E-legitimationsnämnden
Nils Fjelkegård
171 94 SOLNA

Stockholm 2012-09-03

.SE:s svar på E-legitimationsnämndens remiss av utkast till regelverk

.SE har tagit del av E-legitimationsnämndens remiss daterad 2012-07-06 i vilken nämnden efterfrågar **synpunkter på Regelverket och Tillitsramverket** som ett led i det fortsatta arbetet med framtagandet av basstrukturen. .SE har i huvudsak begränsat svaret till dessa båda delar, men vi tar oss också friheten att presentera några korta kommentarer och önskemål kring det fortsatta arbetet.

I remissen anges att en viktig utgångspunkt för E-legitimationsnämndens arbete har varit att den infrastruktur som byggs upp ska kunna nyttjas av såväl offentlig som privat sektor för att säkerställa att utvecklingen av elektronisk legitimering och underskrift inte går skilda vägar och att en Svensk e-legitimation ska kunna användas överallt. Det uppges att det därför har skapats en för offentlig och privat sektor gemensam basstruktur där de centrala komponenterna består av Regelverk, Tillitsramverk och Tekniskt ramverk.

.SE ställer sig positiv till nämndens arbete och de förslag som redovisas. .SE anser också att införandet av en sammanhållen och enhetlig infrastruktur för identifiering och signering inom såväl offentlig som privat sektor främjar utvecklingen på området. De förslag till Regelverk och Tillitsramverk som nu är föremål för remiss är väl genomarbetade.

.SE:s bedömning är dock att basstrukturen kan kräva vissa anpassningar för att användas för identitetsfederationer inom den privata sektorn, men att nuvarande dokument tjänar som en god utgångspunkt för sådana anpassningar.

.SE har uppfattat det som att utfärdarna av Svensk e-legitimation vid anslutning till basinfrastrukturen tar ansvar för hela kedjan, inklusive intygsgivningsfunktion, och att samtliga delar är föremål för kontroll och uppföljning gentemot Tillitsramverket, vilket .SE anser vara positivt då detta utgör grunden för bildandet av flera federationslösningar. Inte minst av den anledningen bör Regelverket endast innehålla de nödvändiga ramar som krävs för en fungerande federation.

Stiftelsen för Internetinfrastruktur
Box 7399, 103 91 Stockholm Tel 08-452 35 00 Fax 08-452 35 02 Org.nr. 802405-0190 www.iis.se

Synpunkter på Övergripande beskrivning av avtalsarkitektur med mera.

.SE tycker det är positivt att samtliga relationer mellan parterna regleras i skriftliga avtal. I dessa avtal kan vid behov särskilda klausuler formuleras om krav på hantering och skydd av personuppgifter och krav på systematiskt arbete med informationssäkerhet.

.SE anser att uppdelningen i modellen mellan Leverantör av eID-tjänst och Utfärdare av Svensk e-legitimation är bra, men inte helt intuitiv.

.SE har inte fullt klart för sig vilka krav som en leverantör av eID-tjänst respektive Tillhandahållare av e-tjänst behöver uppfylla för att godkännas och tillåtas teckna Anslutningsavtal, vilket kan påverka kostnadsbilden för granskning inom privata federationer. (Anslutningsavtal 4.2.1).

Vi har tolkat modellen som att Utfärdaren ansvarar för hela kedjan gentemot E-legitimationsnämnden i dess roll som ansvarig för infrastrukturen och att det är nämnden som gör kontroll och uppföljning av att leverantören uppfyller kraven i Tillitsramverket.

.SE anser också att det är bra att – som vi har förstått det - leverantören av eID-tjänst ansvarar för hela kedjan gentemot förlitande part i federationen, även om man anlitar annan utfärdare av e-legitimationer. Gentemot federationen blir då "Leverantör av eID-tjänst" ansvarig, då detta är den enda avtalsparten. Om det är en annan part än denne som faktiskt utfärdat e-legitimationen, så får ansvarsfrågan regleras dem sinsemellan.

Det viktiga enligt .SE:s uppfattning är att Tillhandahållare av e-tjänst bara har en part att utkräva ansvar av om något skulle gå fel.

Vi föreslår att modellen förtydligas genom några goda exempel eller typfall. Det vore även önskvärt med en steg för steg-beskrivning av hur det går till att ansöka, kontrolleras och bli godkänd för de olika parterna i federationen. En sådan beskrivning skulle sannolikt underlätta förståelsen för modellen.

Utfärdare av attributsintyg

.SE anser det önskvärt att ambitionen för Utfärdare av attributsintyg tydliggörs. Utfärdare av attributsintyg omnämns i dokumentet ”Övergripande beskrivning av avtalsarkitektur”, men vi uppfattar det som att dess roll i federationen är oklar. Till exempel saknas anslutningsavtal, regelverk och inte heller är denna med i figuren på sid 2.

Som exempel på Utfärdare av attributsintyg har attributet ”firmatecknare” nämnts. .SE anser att attribut utfärdade för en tidigare identifierad individ är ett stort och intressant område som kan generaliseras och tillämpas inom flera samhällssektorer så som till exempel för sektorerna skola och eHälsa.

.SE:s uppfattning är att Utfärdare av attributsintyg modellmässigt bör ses som en överliggande tjänst till identifieringstjänsten Svensk e-legitimation. (Det vill säga en attributtjänst kan använda sig av olika identifieringstjänster, som till exempel Svensk e-

legitimation, ACME:s e-legitimation eller en vanlig lösenordsinloggning. Vilka identifieringstjänster som tillåts kombineras med attributtjänsten styrs av e-tjänstetillhandahållarens säkerhetskrav).

Om ”Utfärdare av attributsintyg” hanteras som en överliggande tjänst och inte som en del av "identitetsfederation för Svensk e-legitimation" ökar potentialen för hela konceptet samtidigt som det förenklar arbetet med Svensk e-legitimation. Modellmässigt bör därför inte ”Utfärdare av attributsintyg” jämställas med en ”Leverantör av eID-tjänst”, utan snarare med en ”Tillhandahållare av e-tjänster”. Attributtjänsten ska ses som en påbyggnad till Svensk e-legitimation med sitt separata regelverk och avtal för sina aktuella utfärdare och användare av attributsintyg. Det är .SE:s uppfattning att E-legitimationsnämndens modell kan och bör vidareutvecklas i denna riktning.

.SE menar att utvecklingen av federativa lösningar för olika nationella samverkansinitiativ, i form av olika "attributsfederationer", skulle kunna underlättas om det även finns en samverkan mellan dem. E-legitimationsnämnden skulle kunna vara en sådan naturlig samordnare, men endast under förutsättning att arbete med Svensk E-legitimation inte försenas.

Ytterligare LoA-nivåer

.SE anser det bra att det föreslagna Tillitsramverket har utvecklats till att även omfatta LoA2 och LoA4. Vi uppfattar det som att detta ska ses som ett första steg för att på sikt fullt ut inkludera LoA2 och LoA4 i E-legitimationsnämndens arbete. Det vore ur .SE:s perspektiv önskvärt att tidplanen för utvecklingen av tillitsnivåerna LoA2 och LoA4 klargörs.

Kännetecknen för identitetsfederationer för Svensk e-legitimation

I texten omnämns "identitetsfederationer för Svensk e-legitimation", men inga uttryckliga krav ställs för att en federation för den privata sektorn ska vara en "identitetsfederation för Svensk e-legitimation". .SE anser att E-legitimationsnämnden bör överväga möjligheten att erbjuda ett särskilt kännetecken för "identitetsfederation för Svensk e-legitimation" för den privata sektorn som får användas av de federationsoperatörer som lever upp till kraven. Ett sådant kännetecken kan tjäna som incitament för aktörerna på området.

Synpunkter på Anslutningsavtal för Utfärdare av Svenska e-legitimation

.SE har följande detaljsynpunkter:

Bilagorna är felnumrerade.

p.2.1, stryk ordet ”slags”.

p. 2.2, tydliggör så att det framgår att anslutningsavtalet ger rätt att nyttja Kännetecknen.

3.3, tydliggör första meningen.

p. 4.2 första meningen, byt ut ”och” mot ”eller”.

P 11, är skrivningen tillräckligt omfattande för att vid behov omgående kunna stänga av någon vid ett enskilt tillfälle? Enligt vems uppfattning har utfärdaren agerat på ett sätt som skadar eller riskerar att skada förtroendet för infrastrukturen för svensk e-legitimation?

Synpunkter på Tillitsramverk för Svensk e-legitimation.

Organisation och styrning – Informationssäkerhet

.SE har följande detaljsynpunkter:

Vi föreslår att K.2.4 kompletteras med ytterligare en punkt (f) för att poängtera vikten av systematiskt säkerhetsarbete: Utfärdare av svensk e-legitimation ska regelbundet genomföra förbättringar av sitt arbete med informationssäkerhet samt genomföra lämpliga korrigerande och förebyggande åtgärder.

Handlingars bevarande

K2.8 – .SE anser att det behövs en särskild skrivning om krav på lagring (kryptering) och säkerhetskopiering.

Ansökan, identifiering och registrering

.SE anser att det i K5.3 behövs ytterligare en punkt om gallring i utfärdardeklarationen, eventuellt kan det inkluderas i formuleringen av (g).

Synpunkter på Regelverk för identitetsfederationer för svensk e-legitimation

.SE har följande detaljsynpunkter:

Bilaga C Servicenivåer – .SE noterar att bilagan inte omfattar tillhandahållare av e-tjänster. Är detta ett medvetet val? Skulle det tjäna modellens syfte att ställa någon form av krav på servicenivåer även på ingående tjänster?

.SE anser att Anvisningstjänsten skulle kunna definieras som en tilläggstjänst, och att krav/beskrivning av denna flyttas till Bilaga E. På så sätt kan regelverket förmodligen användas "rakt av" även om en part inte har något önskemål om att tillhandahålla en anvisningstjänst.

Avslutande kommentarer

.SE ställer sig positiv till det arbete som gjorts av E-legitimationsnämnden. .SE arbetar för närvarande tillsammans med andra parter med att etablera en Skolfederation och har på sikt ambitionen att i möjligaste mån använda E-legitimationsnämndens modell och regelverk. Vi bidrar gärna med våra erfarenheter i det fortsatta arbetet och ser fram emot en fortsatt dialog.

Danny Aerts,

Vd

Stiftelsen för Internetinfrastruktur
Box 7399, 103 91 Stockholm Tel 08-452 35 00 Fax 08-452 35 02 Org.nr. 802405-0190 www.iis.se