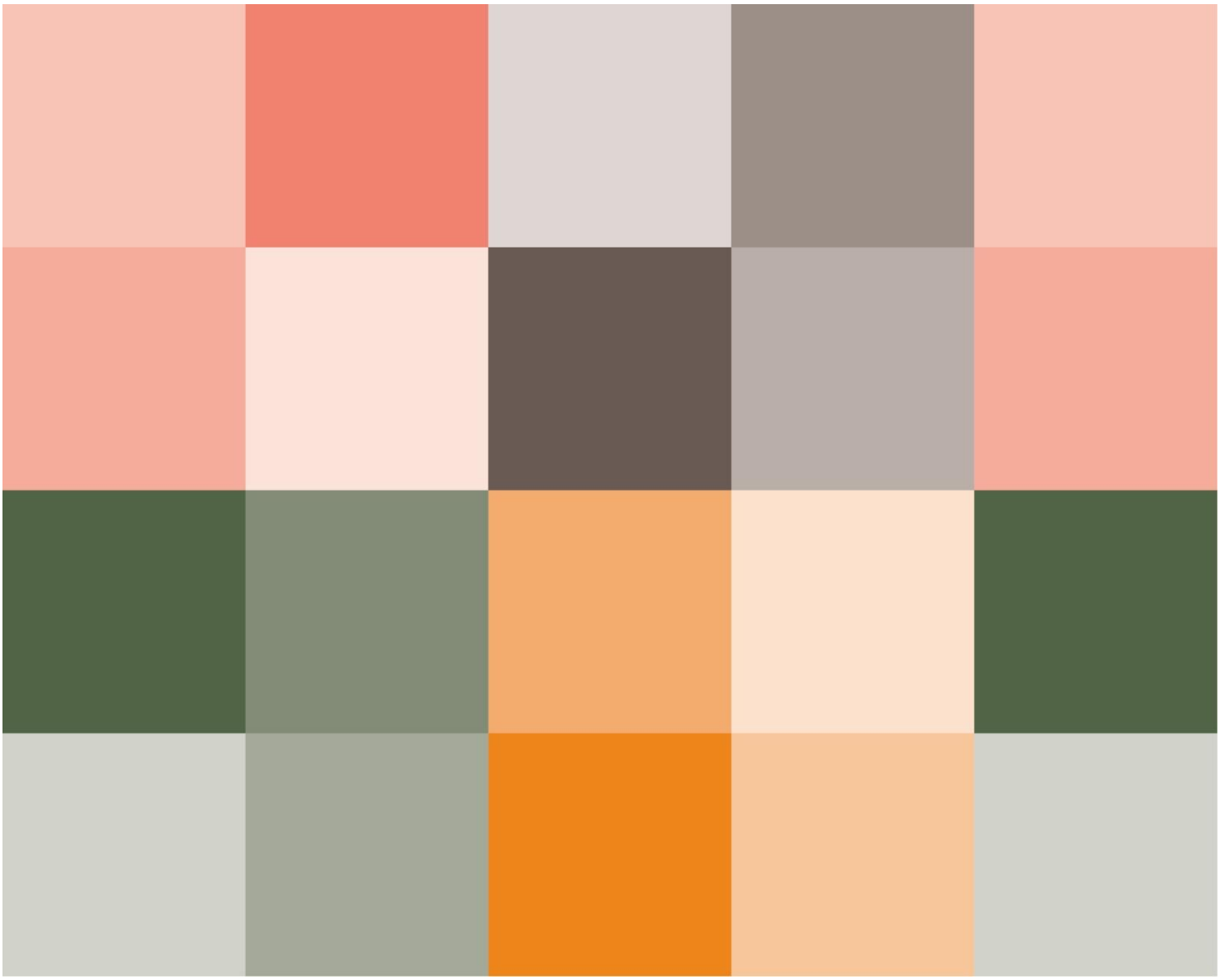

# Ändringshantering

## Normativ specifikation
## Fristående Underskriftstjänst

Version 1.40

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

# Innehållsförteckning

# 1 Inledning

Den normativa specifikationen för fristående underskriftstjänsten har uppdaterats från version 1.3 till version 1.4. Uppdateringen av specifikationen är en mindre uppdatering för att anpassa specifikationen till den senaste versionen av DIGGs tekniskt ramverk. Uppdatering omfattar även vissa förtydliganden. Specifikationen har lagts in i DIGGs dokumentmall och E-legitimationsnämnden har ändrats till DIGG.

Följande viktiga ändringar har gjorts i specifikationen.

- Namnet på tjänsten är ändrat från underskriftstjänst till fristående underskriftstjänst.
- Specifikationen har uppdaterats för att vara följsam till den nya versionen av tekniskt ramverk och tjänsten Sweden Connect.
- Vidare har vissa mindre tekniska ändringar och uppdateringar samma vissa språkändringar och förtydliganden gjorts.

Följande dokument ingår i den normativa specifikationen för underskriftstjänsten.

- Normativ specifikation fristående underskriftstjänst (huvuddokumentet)
- Policy fristående underskriftstjänst
- Tjänstespecifikation fristående underskriftstjänst
- Icke funktionella krav fristående underskriftstjänst

Nedan framgår ändringar som har betydelse för förståelse och för tjänstens funktion i respektive dokument för den normativa specifikationen.

Ändringar är markerade med gult. Tillagd/ändrad text är understruken och borttagen text är ~~överstruken~~.

# 2 Normativ specifikation (huvuddokumentet)

**Avsnitt 1 Inledning**
Text som beskriver tjänsten på en övergripande nivå har lagts till.

**Avsnitt 3 Funktionsprov**
Nytt avsnitt.
Leverantörer av fristående underskriftstjänst kan ansöka hos DIGG att få sin tjänst prövad mot den normativa specifikationen för fristående underskriftstjänst. Funktionsprovet omfattar:

- Tekniska tester av tjänsten i testmiljö
- Avstämning av kravuppfyllnad vid möte med leverantören

Godkänt prov är ett bevis på att tjänsten fungerar som avsett samt att leverantören enligt egen utsago och mot uppvisade bevis kan leverera en tjänst som uppfyller kraven på fristående underskriftstjänsten när provningen genomfördes.
Godkänt genomförd prov medför inte att DIGG tar ansvar för tjänstens funktionalitet när den levereras. Det är alltid upp till beställare av tjänsten att kontrollera att leverantören uppfyller ställda krav.
Leverantörens är alltid ansvarig för levererad tjänst och för att tjänsten uppfyller de krav som framgår att den normativa specifikationen.

**Avsnitt 4.1.2 Testtjänst**
Förtydligande om testtjänst.
Testtjänsten ska vara en spegling av motsvarande produktionstjänst i den bemärkelse att den har samma funktion och samma programvaruversion som tjänsten i produktion.

**Avsnitt 5 Förändringar i fristående underskriftstjänst**
Nytt stycke tre.
Ändringar meddelas på DIGGs webbplats www.digg.se.

**Avsnitt 6 Definitioner**
Användare – definitionen har förtydligats.
Underskriftsprocess – ny definition för att tydliggöra att den fristående underskriftstjänsten är en del i ett större sammanhang för att åstadkomma en elektronisk underskrift.
Fristående underskriftstjänst – ny definition för att tydliggöra den fristående underskriftstjänstens roll i underskriftsprocessen.
Definitionerna underskriftstjänst och stödtjänst har tagits bort.

Underskriftsprocess
En antal samverkande delar som gör att användaren kan skriva under en elektronisk handling. Processen startar med att användaren kommer in i den delen av e-tjänsten som initierar underskrift och slutar med att underskriften är genomförd och den handling som skrivits under är sammanfogad med underskriftscertifikatet på ett kontrollerat sätt.

Fristående underskriftstjänst
Fysiskt avskild del i underskriftsprocessen där användaren kan skriva under en elektronisk handling med en avancerad eller kvalificerad elektronisk underskrift. I den fristående underskriftstjänsten signeras ett kondensat av den handling som skrivs under på ett säkert sätt och ett underskriftscertifikat ställs ut. Vid underskriftstillfället sker legitimering av den fysiska personen i en fristående legitimeringstjänst.
Eng: Sign Service

# 3 Policy

**Avsnitt 2 Policyparametrar**
I tabellen i Datalagring har följande punkt lagts till som förtydligande:
Vilken användarrelaterad information som får lagras av fristående underskriftstjänst.

**Avsnitt 2.1.2 Lagring av användarrelaterad information**
Policy har ändrats:

~~Lagring av personrelaterad information ska begränsas till lagring av certifikat enligt 2.1.1 samt information relaterat till signeringsuppdrag som är felaktiga eller kan misstänkas vara resultatet av en attack mot underskriftstjänsten eller begärande e-tjänst.~~
~~Personrelaterad informationen får lagras maximalt i tre (3) månader, varefter den ska raderas eller avpersonifieras så att alla användarrelaterad information raderas. Detta gäller med följande undantag.~~
~~Lagring av certifikat enligt 2.1.1~~
~~Om händelsen är föremål för polisutredning får informationen lagras så länge som krävs för att stödja utredningen och eventuell efterföljande process i domstol.~~
~~Information som måste sparas i enlighet med svensk lag samt information som måste sparas för att kunna uppfylla ställda säkerhetskrav.~~

Lagring av personrelaterad information ska begränsas till vad som är tillåtet och endast omfatta lagring av certifikat enligt 2.1.1 samt information relaterat till

signeringsuppdrag i den grad som krävs för att understödja utredningar i samband med misstänkta brott.

**Avsnitt 2.2.1 Standardalgoritmer för underskrift**
Stycke ett har förtydligats.

~~Underskriftstjänsten tillämpar en signeringsalgoritm vid underskrift som i sin tur består av en hash-algoritm och en publik-nyckel-algoritm. E-tjänst som begär underskrift kan begära att underskrift ska ske med specifik algoritm. E-tjänsten kan därmed välja en specifik kombination av hash-algoritm och publik-nyckel-algoritm men kan inte specificera nyckellängd för publik-nyckel-algoritmen. Nyckellängd ska väljas i enlighet med policyer nedan.~~

Underskriftstjänsten tillämpar en signeringsalgoritm vid underskrift som i sin tur består av en hash-algoritm, en publik-nyckel-algoritm samt metod för att bereda hash värdet för kryptering med publik-nyckel-algoritmen. E-tjänst som begär underskrift kan begära att underskrift ska ske med specifik algoritm. E-tjänsten kan därmed välja en specifik algoritm men kan inte specificera nyckellängd för publik-nyckel-algoritmen.

Under policy har nyckellängden för RSA-algoritmen tagits bort.
Publik nyckel algoritm: RSA ~~med 2048 bitars nyckel~~

**Avsnitt 2.2.2 Godkända signeringsalgoritmer**
Policy har ändrats enligt följande.

~~Följande algoritmer är godkända för att skapa användares underskrifter samt vid signering av sign request och sign response:~~
~~Hash algoritmer:~~
- ~~SHA-256~~

~~Publik nyckel algoritmer:~~
- ~~RSA med 2048 bitars nyckel~~
- ~~ECDSA där nyckel hämtas från NIST kurvan P-256~~

~~Underskriftstjänsten ska kunna hantera sign requests som signerats med samtliga algoritmer ovan. Signeringsalgoritm för sign response ska alltid vara samma som användes för att signera tillhörande sign request.~~

Algoritmer som tillämpas för elektroniska underskrifter skapade med fristående underskriftstjänst skall följa alla relevanta krav som specificeras i kapitel 8 ”Cryptograhic Algorithms” i Deployment Profile for the Swedish eID Framework, med följande tillägg:

- Underskriftstjänster tillämpar inte metadata för att bestämma vilka algoritmer som tillämpas
- Underskriftstjänster skall kunna hantera signering med RSA-PSS, d.v.s. de algoritmer som definieras av följande identifierare:
  - http://www.w3.org/2007/05/xmldsig-more#sha256-rsa-MGF1
  - http://www.w3.org/2007/05/xmldsig-more#sha384-rsa-MGF1
  - http://www.w3.org/2007/05/xmldsig-more#sha512-rsa-MGF1

**Avsnitt 2.3.2 Lägsta acceptabla tillitsnivå vid underskrift**
Under policy har följande lagts till (anpassning till tekniskt ramverk):

Underskriftstjänsten ska även stödja”uncertified-loa3” enligt kapitel 3.1.1 av ”Swedish eID Framework – Registry for Identifiers”, vilket är en självdeklarerad variant av säkerhetskrav som motsvarar tillitsnivå 3.

**Avsnitt 2.4 Certifikatpolicy**
Stycke ett förtydligat.

~~Underskriftscertifikat innefattar en extension (Certificate policies extension) som ska innehålla en identifierare av en certifikatpolicy. Denna certifikatpolicy har~~

~~som syfte att hjälpa förlitande part att bedöma certifikatets trovärdighet och lämplighet för olika tillämpningar.~~

Certifikatpolicy är en namngiven uppsättning regler som hjälper förlitande part att bedöma certifikatets trovärdighet och lämplighet för en viss gemenskap. Underskriftscertifikat innefattar en extension (Certificate policies extension) som ska innehålla en identifierare av den certifikatpolicy som gäller för tjänsten.

Följande text har lagts till som förtydligande för tolkning av EN-standarderna för utgivande av certifikat:
Krav i EN 319 411-1 samt EN 319 411-2 enligt nedan gäller med följande förtydliganden:

- Fristående underskriftstjänst omfattar endast certifikat för fysisk person, det vill säga krav på certifikat för tjänsteperson, organisation eller fysisk enhet kan bortses från.
- Den som abonnerar på tjänsten och subjektet (den fysiska personen som skriver under) är olika enheter i fristående underskriftstjänst.
- Förnyelse med nyckelbyte (rekey) av certifikat är en funktion som inte stöds i fristående underskriftstjänst.
- Ansvar för identifiering och registrering av fysisk person hanteras av underskriftstjänsten genom att anlita en legitimeringstjänst som uppfyller ställda krav på tillitsnivå. Underskriftstjänsten ansvarar härmed för att begäran av legitimering samt kontroll av identitetsintyg enligt de krav som ställs i gällande certifikatpolicy.
- Leverantören av fristående underskriftstjänst kan välja att i delar inkludera krav av det som framgår av ovanstående förtydliganden utan att frångå standarden EN 319 411-1 eller EN 319 411-2, men det ska då framgå av leverantörens tjänstebeskrivning och CPS.

**Avsnitt 2.4.2 Krav på policy för icke kvalificerade certifikat**
Kravet har ändrats till att tjänsten ska uppfylla profilen NCP+ (Extended Normalized Certificate Policy). I praktiken innebär detta inte några förändrade krav på tjänsten jämfört med föregående version av specifikationen eftersom det redan från början har funnits krav på att tjänsten ska ha en så kallad HSM där krypteringsnycklar för certifikat hanteras.

Bakgrund
Certifikatpolicy för icke kvalificerade certifikat ska uppfylla kraven från standarden EN 319 411-1 enligt profilen NCP+ (Extended Normalized Certificate Policy).

Policy
Underskriftstjänsten ska uppfylla EN 319 411-1 enligt profilen NCP+ (Extended Normalized Certificate Policy).

# 4 Tjänstespecifikation

Referenser har uppdaterats genomgående i dokumentet. Se ändringar gällande avsnitt 7.1 nedan.

**Avsnitt 2.1 Sammanfattning**
Användare – definitionen har förtydligats.
Underskriftsprocess – ny definition för att tydliggöra att den fristående underskriftstjänsten är en del i ett större sammanhang för att åstadkomma en elektronisk underskrift.
Fristående underskriftstjänst – ny definition för att tydliggöra den fristående underskriftstjänstens roll i underskriftsprocessen.
Definitionerna underskriftstjänst har tagits bort.
Stödtjänst – definitionen har förtydligats.

Figur 1 har uppdaterats med fristående underskriftstjänst.

**Avsnitt 2.2 Ingående funktioner**
Figur 2 har uppdaterats med fristående underskriftstjänst.
I förklaringen under figuren har punkt 3 tagits bort.
~~3. Användaren överförs till underskriftstjänstens autentiseringsmodul.~~

**Avsnitt 2.3 Multipla instanser av underskrifttjänsten**
Förtydliganden har gjorts i första stycket.

~~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 tillämpar en rollfördelning där e-tjänsten tillhandahåller funktioner gentemot användaren för att visa och hantera dokument samt sända och ta emot signeringsmeddelanden till underskriftstjänsten. Underskriftstjänsten agerar i detta avseende som underleverantör till e-tjänsten. Underskriftstjänsten ställer ut underskriftscertifikat och tillhandahålla bland annat funktioner för spärrinformation gentemot förlitande part.

**Avsnitt 2.4.4 Legitimering av användare för underskrift**
Sista meningen i stycke fem har tagits bort.
~~Legitimeringskontext specificerar som minst en tillitsnivå men kan även specificera krav på visning av underskriftsmeddelande i legitimeringsprocessen.~~

**Avsnitt 4.2 Representation i metadata**
Första stycket tjänstekategori har ändrats:
http://id.elegnamnden.se/st/1.0/sigservice

Stycket två entitetskategorier nytt stycke:
Bland annat följande entitetskategorier (se [Eid-EntCat]) ska anges i metadata i enlighet med tjänstens roll och avtal:

- Deklaration av om tjänsten representerar publik eller privat aktör (För att möjliggöra användning mot den svenska eIDAS-noden). Exempelvis:
  - `http://id.elegnamnden.se/st/1.0/public-sector-sp`
- Deklaration av ”service entity category” som bl.a. avgör vilka attribut som returneras från legitimeringstjänst.
  - Ex: `http://id.elegnamnden.se/ec/1.0/loa3-pnr`
    - För legitimering mot legitimeringstjänster inom valfrihetssystemet.
  - `http://id.elegnamnden.se/ec/1.0/eidas-naturalperson`
    - För legitimering mot den svenska eIDAS-noden.
  - `http://id.swedenconnect.se/ec/sc/uncertified-loa3-pnr`
    - För legitimering mot andra legitimeringstjänster inom Sweden Connect som myndigheten har avtal med.

Stycke fyra unika nyckelpar nytt stycke:
Underskriftstjänsten ska använda ett unikt nyckelpar per SAML-instans, nyckelmaterial mellan olika logiska SAML-instanser ska således inte delas.

**Avsnitt 4.3 Anslutning till Sweden Connect**
Nytt avsnitt.

Underskriftstjänsten ska i samverkan med respektive till underskriftstjänsten ansluten e-tjänst publicera SAML metadata för underskriftstjänsten till Sweden Connect-federationen.

Underskriftstjänstens SAML-instans ska periodiskt ladda ned giltig metadata från Sweden Connect-federationen och använda denna information vid kommunikation med legitimeringstjänster inom Sweden Connect.

Underskriftstjänsten ska inte vara beroende av manuell uppdatering av SAML metadata.

**Avsnitt 4.4.1.3 PDF Signatur**
Stycke tre och fyra nytt.

Om tidpunkt för underskrift som anges i signed attributes (OID 1.2.840.113549.1.9.5) inte är acceptabel, så ska fristående underskriftstjänst inte genomföra underskrift av detta dokument utan ska istället returnera ett felmeddelande till e-tjänst som begärt underskrift.

CMS Algorithm Protection signed attribute (OID 1.2.840.113549.1.9.52) enligt RFC 6211 som ingår i sign request skall stödjas och införas i signaturen under förutsättning att deklarerade algorithmer är i överensstämmelse med skapad underkrift. Detta attribut bör alltid införas i signed attributes i skapad underskrift även om det inte skickades med i sign request.

**Avsnitt 4.4.1.4 PAdES Signatur**
Tidigare stycke två ersatt med ny text.

~~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.~~

För PAdES gäller samma krav på signed attributes som för PDF signatur med undantag för tidpunkt för underskrift som inte får inkluderas som signed attribute i PAdES signaturer enligt ETSI EN 319 142.

**Avsnitt 4.5.1 Underskrifsuppdrag och sign request**
Tidigare stycke två och tre ersatt med ny text i stycke två.

~~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.~~

Information om underskriftsuppdrag inklusive tillhörande sign request som lagras i underskriftstjänsten enligt avsnitten 2.4.10 och 4.3 ska raderas så snart detta är möjligt i enlighet med kraven som framgår av dokumentet Policy fristående underskriftstjänst.

**Avsnitt 4.5.2 Certifikat**
Nytt stycke tre.
Lagring av certifikat ska ske i enlighet med kraven som framgår av dokumentet Policy fristående underskriftstjänst.

**Avsnitt 4.8 Legitimering av användare**
Nytt stycke sex.
Då en legitimeringsbegäran skapas till en Identity Provider som annonserar i metadata att denne vill ta emot PrincipalSelection-extension ska denna extension användas enligt kapitel 7.2 [Eid-Depl-Prof]. Se också [Eid-Princ-Select].

**Avsnitt 4.8.1 Underskriftsmeddelande**
Sista meningen stycke ett borttagen.
~~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].~~

Nytt stycke fem.
Notera: De specifika "Sign Message Authentication Context" URI:er som tidigare användes för att indikera krav på visning av underskriftsmeddelande och som bevis på visat meddelande ska inte längre användas. Se kapitel 7.2.1 av [Eid-Depl-Pro] och kapitel 2.1.3.8.2 av [Eid-DSS-Pro].

**Avsnitt 4.13 Utfärdande av certifikat**
Nytt stycke tre.
Underskriftstjänsten ska stödja lagring av utökad autentiserings¬information (element <sacex:ExtAuthInfo>) enligt kapitel 2.3.2.1 [Eid-Cert-Prof]. Det ska vara möjligt för en given e-tjänst att konfigurera vilken information som skall ingå i utökad autentiseringsinformation.

**Avsnitt 4.13.1 Utfärdarrutiner**
Tidigare text ersatt.

~~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.~~

Underskriftscertifikat som utfärdas av underskriftstjänsten skall tillämpa certifikatpolicy i enlighet med dokumentet Policy fristående underskriftstjänst, avsnitt 2.3.

**Avsnitt 4.14 Certifikathierarki**
Nytt stycke två.
Om underskriftstjänsten byter rotcertifikat ska detta meddelas anslutna e-tjänster i förväg.

**Avsnitt 4.16 Spärrning av certifikat**
Nytt stycke tre.
Leverantören av underskriftstjänst ska tillhandahålla det certifikat som används för att signera ett signeringssvar (sign response) via säkra kanaler till ansluten e-tjänst. Om underskriftstjänsten uppdaterar eller byter detta certifikat ska det meddelas anslutna e-tjänster i förväg.

**Avsnitt 4.18 Algoritmer**
Tidigare text ersatt.

~~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 4.6, 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~~ |

Vid legitimering av användare i samband med underskrift ska underskriftstjänsten följa och stödja de algoritmer som framgår av kapitel 8 ”Cryptograhic Algorithms” [Eid2-Depl-pProf], det gäller även de algoritmer som är valbara (optional).
Dessa krav gäller även val av algoritmer för signering av sign response, sign request samt för annan signering och kryptering av protokollelement så som sign message eller Signature Activation Protocol (SAP) data.
Krav på algoritmer som tillämpas för elektroniska underskrifter skapade med underskriftstjänsten ska följa de krav som specificeras i dokumentet Policy fristående underskriftstjänst.

### Avsnitt 7.1 Normativa referenser

Nytt stycke tre.
För referenser som är angivna utan versionsnummer gäller att det är senaste publicerade versionen av referensen som gäller. Referenser med ett Eid-prefix är specifikationer som är en del av DIGG:s tekniska ramverk.

Referenser uppdaterade enligt följande.

| [DIGG-Tillit] | **Tillitsramverk för kvalitetsmärket Svensk e-legitimation.** |
|---|---|
| **[Eid-Cert-Prof]** | Certificate Profile for Certificates Issued by Central Signing Services. |
| **[Eid-Registry]** | Swedish eID Framework - Registry for identifiers. |
| **[Eid-Depl-Prof]** | Deployment Profile for the Swedish eID Framework. |
| **[Eid-DSS]** | DSS Extension for Federated Central Signing Services. |
| **[Eid-DSS-Prof]** | Implementation Profile for using OASIS DSS in Central Signing Services. |
| **[Eid-Princ-Select]** | Principal Selection in SAML Authentication Requests. |
| **[Eid-SigAct]** | Signature Activation Protocol for Federated Signing. |
| **[Eid-EntCat]** | Entity Categories for the Swedish eID Framework. |
| **[EN319411-1]** | Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements |
| **[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 |

| | |
|---|---|
| **[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 |
| **[CMS]** | R. Housley. Cryptographic Message Syntax (CMS), IETF (Internet Engineering Task Force) RFC 5652, September 2009 |
| **[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 |
| **[RFC 6211]** | J. Schaad, "Cryptographic Message Syntax (CMS) Algorithm Identifier Protection Attribute", RDC 6211, April 2011 |
| **[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. |

# 5 Icke funktionella krav

Ändringar som påverkar tjänstens funktion är nedan markerade med gult.
Tillagd/ändrad text är understruken och borttagen text är överstruken.

**Avsnitt 4 Underleverantör**
Tidigare text ersatt.

~~För det fall Leverantören av underskriftstjänsten använder underleverantör för att tillhandahålla underskriftstjänsten ska det genom avtal med underleverantören säkerställas att underleverantören i sina delar uppfyller de krav som framgår av denna Normativa specifikation för Underskriftstjänst. Leverantören av underskriftstjänsten ska också kunna visa att denne har den övergripande kontrollen som krävs för att leverera underskriftstjänsten, speciellt när det gäller säkerhet och behandling av personuppgifter.~~

Leverantören av underskriftstjänsten kan använda underleverantör för att tillhandahålla hela eller delar av tjänsten. Att använda underleverantör fråntar inte leverantören ansvar för tillhandahållande av tjänsten. Leverantören har ett helhetsansvar för tjänsten och ansvarar för underleverantörens arbete såsom sitt eget.

Med underleverantör avses en juridisk person som leverantören anlitar för att utföra hela eller delar av underskriftstjänsten. Underleverantören ska fullgöra sina delar av tjänsten enligt den normativa specifikationen för fristående underskriftstjänst.

Leverantören ska ha skriftligt avtal med underleverantör som utför väsentlig del av tjänsten. Med väsentlig del avses stor eller viktig del av tjänsten eller del som påverkar eller kan påverka informationssäkerheten i tjänsten. Exempel på väsentliga delar är drift av tjänsten, behandling av personuppgifter, viktig funktionell del eller säkerhetsrelaterad funktion i tjänsten.

Avtalet ska visa att leverantören har den kontroll som krävs för att säkerställa att de krav som finns på tjänsten uppfylls. Avtalet ska säkerställa att de krav som framgår av den normativa specifikationen för fristående underskriftstjänsten är väl kända och följs av underleverantören i relevanta delar. Varje underleverantör ska ha god kunskap om och följa de krav som ställs på tjänsten genom de policyer, regler och processer som leverantören har för tjänsten.

Leverantören och dess underleverantörer bildar den organisation som tillhandahåller tjänsten, detta benämns också för den verksamhet som tillhandahåller tjänsten. De krav som framgår av avsnitt 6 gäller för den organisation som tillhandahåller tjänsten.

Det ska finnas en beskrivning över den organisation som tillhandahåller tjänsten inklusive de parter som ingår i organisationen och deras respektive ansvar.

Kund ska ha möjlighet att teckna avtal direkt med såväl leverantör som underleverantör avseende till exempel behandling av personuppgifter.

**Avsnitt 5 Tillgänglighet och kapacitet**
Tillagt i slutet av stycke två.
med överenskommen kapacitet.

**Avsnitt 5.1 Svarstider**
Första stycket ändrad formulering

~~Följande krav på svarstider ska gälla för underskriftstjänsten såvida inte annat framgår av enskilt avrop/leverans.~~

Följande krav på svarstider ska gälla som riktvärden för underskriftstjänsten.

**Avsnitt 6.1.1 Policy och processer**
Första stycket förtydligat.

~~Säkerhetspolicy, processer och rutiner som omfattar informationssäkerhetsarbetet, hantering av risker och förbättring av informationssäkerheten ska finnas. Dessa ska vara baserade på ISO-27001 eller motsvarande.~~

Leverantören av underskriftstjänsten ska ha ett dokumenterat och infört ledningssystem för informationssäkerhet som omfattar den verksamhet som tillhandahåller tjänsten. Det ska finnas säkerhetspolicy, dokumenterade processer och rutiner som omfattar informationssäkerhetsarbetet, hantering av risker, uppföljning och förbättring av informationssäkerheten. Ledningssystemet ska vara baserade på ISO-27001 eller likvärdigt.

**Avsnitt 6.2.1 Riskanalys**
Ny text i slutet av stycke två.
Riskanalyser ska genomföras med återkommande intervall. Som underlag för riskanalysen ska finnas en krav- och intressentanalys och uppföljning av riskanalysen ska innefatta en värdering av vidtagna åtgärder och ett formellt utverkande av riskägarens acceptans av kvarvarande risk.

**Avsnitt 6.2.2 Uppföljning/revision**
Nytt avsnitt.
Leverantörens styrning och ledning av informationssäkerhetsarbetet och den egna internkontrollen är centrala delar för att säkerställa leverantörens efterlevnad gentemot ställda krav över tid. Revision av ledningssystemet och säkerheten i tjänsterna ska genomföras med kontinuerliga intervaller enligt plan. Den som utför revision ska har relevant kompetens samt vara oberoende till den verksamhet som hanterar underskriftstjänsten.

**Avsnitt 7.1.2 Skalskydd och tillträde**
Stycke ett förtydligat.
~~Leverantören ska använda skalskydd för skydd av de lokaler som omfattar att tillhandahålla underskriftstjänsten.~~
Leverantören ska användaDet ska finnas skalskydd för som skyddar av de lokaler som omfattar används för att tillhandahålla underskriftstjänsten.

Nytt stycke tre.
Utveckling och test av den fristående underskriftstjänsten ska ske i skyddade miljöer där åtkomst är begränsad till dem som behörigen ska ha tillträdde.

Stycke sex förtydligat.
~~Besökare som inte är anställda av Leverantören och som vistas innanför skalskyddet ska åtföljas.~~
Besökare som inte är behöriga att vistas innanför skalskyddet kan tillåtas tillträde men ska då åtföljas av behörig person.

**Avsnitt 7.2.1 Datasäkerhet**
Stycke ett standard för HSM tillagd.
Underskriftsnycklar samt nycklar för signering av certifikat och spärrlistor, ska skapas och användas i en kvalificerad anordning, så kallad säker hårdvarumodul (HSM), som lägst är certifierad enligt FIPS 140-2 nivå 3 eller EN 419 221-5.

Stycke 13 ändrat från TLS version 1.1 till 1.2
Extern kommunikation mot tjänsten ska ske enligt TLS standarden version 1.2 eller högre.

Stycke 16 attackmönster tillagt.
Systemet ska vara skyddat mot CSRF-attacker (Cross Site Request Forgery), XSS (Cross Site Scripting), och injektionsbaserade attacker och motsvarande kända attackmönster.