.509 standarden. Men det innebär i sin tur att e-legitimationen inte kan användas för att skapa underskrifter på en handling.

Underskriftstjänsten har som syfte att möjliggöra underskrift inom den nya infrastrukturen med stöd av alla typer av e-legitimationer som erbjuder tillräcklig grad av säkerhet.

Genom att införa en eller flera underskriftstjänster som ansluts till e-tjänster som ingår i infrastrukturen, kan en e-tjänst låta en användare skriva under en elektronisk handling med stöd av underskriftstjänsten. Användarens elektroniska underskrift samt användarens tillhörande underskriftscertifikat skapas av underskriftstjänsten efter det att användaren accepterat att skriva under genom att legitimera sig mot underskriftstjänsten.

1.2 SYFTE

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

1.3 MÅL

Målet med underskriftstjänsten är att den håller hög kvalitet, att det är enkelt att tillföra ny funktionalitet samt att den är kostnadseffektiv att förvalta. För dem som ska använda underskriftstjänsten är den enkel att integrera emot.

1.4 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.

1.5 STYRANDE FÖRUTSÄTTNINGAR

Följande styrande förutsättningar ligger till grund för utformning av underskriftstjänsten:

- Att lösningar framtagna med stöd av denna kravspecifikation skall vara tekniskt, funktionellt och säkerhetsmässigt kompatibla till den grad att interoperabilitet kan uppnås mellan organisationer och myndigheter som tillämpa tjänster från olika leverantörer.
- Att handlingar som undertecknas inte skall behöva skickas till underskriftstjänsten.
- Att underskriftstjänsten används i sammanhang där e-tjänsten som begär underskrift säkerställer att användaren kunnat granska och samtycka till det som skall undertecknas samt är införstådd med konsekvenserna av att skriva under med stöd av underskriftstjänsten.
- Att underskriftstjänsten i så liten utsträckning som möjligt skall behöva spara och logga information relaterat till utförda underskrifter, utan att sådan information så långt som möjligt skall kunna signeras elektroniskt och överföras till den som begärt underskrift.
- Att underskriftscertifikat utfärdas för varje underskriftstillfälle och vid det tillfället har användaren legitimerat sig med en giltig e-legitimation för att styrka sin identitet.

1.6 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.
- Stödtjänster som används av e-tjänster för att kunna begära underskrift av underskriftstjänster.

2 FUNKTIONELL BESKRIVNING

2.1 SAMMANFATTNING

Underskriftstjänsten implementeras som en webbtjänst genom vilken användare kan skriva under elektroniska handlingar med stöd av en Svensk e-legitimation. Underskriftstjänsten är i detta sammanhang en del av ett funktionellt flöde som inbegriper följande funktioner och aktörer:

Användare	Innehavare av Svensk e-legitimation som skall kunna skriva under en elektronisk handling.
E-tjänst	En webbtjänst som användaren besöker och där användaren önskar underteckna en elektronisk handling, ex underskrift av självdeklaration i Skatteverkets e-tjänst.
Underskriftstjänst	Tjänst genom vilken användaren kan skriva under den elektroniska handlingen.
Stödtjänst	En tjänst eller funktioner som ingår i, eller anlitas av e-tjänsten för att understödja e-tjänsten med funktioner som krävs för att skriva under med stöd av underskriftstjänsten samt för att kunna kontrollera underskrift på elektroniska handlingar.
Sign request, **underskriftsbegäran** samt **begäran om underskrift**	Ett elektroniskt signerat meddelande som skickas från e-tjänst som begär underskrift, via användaren, till en underskriftstjänst.
Sign response samt **underskriftssvar**	Ett elektroniskt signerat meddelande som returneras från underskriftstjänsten, via användaren, till den e-tjänst som begärde underskrift, innehållande resultatinformation för begärd underskrift.

Det grundläggande flödet vid underskrift illustreras enligt följande bild.

Användaren är i det här fallet inloggad i en myndighets e-tjänst och har nått den punkt där användaren behöver skriva under en elektronisk handling, till exempel en självdeklaration i Skatteverkets e-tjänst. Det aktuella flödet beskrivet nedan förutsätter med andra ord att användaren redan har en giltig e-legitimation som kan användas för att legitimera användaren genom en specifik legitimeringstjänst. Om så ej är fallet så kan användaren inte logga in i e-tjänsten och e-tjänsten kan då inte genomföra begäran om underskrift.

Användaren skriver då under den elektroniska handlingen genom följande förfarande:

- E-tjänsten presenterar den information (alternativt den handling) som användaren skall 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 med stöd av legitimeringstjänsten genom sin e-legitimation (Autentisering).

- Legitimeringstjänsten utfärdar ett identitetsintyg (SAML Identity Assertion) och returnerar användaren till underskriftstjänsten med identitetsintyget bifogat.
- Underskriftstjänsten kontrollerar användarens identitet genom identitetsintyget.
- Underskriftstjänsten skapar användarens elektroniska underskrift samt tillhörande underskriftscertifikat.
- Underskriftstjänsten skapar ett svar på begäran om underskrift (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 lämplig stödtjänst, tar emot svaret från underskriftstjänsten och använder denna information för att foga samman 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 ytterst få skäl att spärra ett underskriftscertifikat då underskriftsnyckeln inte sparas och aldrig kan komma i orätta händer.

Tekniska lösningar och standards 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 även kunna tillhandahålla aktuell spärrinformation.

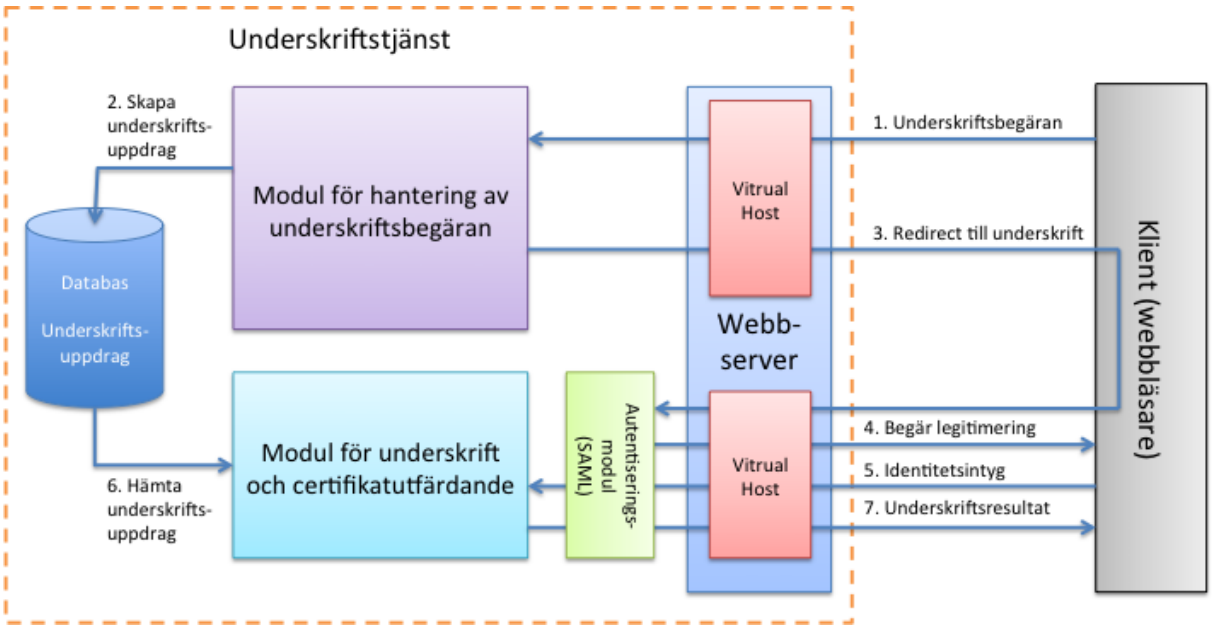
2.2 INGÅENDE FUNKTIONER

Följande funktioner ingår i underskriftstjänsten

Mottagning och kontroll av underskriftsbegäran	Funktion för att ta emot och kontrollera inkommande begäran om underskrift.
Kontroll av data som skall undertecknas	Funktion för att kontrollera den data som skall undertecknas för att säkerställa så långt som möjligt 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.
Legitimering av användare för underskrift	Funktion för att överföra användare till legitimeringstjänst med begäran om legitimering.
Kontroll av legitimerad	Funktion för att kontrollera användarens identitet efter

användares identitet	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.
Databas	Databasfunktioner 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:



Denna 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 i en intern databas.
3. Användaren överförs (redirect) 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 hämtar relevant underskriftsuppdrag från den interna databasen och kontrollerar att användarens styrkta identitet överensstämmer med inkommen begäran om underskrift. Om kontrollen lyckas, skapas nycklar och tillhörande underskriftscertifikat och användarens elektroniska underskrift skapas.
7. Underskriftstjänsten skapar ett svar på begäran om underskrift (sign response) och returnerar användaren till e-tjänsten som begärt underskrift med detta svar.

Notera att detta är ett typflöde om allt går som tänkt. Flödet illustrerar inte eventuella felsituationer där någon av kontrollerna ovan leder till att underskriftsprocessen avbryts.

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 federationens 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 skall 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 federationens 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 skall 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 skall undertecknas

De data som skall 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 skall 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 skall 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.[1]

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 skall returneras efter underskrift.

2.4.4 Legitimering av användare för underskrift

Användare som skall skriva under överförs till en legitimeringstjänst för legitimering. Detta kräver att underskriftstjänsten är registrerad som en e-tjänst i en identitetsfederation där legitimeringstjänsten ingår. Legitimeringstjänstens identitet (entityID) hämtas från den sign request som betjänas.

[1] 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.

Autentiseringsmodulen som begär legitimering hämtar information om legitimeringstjänsten via federationens metadata samt skickar begäran om legitimering till legitimeringstjänsten.

Identitetsintyg (SAML Identity Assurance) som returneras från legitimeringstjänsten äkthetskontrolleras vid mottagandet av autentiseringsmodulen. Underskriftstjänsten kontrollerar sedan att identitetsintyget representerar rätt användare och innehåller nödvändiga uppgifter som krävs för att skapa en underskrift.

2.4.5 Kontroll av legitimerad användares identitet

Den relevanta information om användarens identitet som underskriftstjänsten tar emot från autentiseringsmodulen jämförs med information om användaren som ingår i den begäran om underskrift som betjänas.

Signatur skapas endast om denna information stämmer och unikt identifierar samma användare.

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 det 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 Databas

Följande information lagras i en eller flera databaser:

- 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.

I databasen ingår aldrig de dokument som undertecknas.

Uppgift om inkomna och behandlade underskriftsuppdrag lagras i databasen 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. Varje underskriftsuppdrag i databasen innehåller därför information om det tidsfönster inom vilket underskriftsuppdraget får betjänas samt vilka processteg underskriftsuppdraget slutfört. Underskriftsuppdraget kan tas bort från databasen först en tid efter det att giltighetstiden för tillhörande sign request löpt ut.

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 skall 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 skall 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 federationens 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

Felmeddelande som lämnas av underskriftstjänsten direkt till användare skall 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 skall få ett felmeddelande direkt från underskriftstjänsten om sign request är utställt av behörig e-tjänst som angett en retur URL i enlighet med [Eid2-DSS-Prof]. Om dessa krav är uppfyllda skall användaren returneras till e-tjänsten med sign response som innehåller relevanta felkoder och felmeddelanden.

4 FUNKTIONELLA KRAV

I de funktionella kraven som omgärdar behandling av underskriftsuppdrag ingår konfigurerbara parametrar som sammantaget utgör en policy för underskriftstjänsten. Denna policy skall dokumenteras och godkännas av E-legitimationsnämnden.

4.1 GRÄNSSNITT

Gränssnitt skall utformas i enlighet med avsnitt 3.

4.2 REPRESENTATION I FEDERATIONENS METADATA

Underskriftstjänsten måste vara ansluten som e-tjänst i identitetsfederationen för Svensk e-legitimation i enlighet med det regelverk som antagits för denna identitetsfederation. Detta för

att underskriftstjänsten skall kunna begära legitimering från samtliga legitimeringstjänster som är anslutna till federationen.

Underskriftstjänsten skall vara representerad i federationens metadata i enlighet med metadatakraven i federationens 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 skall kunna opereras i multipla logiska instanser där varje logisk instans tillhandahåller underskriftstjänst till en organisations e-tjänster. Varje logisk instans av underskriftstjänsten skall representeras av ett separat EntityDescriptor element i federationens 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 skall 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 skall 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 skall kontrolleras mot de underskriftsuppdrag som för närvarande behandlas. Inkommande request skall inte betjänas om den unika referensen redan förekommer i databasen. Denna information är inte krypterad eller undertecknad och utgör endast ett första skydd mot ofrivillig upprepning (ex, genom page reload).
2. **Kontroll av underskrift**. Sign request skall vara signerat av behörig e-tjänst och skall 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 skall kontrolleras. Sign requesten skall inte behandlas om den inte är inom sin aktuella giltighetstid. Längden på sign requestens giltighetstid skall kontrolleras. Giltighetstiden får inte överstiga konfigurerad maximal giltighetsid. Detta för att sign requesten skall kunna raderas inom rimlig tid utan att detta innebär risk för återuppspelning av gamla request till underskriftstjänsten. Sign request med för lång giltighetstid skall inte betjänas.

4. **Kontroll av signerad sign request id samt status**. Sign requestens unika identitet hämtas från den verifierade sign requesten och jämförs mot databasen över tidigare underskriftsuppdrag. Sign requesten skall inte betjänas om dess unika identitet representerar ett existerande underskriftsuppdrag i databasen. Samtidigt skall den unika identiteten kontrolleras med avseende på entropi. Underskriftsuppdraget skall 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 skall 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 skall undertecknas

4.3.1.1 XML Signatur enligt XML DSig

Underskrift med XML signatur enligt XML DSig [XML-Dsig] skall stödjas.
Underskriftstjänsten skall 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 skall stödja underskrift enligt XAdES BES [XAdES].
Underskriftstjänsten skall kontrollera att eventuellt bifogat AdES objekt är kompatibelt med XAdES standardens XML schema.

4.3.1.3 PDF Signatur

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

Om tidpunkt för underskrift inte är acceptabel, så skall underskriftstjänsten byta ut angiven tid mot aktuell tidpunkt för underskrift.

4.4 LAGRING AV ANVÄNDARRELATERAD DATA

4.4.1 Underskriftsuppdrag och sign request

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

Underskriftsuppdrag och tillhörande sign request som lagras i underskriftstjänstens databas enligt avsnitt 4.3 skall raderas efter det att underskriftsuppdraget inte längre behövs i

databasen för att skydda mot att gamla sign request skickas om och betjänas mer än en gång. Informationen skall 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 ingår i den policy som skall dokumenteras och godkännas av E-legitimationsnämnden.

4.4.2 Certifikat

Underskriftstjänsten skall kunna konfigureras med avseende på vilken information om utfärdade certifikat som skall sparas till stöd för bl.a. spärrning av certifikat.

Följande varianter skall stödjas:
1. Lagring av samtliga utfärdade certifikat
2. Lagring endast av certifikatserienummer för alla utfärdade certifikat

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

4.5 SIGNERINGSALGORITMER

Underskriftstjänsten skall kunna stödja signering med följande algoritmer:
- RSA med SHA-1
- RSA med SHA-256
- ECDSA (baserat på NIST kurvan P-256) med SHA-256

Underskriftstjänsten skall kunna konfigureras med avseende på vilka signeringsalgoritmer som får användas. Detta innebär bland annat att även om stöd finns för RSA med SHA-1, så skall det vara möjligt att förhindra att algoritmen används genom konfiguration.

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

Om den sign request som ligger till grund för underskrift inte innehåller uppgift om begärd signeringsalgoritm, så skall RSA med SHA-256 tillämpas som standard (default). Detta förval skall dock 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 skall överföras till den legitimeringstjänst som är angiven i tillhörande sign request. Endast identitetsintyg från denna legitimeringstjänst får accepteras.

Underskriftstjänsten skall ha en konfigurerbar policy som anger såväl lägsta som normal tillitsnivå enligt federationens tillitsramverk, med vilken användare legitimeras vid underskrift.

Legitimering vid underskrift skall 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 skall denna högre tillitsnivå tillämpas. Om detta inte är möjligt, så skall underskrift inte genomföras.

Undantag för reglerna ovan gäller om signeringscertifikatet utfärdas som kvalificerat certifikat. Om signeringscertifikatet utfärdas som kvalificerat certifikat så skall tillitsnivå 3 eller högre alltid tillämpas.

Underskriftstjänsten skall 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 skall det räcka med en legitimering som stöd för att skapa samtliga begärda underskrifter. D.v.s. användaren skall inte legitimeras en gång per begärd underskrift utan endast en gång per sign request.

4.8 KONTROLL AV LEGITIMERAD ANVÄNDARES IDENTITET

Användarens identitet som mottagits genom identitetsintyg skall 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 återfinns i mottaget identitetsintyg.

4.9 KONTROLL AV CERTREQUESTPROPERTIES

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

Underskriftstjänsten skall 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 skall stödja underskrift av XML dokument samt underskrift av PDF dokument.

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

Om underskriften är av typen XAdES så skall 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 object innehållande hash över användarens underskriftscertifikat, skall returneras i sign response.

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

4.11 FELMEDDELANDEN

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

4.12 UTFÄRDANDE AV CERTIFIKAT

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

Underskriftstjänsten skall erbjuda underskriftscertifikat i form av PKC certifikat enligt [Eid2-Cert-Prof], d.v.s. icke kvalificerade certifikat. Underskriftstjänsten kan vidare 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 skall kvalificerade och icke kvalificerade certifikat utfärdas med olika utfärdarnycklar under olika utfärdaridentiteter. Underskriftstjänsten skall svara för den certifikatutfärdarfunktion som utfärdar underskriftscertifikat. Underskriftscertifikatens utfärdarfält (issuer field) skall 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 skall uppfylla certifikatpolicyn TS 101 456 från ETSI [TS101456]. Avvikelser från denna policy skall godkännas av E-legitimationsnämnden.

Underskriftscertifikat som utfärdas som icke kvalificerade certifikat skall uppfylla certifikatpolicyn TS 102 042 från ETSI [TS102042] enligt profilen NCP (Normalized Certificate Policy). Avvikelser från denna policy skall godkännas av E-legitimationsnämnden.

4.13 CERTIFIKATHIERARKI

Utfärdade certifikat skall 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, skall underskriftstjänsten returnera en sign response i enlighet med [Eid2-DSS-Prof].

4.15 SPÄRRNING AV CERTIFIKAT

Underskriftstjänsten skall tillhandahålla administratörsgränssnitt för spärrning av certifikat.

Spärrning av certifikat skall kunna ske genom att antingen ange det fullständiga certifikat som skall spärras, eller genom att ange det certifikatserienummer som skall spärras.

4.16 DISTRIBUTION AV SPÄRRINFORMATION

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

Spärrlistan som är relevant för ett certifikat skall 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 skall vara undertecknad med samma nyckel som används för att signera de certifikat som kontrolleras genom spärrlistan.

Spärrlistan skall 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 skall följa NIST SP 800-131 [SP800-131] samt ETSI TS 102 176-1 version 2.11 [ETSI-Algo].

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

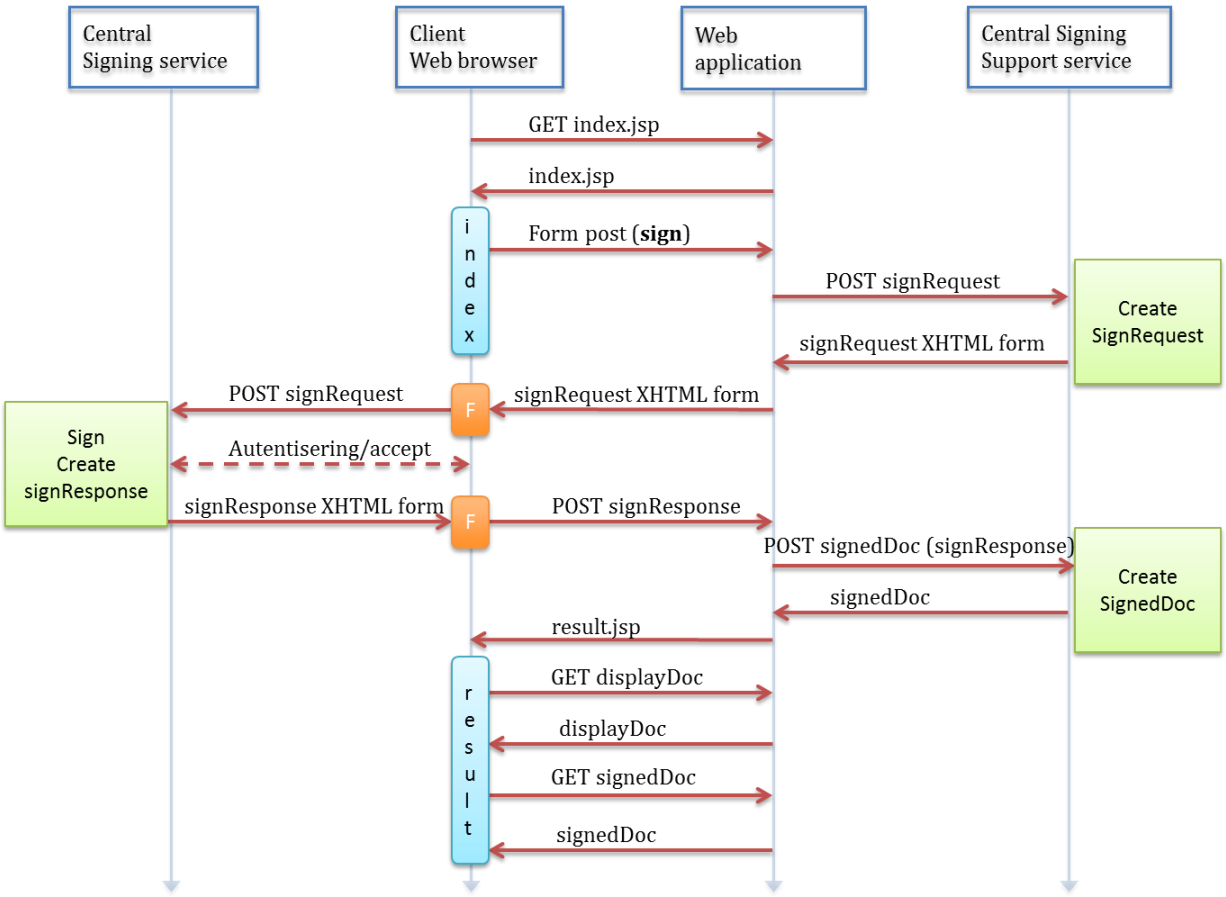
Användningsområde	Algoritm
Symetrisk kryptering	AES-128
Hash algoritm	SHA-256
Publik nyckel algoritm för signering och autentisering	RSA med 2048 bitars modulus.
Publik nyckel algoritm för skapande av symmetrisk sessionsnyckel (Key agreement)	Diffie Hellman, p=2048 bitar
Publik nyckel kryptering med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

5 ICKE FUNKTIONELLA KRAV

Icke funktionella krav framgår av dokumentet ”Icke funktionella krav Underskriftstjänst Svensk e-legitimation”.

6 ANVÄNDNINGSFALL OCH SEKVENSDIAGRAM

Följande sekvensdiagram illustrerar ett typexempel på användning av underskriftstjänsten:



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 skall 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
[Eid2-DSS]	Eid2 DSS Extension for SAML based Central Signing service.
[Eid2-DSS-Prof]	Implementation profile for using OASIS DSS in Central Signing services
[Eid2-Cert-Prof]	Certificate profile for certificates issued by Central Signing services
[Eid2-Depl-prof]	Deployment Profile for the Swedish eID Framework
[XML-Dsig]	D. Eastlake et al, XML-Signature Syntax and Processing, W3C Recommendation, February 2002.
[XAdES]	XML Advanced Electronic Signatures, ETSI, December 2010
[PDF]	Document management -- Portable document format -- Part 1: PDF 1.7, ISO 32000-1:2008
[CMS]	R. Housley Cryptographic Message Syntax (CMS), IETF (Internet Engineering Task Force) RFC 5652, September 2009
[TS101456]	Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates, ETSI publication TS 101 456 V1.4.3, 2007-05-15
[TS102042]	Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates, ETSI publication TS 102 042 V1.3.4, 2007-12-11
[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
[ETSI Algo]	Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms. (http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=31439)
[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)