LEGITIMATIONS NÄMNDEN

Policy Underskriftstjänst
Svensk e-legitimation

Version 1.20
2015-09-15

www.elegnamnden.se

Postadress	Besöksadress	Telefon växel	E-postadress
171 94 SOLNA	**Korta gatan 10**	**010-574 21 00**	**kansliet@elegnamnden.se**

1 INLEDNING OCH SYFTE 3
1.1 AVGRÄNSNINGAR 3
1.2 DEFINITIONER 3
2 POLICYPARAMETRAR 4
2.1 DATALAGRING 4
2.1.1 LAGRING AV INFORMATION TILL STÖD FÖR SPÄRRNING AV CERTIFIKAT 4
2.1.2 LAGRING AV ANVÄNDARRELATERAD INFORMATION 4
2.2 ALGORITMER 5
2.2.1 STANDARDALGORITMER FÖR UNDERSKRIFT 5
2.2.2 GODKÄNDA SIGNERINGSALGORITMER 5
2.3 TILLITSNIVÅ 6
2.3.1 STANDARD TILLITSNIVÅ VID LEGITIMERING VID UNDERSKRIFT 6
2.3.2 LÄGSTA ACCEPTABLA TILLITSNIVÅ VID UNDERSKRIFT 6
2.4 CERTIFIKATPOLICY 6
2.4.1 GODKÄNDA AVVIKELSER FÖR KVALIFICERADE CERTIFIKAT 6
2.4.2 GODKÄNDA AVVIKELSER FÖR ICKE KVALIFICERADE CERTIFIKAT 6
2.5 UNDERSKRIFTSBEGÄRAN 7
2.5.1 MAXIMAL GILTIGHETSTID FÖR SIGN REQUEST 7
2.5.2 MAXIMAL TIDSAVVIKELSE FÖR ANGIVEN TIDPUNKT FÖR UNDERSKRIFT 7

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 Inledning och syfte

Underskriftstjänsten är en del av infrastrukturen för Svensk e-legitimation som stöd för att ge användare av offentliga e-tjänster en möjlighet att skriva under elektroniska handlingar. Denna underskriftstjänst tillhandahålls av ett antal leverantörer i enlighet med gemensamma specifikationer som har till syfte att skapa enhetliga och kompatibla tjänster för offentlig förvaltning.

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

Värden för funktionella parametrar som definieras i detta dokument förvaltas och bestäms av E-legitimationsnämnden i en löpande förvaltningsprocess.

1.1 Avgränsningar

Detta dokument specificerar endast funktionella parametrar. Med funktionella parametrar avses parametrar som styr hur underskriftstjänsten fungerar och som enligt uppställda krav på underskriftstjänsten har definierats med krav på att kunna vara konfigureringsbara.

Detta innefattar inte icke-funktionella aspekter av underskriftstjänsten som säkerhetskrav och krav på tillgänglighet mm.

Detta dokument utgör således inte en komplett kravspecifikation för tjänsterna.

1.2 Definitioner

För detta dokument gäller tillämpliga definitioner som anges i Regelverket för Svensk e-legitimation.

LEGITIMATIONS NÄMNDEN

2 Policyparametrar

Följande policy parametrar specificeras i detta dokument:

Kategori	Policy Parametrar
Datalagring	• Vilka data får lagras som underlag för att kunna spärra underskriftscertifikat
Algoritmer	• Vilken användarrelaterad information får lagras av underskriftstjänsten. • Standardalgoritm för underskrift om ingen anges i sign request • Godkända algoritmer som får accepteras om de begärs i en sign request.
Tillitsnivå	• Standard tillitsnivå som skall begäras vid legitimering för underskrift om inget anges i sign request • Lägsta tillitsnivå som får användas vid legitimering för underskrift.
Certifikatpolicy	• Eventuella godkända avvikelser från certifikatpolicyn TS 101456 för kvalificerade certifikat som utfärdas av underskriftstjänsten. • Eventuella godkända avvikelser från certifikatpolicyn TS 102042 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 underskrift i samband med PDF signatur).

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 skall 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 skall 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 skall 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.

Om incidenten är föremål för polisutredning får informationen lagras så länge som krävs för att stödja utredningen och eventuell efterföljande process i domstol. I annat fall får informationen i sin helhet endast lagras i tre (3) månader, varefter den måste raderas eller avpersonifieras så att alla användarrelaterad information raderas.

Generellt undantag för ovanstående policy är information som måste sparas i enlighet med svensk lag samt information som måste sparas för att kunna uppfylla ställda säkerhetskrav i enlighet med regelverket för Svensk e-legitimation.

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 skall 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 måste därför alltid väljas i enlighet med gällande policyer nedan.

2.2.1 Standardalgoritmer för underskrift

Bakgrund:

Då en e-tjänst inte specificerar val av algoritm så skall 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 skall kunna hantera sign requests som signerats med samtliga algoritmer ovan. Signeringsalgoritm för sign response skall alltid vara samma som användes för att signera tillhörande sign request.

2.3 Tillitsnivå

Samtliga tillitsnivåer som anges i detta avsnitt avser de tillitsnivåer som definieras i tillitsramverket som ingår i regelverket för infrastrukturen för Svensk e-legitimation. E-tjänster kan genom protokoll för begäran av underskrift begära en lägsta tillåten nivå för legitimering av användare i samband med begärd underskrift.

2.3.1 Standard tillitsnivå vid legitimering vid underskrift

Bakgrund:

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

Policy:

Legitimering av användare i samband med underskrift ska ske med lägst tillitsnivå 3 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 en konfigurerad lägsta acceptabla tillitnivå i underskriftstjänsten.

Policy:

Om underskriftscertifikatet utfärdas som ett kvalificerat certifikat så måste användaren legitimerats med lägst tillitsnivå 3.

Om underskriftscertifikatet utfärdas som icke kvalificerat certifikat så får legitimering ske som lägst med tillitsnivå 2 under förutsättning att detta inte strider mot den certifikatpolicy som deklareras i underskriftscertifikatets certifikatpolicy extension.

2.4 Certifikatpolicy

Underskriftscertifikat innefattar en extension (Certificate policies extension) som skall 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 Godkända avvikelser för kvalificerade certifikat

Bakgrund:

Grundkravet på certifikatpolicy för kvalificerade certifikat är att dessa skall uppfylla kraven från standarden ETSI TS 101 456 (http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=26294)

Policy:

Inga avvikelser från kraven ETSI TS 101 456 är godkända.

2.4.2 Godkända avvikelser för icke kvalificerade certifikat

Bakgrund:

Grundkravet på certifikatpolicy för icke kvalificerade certifikat är att dessa skall uppfylla kraven från standarden TS 102 042 från ETSI (http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=41327) enligt profilen NCP (Normalized Certificate Policy).

Policy:

Inga avvikelser från kraven i TS 102 042 (NCP) är godkända.

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 tidsfönser (giltighetstid) inom vilket underskriftsbegäran skall anses vara giltig enligt begärande e-tjänst. Underskriftstjänsten skall 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 skall 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.