Ändringshantering

Underskriftstjänst

Svensk e-legitimation

INNEHÅLL

1 INLEDNING

Den normativa specifikationen för underskriftstjänsten för Svensk e-legitimation har uppdaterats samt harmoniserats med tekniskt ramverk. Följande viktiga ändringar har gjorts i specifikationen

- Den stora ändringen är att underskriftstjänsten har anpassats för att kunna hantera underskriftsmeddelande (sign message), vilket också är den stora ändringen i tekniskt ramverk.
- Krav på kryptering har anpassats till senaste rekommendation från MSB.
- Direkta knytningar till ramavtal har tagits bort för att specifikationen ska kunna står för sig själv och för att kunna användas inom ramen för olika ramavtal.

Vidare har vissa mindre tekniska ändringar och uppdateringar gjorts samma vissa språkförändringar.

Alla dokumenten i den normativa specifikationen är uppdaterade till version 1.20.

Ändringar i dokumenten är nedan markerade med gult. Tillagd text är understruken och borttagen text är överstruken. Språkliga ändringar är inte markerade.

2 POLICY FÖR UNDERSKRIFTSTJÄNST

Endast språkliga ändringar har gjorts.

3 NORMATIV SPECIFIKATION

Avsnitt 3.1.2 stycke 3
Testtjänsten skall i kundens namn kunna vara ansluten till den testfederation som tillhandahålls genom E legitimationsnämndens försorg.

Avsnitt 3.2 stycke 1
Underskrift som uppfyller kraven på kvalificerade elektroniska signaturer enligt lag (2000:832) om kvalificerade elektroniska signaturer är en option att tillhandahålla. ~~E-legitimationsnämnden är dock angelägen att denna tjänst ska finna tillgänglig för offentlig sektor.~~ Om tjänsten tillhandahålls skall den vid behov kunna beställas som tilläggstjänst till bastjänsten. Tjänst för underskrift

Avsnitt 4 stycke 3
~~Vid avrop skall definitionen~~ Tjänsten skall stödja tillämpning av bråd tid ~~kunna tillämpas~~.
Under bråd tid skall tjänsterna vara förbereda och bemanning vara på plats så att tjänsterna i princip kan upprätthållas utan avbrott.

Avsnitt 5 stycke 3
Erfarenhetsutbyte avseende elektroniska underskrifter och relaterade tjänster inom Svensk e-legitimation samt diskussioner om behov av ändringar av Underskrifts-tjänsten sker inom

ramen för ~~det förvaltningsforum för Underskriftstjänsten~~ den förvaltning av federationen för Svensk e-legitimation som E legitimationsnämnden är ~~sammankallande för~~ ansvarig för. ~~Vid behov kan dessa frågor också behandlas inom ramen för den samverkan som specificeras inom ramavtalet.~~

Avsnitt 6
Förutom de definitioner som framgår av regelverket för Svensk e-legitimation ~~ramavtalet~~ samt av de olika dokumenten som hör till denna normativa specifikation gäller följande definitioner för Underskriftstjänsten.

Ord	Förklaring
Aktör	Organisation som tillhandahåller eller använder tjänst i identitetsfederationen.
~~Attributsintyg~~	~~Intyg i elektronisk form med uppgifter om användares juridiska behörighet, organisatoriska roll eller andra egenskaper.~~
Bråd tid	Tidperiod med hög och tidskritisk belastning där aktör behöver extra stöd för att säkerställa kapacitet och tillgänglighet inom identitetsfederationen.
~~eID-tjänst~~	~~Ett antal sammanhållna aktiviteter för legitimering vid elektronisk kommunikation som börjar i utfärdande av e-legitimation och slutar i leverans av identitetsintyg.~~
~~E-legitimation~~	~~Identitetshandling i elektronisk form, som vid elektronisk kommunikation används för legitimering, underskrift eller bådadera.~~
~~Federationsoperatör~~	~~Den aktör som har det övergripande ansvaret för identitetsfederationen.~~
~~Federationstjänste-leverantör~~	~~Den aktör som på federationsoperatörens uppdrag hanterar och levererar federationstjänsterna.~~
~~Federationstjänster~~	~~De centrala tjänsterna inom federationen för hantering av metadata och för att stödja användaren att välja legitimation (anvisning) och därtill hörande tjänster.~~
~~Identitetsfederation~~	~~Samverkan mellan aktörer för elektronisk legitimering.~~
~~Identitetsintyg~~	~~Intyg i elektronisk form med uppgifter om en användares identitet.~~
~~Legitimeringstjänst~~	~~Tjänst som inom identitetsfederationen tillhandahåller identitetsintyg.~~
~~Svensk e-legitimation~~	~~1) Övergripande benämning på den infrastruktur för identitetsfederation som beskrivs av E-legitimationsnämnden. 2) De certifikat, säkerhetsdosor eller andra hjälpmedel för legitimering som tillhandahålls av en utfärdare av e-legitimation och som uppfyller de krav som E-legitimationsnämnden har ställt upp i avtal med utfärdaren.~~

4 ICKE FUNKTIONELLA KRAV

Avsnitt 2 stycke 1
Varje enskilt avrop/leverans ställer krav på underskriftstjänsten avseende tillgänglighet och kapacitet. Tjänsten skall kunna skala för att tillgodose de behov ~~avropen~~ som kunden ställer krav på.

Avsnitt 2.1 stycke 1
Följande krav på svarstider skall gälla för Underskriftstjänsten såvida inte annat framgår av enskilt/avrop/leverans.

Avsnitt 4.2.1 avsnitt 13
Extern kommunikation mot tjänsten skall ske enligt ~~SSL version 3 eller~~ TLS standarden version 1.1 ~~1.0~~ eller högre. Kommunikation med signeringstjänsten för begäran av underskrift samt retur av underskriftssvar skall endast vara åtkomligt via HTTPS på port 443. Krypteringsalgoritmer skall väljas i enlighet med avsnitt 4.17 i Tjänstespecifikationen för Underskriftstjänsten.

5 TJÄNSTESPEC UNDERSKRIFTSTJÄNST

Avsnitt 2.2 stycke 3 punkt 3
Användaren överförs ~~(redirect)~~ till underskriftstjänstens autentiseringsmodul.

Avsnitt 2.2 stycke 4
Notera att ~~detta~~ denna process illustrerar en exempelimplementering ~~är~~ av ett felfritt typflöde ~~om allt går som tänkt~~. Flödet illustrerar inte eventuella felsituationer där någon av kontrollerna ovan leder till att underskriftsprocessen avbryts. Motsvarande resultat kan uppnås av en systemdesign som på olika sätt avviker från beskrivningen ovan så länge det uppnådda resultatet är detsamma.

Avsnitt 2.4.4 stycke 3
Om begäran om underskrift innehåller underskriftsmeddelande som skall visas för användaren så inkluderas detta i begäran om legitimering till legitimeringstjänsten.

Avsnitt 2.4.4 stycke 4
Identitetsintyg (SAML ~~Identity Assurance~~Assertion) som returneras från legitimeringstjänsten äkthetskontrolleras vid mottagandet av autentiseringsmodulen. Underskriftstjänsten kontrollerar sedan att identitetsintyget representerar rätt användare och innehåller nödvändiga uppgifter som krävs för att skapa en underskrift.

Avsnitt 2.4.4 stycke 5 och 6
Vid begäran om legitimering specificeras krav på legitimeringsprocessen (legitimeringskontext) genom en URI identifierare (AuthnContextClassRef) som definierar krav på legitimeringsprocessen i enlighet med [Eid2-Identifiers]. Legitimeringskontext specificerar som minst en tillitsnivå men kan även specificera krav på visning av underskriftsmeddelande i legitimeringsprocessen.

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 4.7 stycke 1
Användare skall överföras till 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].

Avsnitt 4.7
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>) så skall underskriftstjänsten kontrollera i metadata om legitimeringstjänsten som avses användas för legitimering stödjer visning av underskriftsmeddelande samt begärd tillitsnivå. Om legitimeringstjänsten stödjer detta så skall legitimering alltid begäras med en AuthnContextClassRef URI för begärd tillitsnivå som innefattar krav på visning av underskriftsmeddelandet i enlighet med [Eid2-Identifiers].

Om legitimeringstjänsten inte stödjer visning av underskriftsmeddelande och underskriftsmeddelandet har attributet MustShow satt till true, så skall ingen legitimering begäras. Istället så skall underskriften returnera användaren med ett felmeddelande till e-tjänsten som begärt underskrift.

Legitimeringsbegäran 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.

Avsnitt 4.8 stycke 2
Legitimering av användare accepteras endast om samtliga användarattribut och dess värden som specificerats i sign requesten återfinns i mottaget identitetsintyg samt att identitetsintyget är utfärdat för den tillitsnivå och legitimeringsprocess som specificerats i begäran om legitimering som AuthnContextClassRef URI.

Avsnitt 4.8 stycke 2
Val av algoritmer och nyckellängder för autentisering, kryptering och signering skall följa NIST SP 800-131 [SP800-131] samt ETSI TS ~~102~~ 119 ~~176~~-1312 version 1.1.1 ~~2.11~~ [ETSI-Algo].

Avsnitt 7.1 tabell

[Eid2-DSS]
~~Eid2~~ DSS Extension for ~~SAML based~~Federated Central Signing Services.

[Eid2-Identifiers]
Registry for identifiers assigned by the Swedish e- identification board

[ETSI Algo]
Electronic Signatures and Infrastructures (ESI);
Cryptographic Suites~~Electronic Signatures and Infrastructures (ESI);~~
~~Algorithms and Parameters for Secure Electronic Signatures;~~
~~Part 1: Hash functions and asymmetric algorithms.~~
(http://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.01.01_60/ts_119312v010101p.pdf ~~http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=31439)~~