E-LEGITIMATIONS NÄMNDEN

Policy Underskriftstjänst

Version 1.30
2018-08-01

Versionshantering

Version	Datum	Beskrivning	Sign
1.00	2014-04-15	Första fastställda versionen	E-legitimationsnämnden
1.20	2015-09-15	Uppdatering av versionsnummer för att följa versionsnummer i den normativa specifikationen för underskriftstjänsten. Rättning av stavfel i text.	E-legitimationsnämnden
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-legitimationsnämnden

E-LEGITIMATIONS NÄMNDEN

1 Inledning och syfte

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

Detta dokument specificerar värden för parametrar som påverkar underskriftstjänstens 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 E-legitimationsnämnden.

1.1 Omfattning

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

Den Normativa specifikationen för Underskriftstjänsten omfattar följande dokument:

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

E-LEGITIMATIONS NÄMNDEN

2 Policyparametrar

Följande policyparametrar specificeras i detta dokument:

Kategori	Policy Parametrar
Datalagring	• Vilka data som får lagras som underlag för att kunna spärra underskrifts-certifikat.
Algoritmer	• Vilken användarrelaterad information som får lagras av underskriftstjäns-ten. • 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 under-skriftstjänsten. • Krav på certifikatpolicyn för icke-kvalificerade certifikat som utfärdas av underskriftstjänsten.
Underskriftsbegäran	• Maximal giltighetstid som en sign request får ha angivet för att accepteras av underskriftstjänsten. • Maximal tidsavvikelse mellan angiven tid för underskrift i sign request och aktuell tidpunkt för hanteringen av uppdraget (gäller särskilt data för under-skrift 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 som 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 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.

2.2 Algoritmer

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.

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 med 2048 bitars nyckel**

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:

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.

2.3 Tillitsnivå

Tillitsnivåer som anges i detta avsnitt avser de tillitsnivåer som framgår av E-legitimationsnämndens Tillitsramverk (ELN-0700-v1.4) 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 Tjänstespecifikationen för Underskriftstjänsten.

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.

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

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.

2.4.1 Krav på policy för kvalificerade certifikat

Bakgrund:

Grundkravet på certifikatpolicy för kvalificerade certifikat är att dessa 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:

Alla krav i EN 319 411-2 enligt profilen QCP-n-qscd ska vara uppfyllda.

2.4.2 Krav på policy för icke kvalificerade certifikat

Bakgrund:

Grundkravet på certifikatpolicy för icke kvalificerade certifikat är att dessa ska uppfylla kraven från standarden EN 319 411-1 enligt profilen NCP (Normalized Certificate Policy).

Policy:

Alla krav i EN 319 411-1 enligt profilen NCP (Normalized Certificate Policy) ska vara uppfyllda.

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.