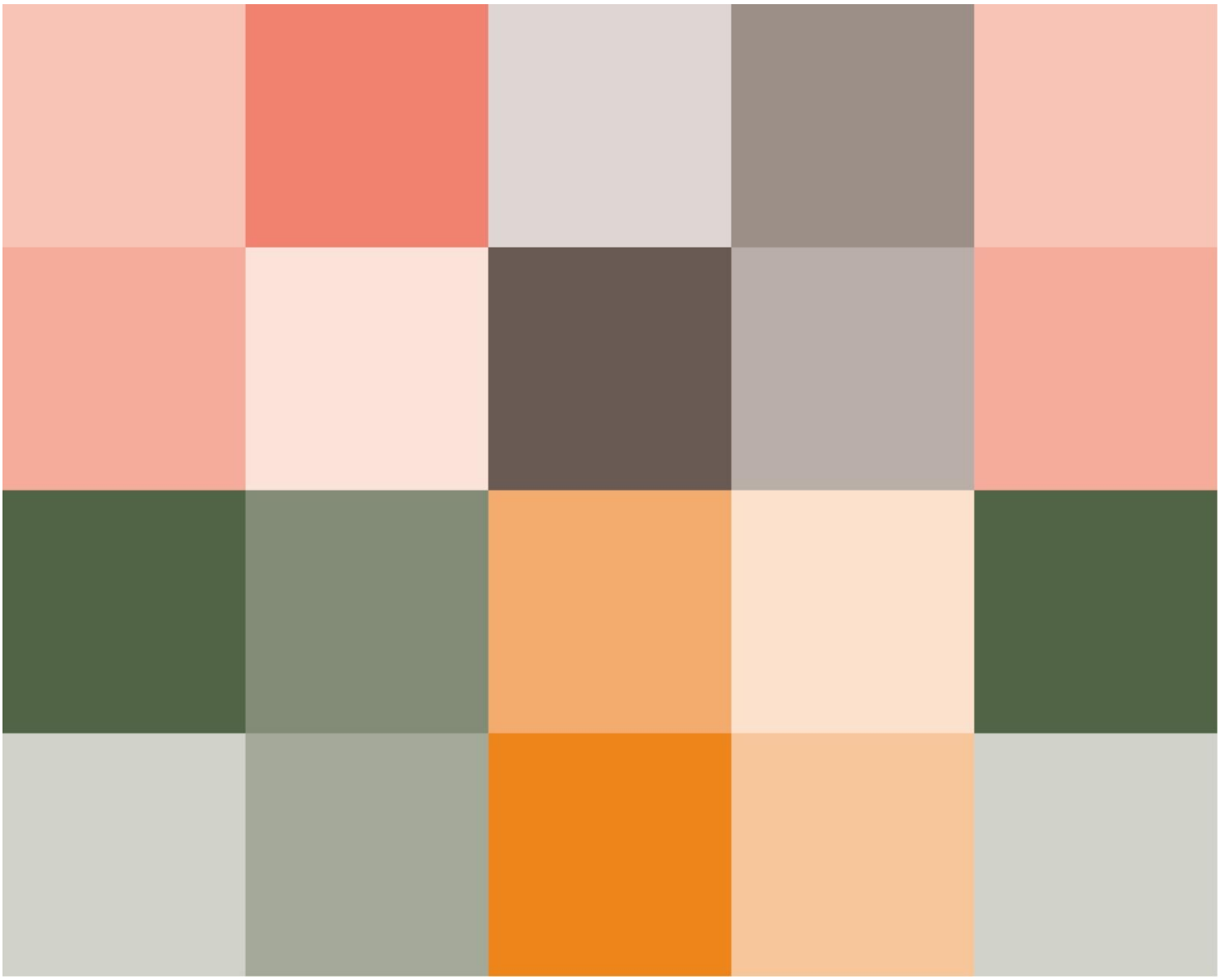

Normativ specifikation

Fristående Underskriftstjänst

Policy fristående underskriftstjänst

Version 1.40

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Innehållsförteckning

Versionshantering

Version	Datum	**Beskrivning**	Sign
1.00	2014-04-15	Första fastställda versionen	E-legitimations-nämnden
1.20	2015-09-15	Uppdatering av versionsnummer för att följa versionsnummer i den normativa specifikationen för underskriftstjänsten. Rättning av stavfel i text.	E-legitimations-nämnden
1.30	2018-08-01	Knytningar till Svensk e-legitimation borttaget. Referens till Tjänstespecifikation när det gäller tillitsnivåer enligt eIDAS inlagd i avsnitt 2.3. Uppdatering av standarder för certifikatpolicy i avsnitt 2.4. Språkliga justeringar.	E-legitimations-nämnden
1.40	2020-04-22	Dokumentet inlagt i DIGGs dokumentmall och E-legitimationsnämnden ändrat till DIGG. Underskriftstjänst ändrat till fristående underskriftstjänst. Anpassningar gjorda till den senaste versionen av DIGGs tekniska ramverk vilket bland annat omfattar förtydligande avseende algoritmer avsnitt 2.2, tillägg för stöd av uncertified-loa3 i avsnitt 2.3.1. Förtydliganden om certifikatpolicy gjord i avsnitt 2.4.	DIGG

1 Inledning och syfte

Fristående underskriftstjänst (i det fortsatta även benämnt underskriftstjänsten) ger möjlighet att med hög säkerhet genomföra elektronisk underskrift med stöd av e-legitimationer.

Detta dokument specificerar värden för parametrar som påverkar tjänstens funktion och som i enlighet med gällande funktionella krav ska vara konfigureringsbara och föränderliga över tid.

Värden för parametrar som definieras i detta dokument förvaltas och bestäms av DIGG.

1.1 Omfattning

Detta dokument är en del av den Normativa specifikationen för fristående underskriftstjänst vilken sammantaget omfattar de krav som ställs på fristående underskriftstjänst.
Den Normativa specifikationen för Fristående underskriftstjänst omfattar följande dokument:

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

1.2 Avgränsningar

Detta dokument specificerar endast vissa funktionella parametrar. Med funktionella parametrar avses parametrar som styr hur underskriftstjänsten fungerar och som enligt uppställda krav på underskriftstjänsten ska vara konfigureringsbara.

1.3 Definitioner

De definitioner som framgår av dokumentet Normativ specifikation för fristående underskriftstjänst gäller.

2 Policyparametrar

Följande policyparametrar specificeras i detta dokument:

Kategori	Policy Parametrar
Datalagring	• Vilka data som får lagras som underlag för att kunna spärra underskriftscertifikat. • Vilken användarrelaterad information som får lagras av fristående underskriftstjänst.
Algoritmer	• Vilken användarrelaterad information som får lagras av fristående underskriftstjänst. • Standardalgoritm för underskrift om ingen anges i sign request. • Algoritmer som får accepteras om de begärs i en sign request.
Tillitsnivå	• Normal tillitsnivå som ska begäras vid legitimering för underskrift om inget anges i sign request. • Lägsta tillitsnivå som får användas vid legitimering för underskrift.
Certifikatpolicy	• Krav på certifikatpolicyn för kvalificerade certifikat som utfärdas av fristående underskriftstjänst. • Krav på certifikatpolicyn för icke-kvalificerade certifikat som utfärdas av fristående underskriftstjänst.
Underskriftsbegäran	• Maximal giltighetstid som en sign request får ha angivet för att accepteras av fristående underskriftstjänst. • Maximal tidsavvikelse mellan angiven tid för underskrift i sign request och aktuell tidpunkt för hanteringen av uppdraget (gäller särskilt data för underskrift i samband med underskrift av PDF).

2.1 Datalagring

Detta avsnitt behandlar parametrar rörande lagring av data i underskriftstjänst.

2.1.1 Lagring av information till stöd för spärrning av certifikat

Bakgrund:
Underskriftstjänster behöver lagra viss information om utfärdade certifikat för att kunna spärra utfärdade certifikat vid behov. Många existerande programvaror som används för att skapa spärrlistor kräver tillgång till de certifikat som ska spärras för att kunna spärra dem.

Policy:
Underskriftstjänster får lagra samtliga utfärdade certifikat tillsammans med systemloggar. Systemloggar ska inte innehåller personrelaterad information.

För spärrade certifikat och certifikat under spärrning får nödvändig information om omständigheter runt spärrning lagras som stöd för framtida tvister och utredningar.

2.1.2 Lagring av användarrelaterad information

Bakgrund:
Grundprincipen vad gäller lagring av personrelaterad information i underskriftstjänsten är att detta ska ske i så liten utsträckning som möjligt. Underskriftstjänstens protokoll är utformat så att all relevant information om varje underskrift överförs till e-tjänsten som begär underskrift.

Policy:
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.

2.2 Algoritmer

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.

2.2.1 Standardalgoritmer för underskrift

Bakgrund:
Då en e-tjänst inte specificerar val av algoritm så ska underskriftstjänsten välja att använda konfigurerad standardalgorim.

Policy:
Följande signeringsalgoritm tillämpas vid skapande av användares underskrift om inget annat anges i signeringsuppdragets sign request.

Hash algoritm:	SHA-256
Publik nyckel algoritm:	RSA

2.2.2 Godkända signeringsalgoritmer

Bakgrund:
Om e-tjänst som begär underskrift begär specifik signeringsalgoritm i underskriftsuppdraget så måste begärd signeringsalgoritm överensstämma med ett antal godkända algoritmer:

Policy:
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

2.3 Tillitsnivå

Tillitsnivåer som anges i detta avsnitt avser de tillitsnivåer som framgår av DIGGs Tillitsramverk för kvalitetsmärket Svensk e-legitimation och som ska användas när legitimering sker med svensk e-legitimeringstjänst. E-tjänst kan genom protokoll för begäran av underskrift begära en lägsta tillåten nivå för legitimering av användare i samband med begärd underskrift.

Om legitimering sker med utländsk e-legitimering via den svenska eIDAS-noden Sweden Connect gäller tillitsnivåer enligt eIDAS. Hur detta ska hanteras framgår av dokument Tjänstespecifikation fristående underskriftstjänst.

2.3.1 Normal tillitsnivå vid legitimering vid underskrift

Bakgrund:
Då en e-tjänst inte specificerar val av tillitsnivå så ska underskriftstjänsten välja att använda konfigurerad lägsta tillitsnivå.

Policy:
Legitimering av användare i samband med underskrift ska ske med tillitsnivå 3 eller högre om inget annat anges i begäran om underskrift från e-tjänsten.

2.3.2 Lägsta acceptabla tillitsnivå vid underskrift

Bakgrund:
Om e-tjänst som begär underskrift begär specifik lägsta acceptabla tillitsnivå i underskriftsuppdraget så måste denna tillitsnivå även uppfylla konfigurerad lägsta acceptabla tillitnivå i underskriftstjänsten.

Policy:
Om underskriftscertifikatet utfärdas som ett kvalificerat certifikat ska användaren legitimeras med lägst tillitsnivå 3.

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.

Om underskriftscertifikatet utfärdas som icke kvalificerat certifikat ska användaren legitimeras med lägst tillitsnivå 2 under förutsättning att detta inte strider mot den certifikatpolicy som deklareras i underskriftscertifikatets certifikatpolicyextension.

2.4 Certifikatpolicy

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.

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.

2.4.1 Krav på policy för kvalificerade certifikat

Bakgrund:
Certifikatpolicy för kvalificerade certifikat ska uppfylla kraven från standarden EN 319 411-2 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).

Policy:
Underskriftstjänsten ska uppfylla EN 319 411-2 enligt profilen QCP-n-qscd.

2.4.2 Krav på policy för icke kvalificerade certifikat

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).

2.5 Underskriftsbegäran

Detta avsnitt behandlar parametrar rörande underskriftsbegäran från e-tjänst genom en sign request.

2.5.1 Maximal giltighetstid för sign request

Bakgrund:
Underskriftsbegäran i form av en sign request innehåller ett SAML element <conditions> som bl.a. innehåller uppgift om det tidsfönster (giltighetstid) inom vilket underskriftsbegäran ska anses vara giltig enligt begärande e-tjänst. Underskriftstjänsten ska kontrollera att en underskriftsbegäran behandlas under sin giltighetstid men även att angiven giltighetstid är inom giltiga ramar.

Giltighetstiden styr hur länge som underskriftstjänsten behöver spara underskriftsbegäran för att säkerställa att samma underskriftsbegäran inte behandlas flera gånger.

Styrande faktorer för hur giltighetstid bör begränsas är dels att hålla tiden kort så att underskriftstjänsten behöver hålla reda på så få aktiva underskriftsuppdrag som möjligt, men ändå så lång att användaren hinner genomföra legitimering och eventuella slutgiltiga kontroller innan legitimering för underskrift fullbordas.

Policy:
En sign request får ha en maximal giltighetstid på 10 minuter.

2.5.2 Maximal tidsavvikelse för angiven tidpunkt för underskrift

Bakgrund:
I vissa underlag för underskrift som ingår i elementet <dss:InputDocuments> i en sign request, bl.a. i underlag för underskrift av PDF, kan det ingå en tidsangivelse för när underskriften skapades. Denna tidpunkt signeras i underskriftsprocessen och ska därför kontrolleras så att den inte avviker från verklig tidpunkt för underskrift utöver en maximal godkänd tidsavvikelse.

Hänsyn bör här tas till den tid hela underskriftsprocessen kan ta, inklusive tid för användarens legitimeringsprocess.

Policy:
Uppgift om tidpunkt för underskrift som ingår i underlag för underskrift i sign request får ha en maximal avvikelse på 15 minuter från verklig tidpunkt för skapande av underskrift.