Ändringshantering

Normativ specifikation
Underskriftstjänst

INNEHÅLL

1 INLEDNING

Den Normativa specifikationen för Underskriftstjänsten har uppdaterats, från version 1.2 till version 1.3, för att harmonisera med senaste versionen av tekniskt ramverk och eIDAS. Följande viktiga ändringar har gjorts i specifikationen.

- Specifikationen har uppdateras för att vara följsam till den nya versionen av tekniskt ramverk som träder i kraft 29 september 2018.
- Standarder för underskriftscertifikat har uppdaterats och refererar nu till EN-standarder för certifikatpolicy.
- Krav på tillitsnivåer refererar till E-legitimationsnämndens Tillitsramverk och det finns beskrivet hur eIDAS tillitsnivåer ska hanteras.
- Standard för underskrift enligt XAdES har uppdaterats och refererar nu till EN-standard.
- Krav på stöd för underskrift enligt PDF Advanced Electronic Signatures (PAdES) har lagts till (detta har redan tidigare testats med godkänt resultat hos de leverantörer som har godkända underskriftstjänster).
- Lagring av information i underskriftstjänsten behöver inte göras i databas, ordet databas är borttaget.
- Krav på stöd för protokollet Signature Activation Protocol samt att det ska användas vid begäran om kvalificerad underskrift har lagts till.
- Knytningar till Svensk e-legitimation borttaget och ersatt med eID-systemet där det är lämpligt samt följdändringar med anledning av detta.

Vidare har vissa mindre tekniska ändringar och uppdateringar samma vissa språk ändringar och förtydliganden gjorts.

Följande dokument ingår i den normativa specifikationen för underskriftstjänsten.

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

Nedan framgår tekniska och funktionella ändringar i de dokument som omfattar den normativa specifikationen.

2 NORMATIV SPECIFIKATION (HUVUDDOKUMENT)

Avsnitt 1 Inledning
Inga ändringar som påverkar underskriftstjänsten eller dess funktionalitet.
En stor del av bakgrundbeskrivningen är borttagen och det är också förtydligat att annan myndighet kan ansvara för den normativa specifikationen för underskriftstjänsten.

Avsnitt 3 Tjänster
Detta med Svensk e-legitimation har tagits bort. När det gäller kvalificerade underskrifter hänvisas nu till eIDAS då tidigare lagstiftning som reglerade detta har upphört att gälla.

Avsnitt 3.1.2 Testtjänst
Inga ändringar som påverkar underskriftstjänsten eller dess funktionalitet.
Krav kring test tjänst har förenklats och detta med anslutning till testfederation har tagits bort.

Avsnitt 3.2 Underskrift som uppfyller kraven på kvalificerade elektroniska underskrifter
När det gäller kvalificerade underskrifter hänvisas nu till eIDAS då tidigare lagstiftning som reglerade detta har upphört att gälla.

Avsnitt 4 Kompletterande krav tjänstehantering
Inga ändringar som påverkar underskriftstjänsten eller dess funktionalitet.
Hela detta avsnitt har flyttats till dokumentet icke funktionella krav.

Avsnitt 4 Förändringar i underskriftstjänsten (tidigare avsnitt 5)
Inga ändringar som påverkar underskriftstjänsten eller dess funktionalitet.
Avsnitt om erfarenhetsutbyte inom federationen har tagits bort.

Avsnitt 5 Definitioner (tidigare avsnitt 6)
Inga ändringar som påverkar underskriftstjänsten eller dess funktionalitet.
Generellt har detta med identitetsfederation tagits bort och eID-systemet har lagts till där det är lämpligt i syfte att ha ett begrepp som talar om alla de olika delar och funktioner som behövs för att genomföra en elektronisk underskrift.
Följande definitioner är tillagda: Användare, E-tjänst, eID-system, Elektroniska legitimering, Elektronisk underskrift, Avancerad elektroniska underskrift, Kvalificerad elektronisk underskrift, Underskriftstjänst, Stödtjänst, eIDAS.

3 POLICY FÖR UNDERSKRIFTSTJÄNST

Avsnitt 1.1 Omfattning
Nytt avsnitt med förtydligande om vilka dokument som ingår i den normativa specifikationen för underskriftstjänsten.

Avsnitt 1.3 Definitioner
Definitioner framgår av dokumentet Normativ specifikation för Underskriftstjänst.

Avsnitt 2.1.2 Lagring av användarrelaterad information
Policy:
Förtydligande av hur personrelaterad information får lagras.

Avsnitt 2.3
Referens till E-legitimationsnämndens tillitsramverk uppdaterad.
Referens till dokumenten Tjänstespecifikation för Underskriftstjänsten när det gäller hantering av tillitsnivåer enligt eIDAS inlagd.

Avsnitt 2.4
Standard för certifikatpolicy är uppdaterad och refererar nu till:
EN 319 411-2 för kvalificerade certifikat samt
EN 319 411-1 för icke kvalificerade certifikat.

4 TJÄNSTESPECIFIKATION UNDERSKRIFTSTJÄNST

Ändringar i dokumentet är nedan markerade med gult. Tillagd text är understruken och borttagen text är överstruken.

Avsnitt 1.6 Styrande förutsättningar

- 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.

Avsnitt 1.7 Avgränsningar

- 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 ~~kunna begära underskrift av underskriftstjänster~~.
- Funktioner för elektronisk legitimering (se nedan).

Avsnitt 1.8 Elektronisk legitimering
Nytt avsnitt
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

Avsnitt 2.1 Sammanfattning

Användare	Fysisk person som har e-legitimation och nyttjar tjänst inom ett eID-systemet. I samband med underskriftstjänsten, specifikt nyttjar e-tjänst i syfte att skriva under elektronisk handling.~~Innehavare av Svensk e-legitimation som skall kunna skriva under en elektronisk handling.~~

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.

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 legitimerar sig ~~legitimeras med stöd av~~ i legitimeringstjänsten ~~genom~~ med sin e-legitimation (Autentisering) ~~samt~~ 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 ~~(SAML Identity Assertion)~~ och returnerar användaren till underskriftstjänsten med identitetsintyget bifogat.
- Underskriftstjänsten kontrollerar identitetsintygets äkthet ~~och~~ samt användarens identitet och avsikt att skriva under ~~genom identitetsintygetsom~~ fastställts vid legitimering.
- E-tjänsten, eventuellt med stöd av ~~lämplig~~ stödtjänst, tar emot svaret från underskriftstjänsten gör en äkthetskontroll och ~~använder denna information för att~~ fogar samman underskriftssvaret med handlingen till en undertecknad elektronisk handling.

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~~ eftersom underskriftsnyckeln ~~inte sparas och aldrig kan komma i orätta händer~~ raderas så fort den har använts och underskriftscertifikatet är utställt.

Avsnitt 2.2 Ingående funktioner

~~Legitimering av användare för underskrift~~

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.

~~Databas~~ Lagrad information om uppdraget
~~Databas~~ Funktioner för lagring av information relaterat till pågående och behandlade underskriftsuppdrag.

2. Inkommen begäran om underskrift kontrolleras. Om begäran om underskrift är OK, skapas ett underskriftsuppdrag ~~i en intern databas~~. 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.
6. Underskriftstjänsten ~~hämtar relevant underskriftsuppdrag från den interna databasen och~~ 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.

Avsnitt 2.4.4 Legitimering av användare för underskrift
Användare som ska skriva under överförs till en legitimeringstjänst för legitimering. ~~Detta kräver att underskriftstjänsten är registrerad som en e-tjänst i en identitetsfederation där legitimeringstjänsten ingår.b~~ Legitimeringstjänstens identitet (entityID) hämtas från den sign request som betjänas. Om specifik legitimeringstjänst specificeras så används denna vid legitimering för underskrift.

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

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 ~~(SAML Assertion)~~ som returneras från legitimeringstjänsten äkthetskontrolleras vid mottagandet ~~av autentiseringsmodulen~~. Underskriftstjänsten kontrollerar ~~sedan att identitetsintyget representerar rätt användare och~~ användarens identitet som säkerställts genom legitimering uppfyller ställda säkerhetskrav samt innehåller nödvändiga uppgifter som krävs för att skapa en underskrift.

En underskriftstjänst som mottar en begäran om underskrift som innehåller underskriftsmeddelande, kontrollerar ~~i federationens metadata~~ om angiven legitimeringstjänst kan visa underskriftsmeddelande. Om så är fallet så begärs alltid legitimering med krav på visning av underskriftsmeddelande.

Avsnitt 2.4.5 Kontroll av legitimerad användares
Den relevanta information om användarens identitet samt avsikt att skriva under som underskriftstjänsten tar emot ~~från~~ 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.

Avsnitt 2.4.10 Lagrad information om uppdraget
~~Databas~~ Lagrad information om uppdraget
Följande information lagras ~~i en eller flera databaser~~ om uppdraget:

~~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~~ Den lagrade informationen om underskriftsuppdraget ~~i databasen~~ innehåller därför information om det tidsfönster inom vilket underskriftsuppdraget får betjänas samt vilka processteg underskriftsuppdraget slutfört. Den lagrade informationen om underskriftsuppdraget kan tas bort ~~från databasen~~ först en tid efter det att giltighetstiden för tillhörande sign request löpt ut. Den lagrade informationen ska skyddas avseende tillgänglighet och integritet.

Avsnitt 3.2 Grafiska gränssnitt
Det grafiska gränssnittet designas för att kunna lämna felmeddelande enligt vad som framgår av avsnitt 4.11. ~~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 inte 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.~~

Not: den borttagna texten i detta avsnitt innebär inte att kraven försvunnit. Kravet framgår förtydligat av avsnitt 4.11.

Avsnitt 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. Denna policy skall dokumenteras och godkännas av E-legitimationsnämnden.

Avsnitt 4.2 Representation i 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 ska vara representerad i ~~federationens~~ metadata i enlighet med metadatakraven i deployment-profil [Eid2-Depl-Prof] så att den bland annat kan identifieras som underskriftstjänst genom att specificera tjänstekategori

Avsnitt 4.3 Kontroll av inkommande sign request
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 skallska kontrolleras mot de underskriftsuppdrag som för närvarande behandlas. Inkommande request skallska inte betjänas om den unika referensen redan förekommer i ~~databasen~~ den lagrade informationen om uppdraget. ~~Denna information~~ Den unika referensen är inte krypterad eller undertecknad och utgör endast ett första skydd mot ofrivillig upprepning (ex, genom page reload).

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 i den lagrade informationen om underskriftsuppdrag. Sign requesten skallska inte betjänas om dess unika identitet representerar ett existerande underskriftsuppdrag ~~i databasen~~. Samtidigt skallska den unika identiteten kontrolleras med avseende på entropi. Underskriftsuppdraget skallska inte accepteras om den unika identiteten representeras av mindre än 64 bitars data.

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

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

Avsnitt 4.4.1 Underskriftsuppdrag och sign request
Information om underskriftsuppdrag ~~och~~ inklusive tillhörande sign request som lagras i underskriftstjänsten ~~databas~~ enligt avsnitten 2.4.10 och 4.3 ska 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.

Specifikation av vilken användarrelaterad information som lagras ~~ingår i den policy som skall dokumenteras och godkännas av E-legitimationsnämnden~~ framgår av dokumentet Policy för Underskriftstjänsten.

Avsnitt 4.4.2 Certifikat
Underskriftstjänsten ska lagra uppgifter om utfärdade certifikat som gör det är möjligt med spärrning av 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~~

Avsnitt 4.5 Signeringsalgoritmer
Underskriftstjänsten skallska kunna stödja signering med ~~följande~~ de algoritmer som framgår av avsnitt ”Godkända signeringsalgoritmer” i dokumentet ”Policy för Underskriftstjänsten”:
~~• RSA med SHA-256~~
~~• ECDSA (baserat på NIST kurvan P-256) med SHA-256~~

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)~~ ska den algoritm som framgår att avsnitt ”Standardalgoritmer för underskrift” i dokumentet ”Policy för underskriftstjänsten” användas. Detta förval skallska dock kunna konfigureras som en del av underskriftstjänstens policy.

Avsnitt 4.7 Legitimering av användare
Användare skallska ~~överföras till~~ legitimeras av den legitimeringstjänst som är angiven i tillhörande sign request. ~~Endast identitetsintyg från denna legitimeringstjänst får accepteras. Legitimering skall begäras i enlighet med [Eid2-Depl-prof] vad gäller krav på underskriftstjänster. Som stöd för detta skall underskriftstjänstens metadata uppfylla kraven i [Eid2-Depl-prof]~~.

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

~~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.~~

Avsnitt 4.7.1 Underskriftsmeddelande
~~Om sign request innehåller ett underskriftsmeddelande (elementet <SignMessage>) så skall detta inkluderas begäran om underskrift i enlighet med [Eid2-Depl-prof].~~
~~Om underskriftsmeddelandet har attributet MustShow satt till true, så skall legitimering endast begäras med en AuthnContextClassRef URI för begärd tillitsnivå som innefattar krav på visning av underskriftsmeddelandet i enlighet med [Eid2-Identifiers].~~

Om sign request innehåller ett underskriftsmeddelande ~~(elementet <SignMessage>sign message)~~ så ska underskriftstjänsten kontrollera ~~i metadata~~ om angiven legitimeringstjänst ~~som avses användas för legitimering~~ stödjer visning av underskriftsmeddelande. Kontroll ska också göras att ~~samt~~ begärd tillitsnivå stöds. Om legitimeringstjänsten stödjer detta så ska legitimering ~~alltid~~ 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 ~~ingen legitimering begäras. Istället så skall underskriften~~ användaren inte legitimeras. Underskriften ska då istället returnera användaren med ett felmeddelande till e-tjänsten som begärt underskrift.

Legitimerings~~begäran~~ utan ~~krav på~~ 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.

Avsnitt 4.7.2 Signature Activation Protocol
Nytt avsnitt
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 skall 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.

Avsnitt 4.7.3 Legitimering med utländsk e-legitimation enligt eIDAS
Nytt avsnitt
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.

Avsnitt 4.8 Kontroll av legitimerad identitet samt avsikt att skriva under

Kontroll av ~~legitimerad användare~~ identitet samt avsikt att skriva under
Användarens identitet som ~~mottagits~~ autentiserats genom ~~identitetsintyg~~ legitimering skallska 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~~ 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 skall denna kontrolleras i enlighet med [ELN-0613].

Avsnitt 4.10 Underskrift
Underskriftstjänsten ska stödja underskrift ~~av XML-dokument samt underskrift av PDF dokument~~ enligt vad som framgår av avsnitt 4.3.1.

Avsnitt 4.11 Felmeddelanden
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.

Avsnitt 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)~~TS 101 456 från ETSI [TS101456]~~ enligt vad som framgår av Policy Underskriftstjänst. ~~Avvikelser från denna policy skall godkännas av E-legitimationsnämnden.~~

Underskriftscertifikat som utfärdas som icke kvalificerade certifikat ska uppfylla certifikatpolicyn EN 319 411-1 [EN319411-1] ~~TS 102 042 från ETSI [TS102042]~~ enligt profilen NCP (Normalized Certificate Policy) enligt vad som framgår av Policy Underskriftstjänst. ~~Avvikelser från denna policy skall godkännas av E-legitimationsnämnden~~

Avsnitt 4.15 Spärrning av certifikat

Spärrning av certifikat ska kunna ske ~~genom att antingen ange det fullständiga certifikat som skall spärras, eller genom att ange det certifikatserienummer som skall spärras~~ baserat på de uppgifter som lagras om certifikatet i underskriftstjänsten.

Avsnitt 7.1 Normativa referenser

[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

~~[XAdES]~~
~~XML Advanced Electronic Signatures, ETSI, December 2010~~

[EN319411-1] ~~[TS101456]~~
Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates;
Part 1: General requirements – Latest published version
~~Policy requirements for certification authorities issuing qualified certificates, ETSI publication TS 101 456 V1.4.3, 2007-05-15~~

[EN319411-2] ~~[TS102042]~~
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
~~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~~

[ETSI EN 319 132]
Electronic Signatures and Infrastructures (ESI); XAdES digital signatures
Part 1: Building blocks and XAdES baseline signatures samt

[ETSI EN 319 142]
Electronic Signatures and Infrastructures (ESI); PAdES digital signatures;
Part 1: Building blocks and PAdES baseline signatures samt

5 ICKE FUNKTIONELLA KRAV

Avsnitt 2 Omfattning
Nytt avsnitt med förtydligande om vilka dokument som ingår i den normativa specifikationen för underskriftstjänsten.

Avsnitt 3 Definitioner
Definitioner framgår av dokumentet Normativ specifikation för Underskriftstjänst.

Avsnitt 4 Underleverantörer
Nytt avsnitt med förtydliganden om krav på underleverantörer.

Avsnitt 5 Tillgänglighet och kapacitet
Uppgifter om behov inom offentlig sektor borttaget. Tillagt i detta avsnitt, som förtydligande, att stöd ska finnas för bråd tid.

Avsnitt 5.1 Svarstider
Förtydligande av externa processer att det är sådan funktion som ligger utanför den funktion som framgår av den Normativa specifikationen för Underskriftstjänsten.

Avsnitt 6.3 Övervakning och kontroll
Förtydliganden om leverantörens ansvar när det gäller rapportering av incidenter och statistik.