Regelverk för Infrastrukturen för Svensk e-legitimation

1 **Bakgrund** **186**

2 **Definitioner** **187**

3 **Det samordnade området** **188**

4 **Regelverkets delar** **193**

5 **Anslutning** **195**

6 **Utfärdande, m.m.** **198**

7 **Regler för användare, m.m.** **205**

8 **Regler för e-tjänsteleverantörer** **207**

9 **Persondataskydd** **209**

10 **Bevarande, säkerhet och tillsyn** **210**

1. Bakgrund

1.1 Av lagen (2011:000) om valfrihet för Svensk e-legitimation följer att E-legitimationsnämnden får tillhandahålla ett valfrihetssystem för en *Infrastruktur för Svensk e-legitimation*. Användare av e-legitimationer ska kunna välja leverantör bland dem som anslutits till denna infrastruktur.

1.2 E-legitimationsnämnden ska enligt förordningen (2010:1497) med instruktion för nämnden stödja och samordna elektronisk identifiering och signering i den offentliga förvaltningens e-tjänster samt utveckla specifikationer och liknande krav som ska vara gemensamma för myndigheter under regeringen i deras användning av e-legitimationer.

1.3 Detta regelverk tillämpas inom *Infrastrukturen för Svensk e-legitimation*. Till denna infrastruktur hör att

a) utfärda, använda, verifiera och spärra *Svensk e-legitimation*,

b) tillhandahålla en *Infrastruktur för identifiering* där

i. e-tjänsteleverantörer kan erhålla *identitets- och attributsintyg* för att granska om uppgifter som lämnats om identitet eller juridisk behörighet eller andra attribut är riktiga,

ii. *centrala register* över aktörer förmedlar uppgifter om aktörernas tjänster och funktioner för tillit och säkert informationsutbyte,

iii. en *anvisningstjänst* kan ge användaren av en e-tjänst hjälp att välja e-legitimation att bruka i e-tjänsten,

c) tillhandahålla en *signeringstjänst* som gör det möjligt för användaren att skriva under elektroniska handlingar.

1.4 Dessa regler har till syfte att etablera funktioner för e-legitimationer, elektroniska underskrifter och identitets- och attributsintyg som är enkla att förstå och använda och som på ett balanserat sätt kan tillgodose skyddet för

rättssäkerheten, informationssäkerheten och enskildas personliga integritet.

1.5 De tekniska och administrativa lösningarna ska utformas så att så få personuppgifter som möjligt samlas in, lämnas ut eller annars behandlas och att inte fler uppgifter än nödvändigt samlas in och bevaras så att de blir direkt tillgängliga.

1.6 Den som tillhandahåller tjänster för identifiering inom Infrastrukturen för Svensk e-legitimation ska få tillhandahålla motsvarande tjänster åt företag och andra organisationer inom ramen för en anknytande infrastruktur för näringslivet. Detta regelverk har utformats i syfte att underlätta införandet av en sådan parallell infrastruktur.

2. Definitioner

I detta regelverk används följande beteckningar i nedan angiven betydelse.

1. *Svensk e-legitimation*; de certifikat, säkerhetsdosor eller andra hjälpmedel för identifiering som har anslutits till Infrastrukturen för Svensk e-legitimation,
2. *Infrastrukturen för Svensk e-legitimation*; den Infrastruktur för elektronisk legitimering och elektronisk underskrift som E-legitimationsnämnden inrättat för samverkan mellan identitetsutfärdare, e-tjänsteleverantörer och användare av Svensk e-legitimation,
3. *Infrastrukturen för identifiering*; en del av Infrastrukturen för Svensk e-legitimation där e-tjänsteleverantörer kan erhålla identitets- och attributsintyg för att granska om uppgifter som lämnats om identitet eller juridisk behörighet eller andra attribut är riktiga,
4. *Identitetsutfärdare*; den som utfärdar identitetsintyg inom Infrastrukturen för identifiering,

5. *Attributsutfärdare*; den som utfärdar attributsintyg inom Infrastrukturen för identifiering eller en annan anknytande infrastruktur,
6. *E-tjänsteleverantör*; den som tillhandahåller en e-tjänst som stöds av Svensk e-legitimation,
7. *Användare*; den som har en privat e-legitimation eller en e-tjänstelegitimation som godtas som Svensk e-legitimation,
8. *Identitetsintyg*; ett av en identitetsutfärdare utställt intyg i elektronisk form med uppgifter om en användares identitet och attribut,
9. *Attributsintyg*; ett av en attributsutfärdare utställt intyg i elektronisk form med uppgifter om användares juridiska behörighet, organisatoriska roll eller andra egenskaper,
10. *Centralt utfärdarregister*; ett register som E-legitimationsnämnden för över identitets- och attributsutfärdare som är anslutna till Infrastrukturen för identifiering,
11. *Centralt e-tjänsteregister*; ett register som E-legitimationsnämnden för över e-tjänsteleverantörer som är anslutna till Infrastrukturen för identifiering,
12. *Tillitsnivå*; den skyddsklass till vilken en e-legitimation hänförs,
13. *Signaturtjänsten*; det tekniska och administrativa stöd som E-legitimationsnämnden lämnar åt en e-tjänsteleverantör för att användare ska kunna skriva under handlingar elektroniskt, och
14. *Anvisningstjänsten*; det tekniska och administrativa stöd som E-legitimationsnämnden lämnar åt en e-tjänsteleverantör för att användare ska kunna välja e-legitimation.

3. Det samordnade området

Aktörer och uppgifter

1.7 *E-legitimationsnämnden* ska utveckla och svara för Infrastrukturen för Svensk e-legitimation. Till nämndens uppgifter hör att

a) *utarbeta underlag* för föreskrifter beträffande Infrastrukturen för Svensk e-legitimation, avtal och allmänna

villkor i de delar Infrastrukturen för Svensk e-legitimation regleras genom civilrättsliga överenskommelser samt riktlinjer, vägledningar, dokumentation och tekniska krav för Infrastrukturen för Svensk e-legitimation,

b) *meddela föreskrifter* inom ramen för den normgivningskompetens som delegeras till nämnden,

c) *upphandla leverantörer* av tekniska tjänster för Infrastrukturen för Svensk e-legitimation,

d) *sluta avtal* med aktörer inom Infrastrukturen för Svensk e-legitimation,

e) *inrätta en Infrastruktur för identifiering* inom ramen för Infrastrukturen för Svensk e-legitimation, och för denna infrastruktur

i. inrätta ett valfrihetssystem för Infrastrukturen för identifiering, och

ii. besluta och avtala om anslutning till Infrastrukturen för identifiering.

1.8 *Identitetsutfärdare* som ansluts till Infrastrukturen för identifiering ska tillhandahålla identitetsintyg åt e-tjänsteleverantörer. Den som lämnar identitetsintyg inom Infrastrukturen för identifiering ska ha ställt ut de e-legitimationer som brukas eller – såvitt är av betydelse för ett lämnat intyg – svara för e-legitimationen och anknytande funktioner som om Identitetsutfärdaren själv hade ställt ut e-legitimationen och tillhandahållit anknytande funktioner.

1.9 *Attributsutfärdare* som anslutits till Infrastrukturen för identifiering ska tillhandahålla uppgifter åt e-tjänsteleverantörer om juridisk behörighet, roll, personnummer eller annat av betydelse för en e-tjänsteleverantör som ska kontrollera uppgifter om användare.

1.10 *Användare* brukar privat e-legitimation eller e-tjänstelegitimation i e-tjänster. Användaren väljer en identitetsutfärdare som nämnden anslutit till Infrastrukturen för identifiering. E-legitimationsnämnden informerar på sin webbplats om vilka identitetsutfärdare som har anslutits.

1.11 *E-tjänsteleverantörer*, anslutna till Infrastrukturen för identifiering, tillhandahåller e-tjänster där det krävs elektronisk legitimering eller elektronisk underskrift.

Register

1.12 E-legitimationsnämnden ska föra register över

a) de identitetsutfärdare och attributsutfärdare som är anslutna till Infrastrukturen för identifiering (*utfärdarregister*), och

b) de e-tjänsteleverantörer som är anslutna till Infrastrukturen för identifiering (*e-tjänsteregister*).

1.13 I dessa register ska finnas uppgifter om

a) elektroniska adresser till anslutna identitets- och attributsutfärdare och e-tjänsteleverantörer,

b) vilka uppgifter en e-tjänsteleverantör behöver för en viss e-tjänst,

c) vilka identitetsuppgifter och attribut som en identitets- eller en attributsutfärdare kan tillhandahålla, och

d) de certifikat och nycklar som en utfärdare av identitets- eller attributsintyg använder för att stämpla intygen och som e-tjänsteleverantörer använder för att kontrollera om mottagna intyg är äkta.

1.14 Uppgifter i utfärdarregistret ska få användas även inom anknytande infrastrukturer för motsvarande tjänster åt företag och andra organisationer, som registreras i e-tjänsteregister som inte är en del av Infrastrukturen för identifiering.

1.15 Utfärdar- och e-tjänsteregistren får inte innehålla personuppgifter såsom information om kommunikation mellan användare och e-tjänsteleverantörer, innehållet i identitets- eller attributintyg eller handlingar som ska skrivas under eller har undertecknats elektroniskt.

1.16 I förordningen (2010:000) om Infrastrukturen för Svensk e-legitimation finns föreskrifter om registrering i utfärdar- och e-tjänsteregistren.

Anvisningstjänst

1.17 E-legitimationsnämnden ska tillhandahålla en tjänst som tillför stöd, dels åt användare när de ska välja e-legitimation i en e-tjänst, dels åt den som tillhandahåller e-tjänsten beträffande vilken utfärdare av e-legitimationer som användaren valt (anvisningstjänst).
E-legitimationsnämnden ska svara gentemot användaren för dessa funktioner.

Signeringstjänst

1.18 E-legitimationsnämnden tillhandahåller inom ramen för Infrastrukturen för Svensk e-legitimation en tjänst som ger stöd för elektronisk underskrift av handlingar (signaturtjänst).

E-legitimationsnämnden ska svara gentemot användaren för signaturtjänsten.

Underleverantörer

1.19 E-legitimationsnämnden får överlämna den tekniska driften och skötseln av register och tjänster till underleverantörer men ska svara för verksamheten som om nämnden hade utfört åtgärderna själv.

E-legitimationer, m.m.

1.20 *E-legitimationer* såsom certifikat, säkerhetsdosor och liknande som ansluts till Infrastrukturen för Svensk e-legitimation utfärdas för användare som *privat e-legitimation* eller – i egenskap av anställd eller uppdragstagare – *som e-tjänstelegitimation*.

1.21 *Användare anskaffar* privat e-legitimation från identitetsutfärdare som är anslutna till Infrastrukturen för Svensk e-legitimation.

1.22 *Myndigheter* och andra organisationer *anskaffar e-tjänstelegitimationer* för sina arbets- och uppdragstagare från identitetsutfärdare som är anslutna till Svensk e-legitimation.

1.23 Svensk e-legitimation och tillhörande identitetsintyg ska utfärdas i enlighet med kraven för tillitsnivå 3 eller högre i tillitsramverket [baserat på Kantara IAF, blivande ISO 29115], *bilaga 9*.

1.24 E-tjänsteleverantören bestämmer vilken tillitsnivå för identifiering, vilket slag av elektronisk underskrift och vilka attribut som ska krävas av användare och dem som användare företräder.

Användning av e-legitimationer m.m.

1.25 En Svensk e-legitimation används vanligtvis på följande sätt mellan enskilda och e-tjänsteleverantörer.

a) *Privat e-legitimation* används av fysiska personer när de kommunicerar för egen räkning.

b) *E-tjänstelegitimation* används av fysiska personer när de kommunicerar i egenskap av anställda eller uppdragstagare.

En användare kan emellertid bruka en privat e-legitimation även i egenskap av företrädare för annan och den som har tilldelats en e-tjänstelegitimation får, om arbets- eller uppdragsgivaren godtar det, bruka e-tjänstelegitimationen också för egen räkning.

1.26 *En användare* som tilldelats en privat e-legitimation eller en e-tjänstelegitimation brukar den för

1) *legitimering* vid

a) *tillträde*, för att elektroniskt få tillgång till uppgifter som får lämnas ut till honom eller henne och för att få skydd

mot att obehöriga får tillgång till uppgifterna under sken av att vara honom eller henne,

b) *uppgiftslämnande*, för att få lämna uppgifter elektroniskt och för att få skydd mot att obehöriga lämnar uppgifter under sken av att vara honom eller henne,

2) *elektronisk underskrift*, för att ställa ut elektroniska handlingar som är skyddade mot förfalskning och förnekande av elektronisk underskrift på liknande sätt som en handling som är undertecknad på traditionellt sätt.

1.27 Genom en *anvisningstjänst* stöds funktioner för att användare ska kunna välja en e-legitimation som har en säkerhetsnivå eller andra egenskaper som är förenliga med de krav som gäller för e-tjänsten.

1.28 En myndighet använder identitetsintyg för att kontrollera

1) *legitimering*,

a) vid *tillträde*, för att kunna ge tillgång till uppgifter elektroniskt så att inte obehöriga får ut uppgifterna,

b) vid *uppgiftslämnande*, för att kontrollera vem som är ansluten när vissa uppgifter lämnas, och

2) *elektronisk underskrift*, för att granska om en handling som har undertecknats elektroniskt är utställd av den som anges som undertecknare.

1.29 En myndighet använder ett attributsintyg för att kontrollera om en person har juridisk behörighet att agera för annans räkning, viss befattning eller annan roll eller egenskap eller på annat sätt är förknippad med något som en attributsutfärdare kan intyga.

4. Regelverkets delar

1.30 Infrastrukturen för Svensk e-legitimation regleras genom detta regelverk, när föreskrifter inte ges i lag eller författning, och i följande avtal.

Avtal efter upphandling av teknisk drift

1.31 E-legitimationsnämnden tecknar *leveransavtal* med den som enligt upphandling rörande Infrastrukturen för Svensk e-legitimation ska sköta teknisk drift av

a) utfärdarregister och e-tjänsteregister,

b) anvisningstjänst, och

c) signeringstjänst.

Avtal efter upphandling av valfrihetssystem

1.32 E-legitimationsnämnden tecknar efter upphandling av valfrihetssystem för Infrastrukturen för Svensk e-legitimation avtal med de

a) identitetsutfärdare som uppfyller de krav som ställs upp inom valfrihetssystemet, och

b) myndigheter som ansluter sig som e-tjänsteleverantörer och uppfyller föreskrivna krav.

c) Dessa avtal ska innehålla de ramar som anges i *bilaga 4 och 5*.

Avtal om e-legitimationer för fysiska personer

1.33 En fysisk person som ansöker om en e-legitimation för att identifiera sig eller skriva under elektroniskt ska sluta avtal med utfärdaren av e-legitimationen.

1.34 Juridiska personer som ansöker om e-tjänstelegitimationer för anställda eller uppdragstagare ska sluta avtal med en utfärdare som är ansluten till Svensk e-legitimation.

5. Anslutning

Anslutning av identitetsutfärdare till Infrastrukturen för identifiering

1.35 Anslutning av identitetsutfärdare till Infrastrukturen för identifiering sker efter *ansökan* hos E-legitimationsnämnden genom att nämnden *tecknar avtal* med utfärdaren.

1.36 Den som uppfyller kraven i ett förfrågningsunderlag enligt lagen (2011:000) om valfrihet för Svensk e-legitimation och godtar de juridiska, tekniska och administrativa villkoren ska ha rätt att bli ansluten till Infrastrukturen för identifiering.

Anslutning av attributsutfärdare till Infrastrukturen för identifiering

1.37 Anslutning av attributsutfärdare till Infrastrukturen för identifiering sker genom

a) *beslut* av E-legitimationsnämnden, efter ansökan av *en myndighet under regeringen*, och

b) *avtal*, efter ansökan av *annan* än myndighet under regeringen.

1.38 En attributsutfärdare får anslutas till Infrastrukturen för identifiering om utfärdaren

a) enligt lag eller författning ska registrera och tillhandahålla de uppgifter som avses lämnas i attributsintygen och uppgifterna är av generell betydelse från kontrollsynpunkt, eller

b) det finns särskilda skäl från kontrollsynpunkt att ett visst slag av attribut från en viss utfärdare ska kunna lämnas inom Infrastrukturen för identifiering.

1.39 Särskilda skäl från kontrollsynpunkt föreligger om det finns ett utbrett behov inom offentlig förvaltning av tillförlitlig åtkomst till uppgiften och den inte finns tillgänglig på fungerande sätt i annan ordning.

1.40 E-legitimationsnämnden får i ett beslut om anslutning som villkor föreskriva att attributsutfärdaren ska följa de juridiska, tekniska och administrativa villkor som nämnden bestämmer.

1.41 E-legitimationsnämnden får ingå avtal om anslutning av en attributsutfärdare endast om utfärdaren accepterar de juridiska, tekniska och administrativa villkoren för anslutning till Infrastrukturen för identifiering.

Anslutning av e-tjänsteleverantörer till Infrastrukturen för identifiering

1.42 Anslutning av e-tjänsteleverantörer till Infrastrukturen för identifiering sker genom

a) beslut av E-legitimationsnämnden, efter ansökan av *en myndighet under regeringen*, och

b) avtal, efter ansökan av *annan* än myndighet under regeringen.

1.43 E-legitimationsnämnden får i ett beslut om anslutning som villkor föreskriva att e-tjänsteleverantören ska följa de juridiska, tekniska och administrativa villkor som nämnden bestämmer.

1.44 E-legitimationsnämnden får ingå avtal om anslutning av en e-tjänsteleverantör endast om utfärdaren accepterar de juridiska, tekniska och administrativa villkoren för anslutning till Infrastrukturen för identifiering.

E-legitimationsnämnden agerar som mellanman vid anslutning till Infrastrukturen för identifiering

1.45 Vid anslutning genom avtal till Infrastrukturen för identifiering beslutar E-legitimationsnämnden om tilldelning av ramavtal och tecknar upphandlingskontrakt för e-tjänsteleverantörernas räkning så att ett kontraktsförhållande uppkommer mellan e-tjänsteleverantören och

varje identitetsutfärdare och attributsutfärdare som genom avtal ansluts till Infrastrukturen för identifiering; jfr 3 § lagen (2011:000) om valfrihet för Svensk e-legitimation.

1.46 Vid anslutning genom beslut av E-legitimationsnämnden gäller de villkor som följer av E-legitimationsnämndens beslut.

Anslutning av e-tjänsteleverantörer till signaturtjänsten

1.47 Anslutning av e-tjänsteleverantörer till signaturtjänsten sker genom

a) beslut av E-legitimationsnämnden, efter ansökan av *en myndighet under regeringen*, och

b) avtal, efter ansökan av *annan* än myndighet under regeringen.

1.48 E-legitimationsnämnden får i ett beslut om anslutning som villkor föreskriva att e-tjänsteleverantören ska följa de juridiska, tekniska och administrativa villkor som nämnden bestämmer.

1.49 E-legitimationsnämnden får ingå avtal om anslutning av en e-tjänsteleverantör endast om utfärdaren accepterar de juridiska, tekniska och administrativa villkoren för anslutning till signaturtjänsten.

Aktivering efter beslut eller avtal om anslutning

1.50 Identitetsutfärdares, attributsutfärdares och e-tjänsteleverantörers anslutningar och funktioner, som samverkar med Infrastrukturen för Svensk e-legitimation, får inte aktiveras förrän de testats och E-legitimationsnämnden funnit att de fungerar på ett tillförlitligt sätt.

6. Utfärdande, m.m.

Tillförlitliga regler och rutiner

1.51 Utfärdare av Svensk e-legitimation, identitetsutfärdare och attributsutfärdare ska tillämpa sådana regler och rutiner att det – utifrån tillämplig tillitsnivå – finns fog för att lita på de e-legitimationer, identitetsintyg och attributsintyg som tillhandahålls. Dessa rutiner regleras från tekniska, administrativa och operativa utgångspunkter i tillitsramverket (bilaga 9).

Svensk e-legitimation

Ansökan, m.m.

1.52 Identitetsutfärdare som är anslutna till Infrastrukturen för Svensk e-legitimation ska utfärda e-legitimation till den som ansöker i enlighet med detta regelverk. [Identitetsutfärdare får dock uppställa särskilda villkor för utfärdande om villkoren är icke-diskriminerande och rör ett berättigat intresse hos identitetsutfärdaren.] Svensk e-legitimation får utfärdas endast efter skriftlig ansökan i traditionell form. Ansökan ska vara undertecknad på traditionellt sätt, med intyg om att lämnade uppgifter är riktiga och fullständiga.

1.53 Om en sökande har legitimerat sig eller skrivit under enligt det förenklade förfarande som anges i 1.60 får en sådan underskrift eller legitimering för uppgiftslämnande ersätta ett förfarande enligt 1.52.

1.54 Vid ansökan om en e-legitimation enligt en lägre tillitsnivå än nivå tre får den sökande identifieras enligt de förenklade förfaranden som anges.

1.55 En ansökan om Svensk e-legitimation ska innehålla de uppgifter som är nödvändiga för att identitetsutfärdaren ska kunna tillhandahålla sådan legitimation och utfärda identitetsintyg.

1.56 Utfärdaren ska i avtal med den som ansöker om Svensk e-

legitimation som villkor föreskriva att användaren ska skydda sin e-legitimation och sin personliga kod enligt 1.93 och när det är tillämpligt välja programvara och utrustning enligt vad som anges i 1.92.

Information om villkor

1.57 Utfärdaren ska informera den som ansöker om Svensk e-legitimation om avtalsvillkorens innehåll. En utfärdare som vill införa villkor som inte finns med i ansökningshandlingen ska tydligt hänvisa till villkoren och utforma rutinerna så att villkoren kommer sökanden tillhanda innan denne undertecknar eller annars ingår avtal med utfärdaren.

1.58 Utfärdaren ska tillhandahålla uppgifter om avtal, villkor, policies, utfärdardeklarationer, regelverk och anknytande uppgifter till anslutna användare, arbets- och uppdragsgivare, e-tjänsteleverantörer och andra som behöver uppgifter i samband med kontroller av legitimeringar eller handlingars äkthet.

Kontroll av sökandens identitet

1.59 Utfärdare av Svensk e-legitimation ska kontrollera den sökandes identitet vid ett personligt besök, på likvärdigt sätt som vid en ansökan om en traditionell identitetshandling.

1.60 Om en sökande redan har identifierats vid ett personligt besök för att få använda bank på Internet eller någon liknande tjänst för ekonomiskt eller rättsligt betydelsefulla mellanhavanden får utfärdaren identifiera den sökande genom denna tjänst i stället för enligt 1.59. En sådan förenklad rutin får dock inte användas om den har spärrats eller om det annars kan antas att den inte fungerar på ett tillförlitligt sätt.

Kontroll av uppgifter och utlämnande av Svensk e-legitimation

1.61 En utfärdare av en e-legitimation ska

1) kontrollera att ansökan om e-legitimation är behörigen undertecknad på papper eller lämnad elektroniskt enligt 1.53 – eller enligt 1.54 om det är förenligt med den aktuella tillitsnivån – och att de uppgifter som den sökande lämnar enligt är fullständiga och stämmer överens med uppgifter som finns registrerade i ett officiellt register, och

2) *tillhandahålla* e-legitimationer på ett säkert sätt.

1.62 Om en utfärdare tillhandahåller en e-legitimation, som användaren ska inneha och en personlig kod som användaren ska bruka för att aktivera legitimationen, ska dessa befordras

1) i separata försändelser och lämnas ut till sökanden vid personligt besök hos utfärdaren eller ett ombud för utfärdaren, eller

2) genom ett elektroniskt förfarande som är förenligt med 6.3 eller 6.4 om detta kan förenas med den tillämpliga tillitsnivån.

Spärrtjänst och spärrkontrolltjänst

1.63 Utfärdare av Svensk e-legitimation ska tillhandahålla en tjänst där användaren kan spärra sin e-legitimation (spärrtjänst). Tjänsten ska ha god tillgänglighet och utfärdaren ska behandla anmälan om spärr skyndsamt.

En myndighet som tillhandahåller en e-tjänst ska också kunna anmäla spärr av en e-legitimation. Identitetsutfärdaren ska spärra e-legitimationen efter en bedömning utifrån angivna skäl [och enligt vissa regler].

Särskilda regler för e-tjänstelegitimationer

1.64 Bestämmelserna om personliga e-legitimationer gäller i tillämpliga delar även för e-tjänstelegitimationer.

1.65 Identitetsutfärdare som är anslutna till Infrastrukturen för Svensk e-legitimation för att utfärda e-tjänstelegitimationer ska utfärda sådan legitimation till den som ansöker i enlighet med detta regelverk. [Identitetsutfärdare får dock uppställa särskilda villkor för utfärdande om villkoren är icke-diskriminerande och rör ett berättigat intresse hos identitetsutfärdaren.]

1.66 En e-tjänstelegitimation får utfärdas endast efter skriftlig ansökan i traditionell form av en arbets- eller uppdragsgivare. Ansökan ska vara undertecknad på traditionellt sätt av arbets- eller uppdragsgivaren. Om denne är en juridisk person ska ansökan vara undertecknad av en behörig företrädare. Utfärdaren ska kontrollera att uppgifterna om behörighet är riktiga.

1.67 Om en arbets- eller uppdragsgivare eller en behörig företrädare för denne har legitimerat sig eller skrivit under enligt förenklade förfarande som anges i 1.60 får en sådan underskrift eller legitimering för uppgiftslämnande ersätta ett förfarande enligt 1.52.

1.68 Den arbets- eller uppdragsgivare som ansöker om en e-tjänstelegitimation

a) bestämmer hur e-tjänstelegitimationen får användas, t.ex. om den får användas även utanför tjänsten, och

b) får spärra e-legitimationen.

1.69 [Närmare regler om uppgiftslämnande vid ansökan och utlämnande, RA-funktion]

1.70 Utfärdaren får lämna ut en e-tjänstelegitimation endast till

a) den som har legitimerat sig med en godkänd legitimationshandling eller på motsvarande sätt [enligt närmare regler på lägre nivå] och visat att han eller hon är behörig att företräda arbets- eller uppdragsgivaren, eller

b) den användare för vilken e-tjänstelegitimationen utfärdats, om arbets- eller uppdragsgivaren skriftligen har godkänt att den lämnas ut direkt till amvändaren.

Vid utelämnandet får förenklade rutiner enligt 1.67 användas.

Identitets- och attributsintyg

1.71 Den som utfärdar identitets- eller attributsintyg inom Infrastrukturen för identifiering ska innan ett intyg lämnas ha utfört kontroller i enlighet med kraven för den aktuella tillitsnivån, vilka anges i tillitsramverket (bilaga 9).

1.72 Utfärdare och e-tjänsteleverantörer ska kontrollera varandras identitet och skydda sin kommunikation mot manipulationer och förfalskningar genom den hantering av certifikat och elektroniska stämplar som ingår i de tekniska och administrativa funktioner som utgör en del av de standardiserade rutinerna inom Infrastrukturen för identifiering.

Utfärdares ansvar

1.73 En utfärdare av Svensk e-legitimation ansvarar gentemot innehavare av Svensk e-legitimation regleras beträffande privat e-legitimation i avtal med användare och för e-tjänstelegitimationer i avtal med arbets- och uppdragsgivare.

1.74 En identitetsutfärdares ansvar gentemot en e-tjänsteleverantör för uppgifter i identitetsintygen regleras i avtal som E-tjänsteleverantören i egenskap av mellanman sluter mellan identitetsutfärdare och e-tjänsteleverantören vid anslutning enligt avsnitt 4 ovan till Infrastrukturen för identifiering.

1.75 Eftersom myndigheter under regeringen utgör samma juridiska person och sådana myndigheter ansluts genom beslut av E-legitimationsnämnden ingås sådant avtal mellan staten och respektive utfärdare av identitetsintyg genom att [ ].

1.76 Attributsutfärdares ansvar för utfärdade intyg följer allmänna regler eftersom Infrastrukturen för Svensk e-legitimation endast tillhandahåller funktioner för att förmedla sådana intyg med stöd av de register och transportmekanismer som hör till Infrastrukturen för identifiering.

1.77 [Genom denna reglering kan rättsliga skillnader när användare betalar för legitimationen – öppet system – respektive e-tjänsteleverantören betalar för förlitandet – slutet system – hanteras].

Utformning av tekniska hjälpmedel

1.78 Om identitetsutfärdaren förser användaren med tekniska hjälpmedel för att hantera e-legitimationen på ett tillförlitligt sätt ska sådana hjälpmedel utformas så att det krävs en aktiv handling för att legitimera sig eller skriva under. Rutinerna bör ta sikte på att likna de omständigheter som användaren ställs inför när han eller hon

1) visar upp en traditionell legitimationshandling för identitetskontroll, eller

2) fattar en penna och skriver under.

1.79 Tekniska hjälpmedel eller tjänster för att granska utkast inför underskrift eller att presentera underskrivna eller stämplade handlingar ska utformas så att de möjliggör

1) en tydlig och begriplig presentation av uppgifterna, och

2) att läsaren av utkast eller färdiga handlingar

b) tydligt kan se all text och om texten är undertecknad respektive stämplad, samt

c) inte ges skäl att förväxla

i. den text som granskas, för att undertecknas eller stämplas, med annan text,

ii. den underskrivna eller stämplade texten med oskyddad text eller med text som hör till andra dokument, eller

iii. elektroniskt bestyrkta handlingar med andra handlingar.

Motsvarande krav gäller för hjälpmedel eller tjänster som identitets- och attribututfärdare tillhandahåller för att presentera identitets- och attributsintyg.

1.80 Om ett tekniskt hjälpmedel för granskning av handlingar stöder hantering av olika versioner eller liknande får underskrifter och stämplar inte presenteras så att det finns risk för att läsaren missförstår vad som har undertecknats eller stämplats.

Bevarande av handlingar

1.81 Utfärdare av Svensk e-legitimation ska bevara

1) ansökningshandlingar och handlingar som rör utlämnande, mottagande eller spärr av e-legitimationer.
2) avtal, policydokument och utfärdardeklarationer, och
3) övriga handlingar och uppgifter som kan behövas för att kontrollera legitimering och elektroniska underskrifter, identifiera personer och hantera insynsskydd.

1.82 Handlingarna ska bevaras och skyddas under den tid som behövs för att tillgodose ändamålen med elektroniska underskrifter m.m. Tiden för bevarande ska inte understiga tio år och material ska kunna tas fram i läsbar form under hela denna tid. Myndigheter och andra organ för vilka arkivlagen (1990:782) gäller får gallra allmänna handlingar endast om åtgärden har stöd i lag eller annan författning eller beslut om gallring.

1.83 Identitetsutfärdare ska lämna ut information om enskilda händelser på begäran av den som behöver kontrollera en legitimering eller en underskrift. Arkiverat material får emellertid inte lämnas ut i strid mot lag eller författning eller avtal med innehavaren av e-legitimationen.

1.84 En utfärdare av Svensk e-legitimation som upphör med

sin verksamhet ska informera sina användare och berörda e-tjänsteleverantörer. Utfärdaren ska hålla arkiverat material tillgängligt.

1.85 E-legitimationsnämnden ska [på motsvarande sätt under den tid som behövs bevara handlingar av betydelse för kontroller av identitet, handlingars äkthet eller annat av betydelse inom Infrastrukturen för Svensk e-legitimation].

7. Regler för användare, m.m.

Användare av Svensk e-legitimationer som sökande och innehavare

Ansökan och avtalsvillkor

1.86 Användare ska ansöka om e-legitimation hos en utfärdare av Svensk e-legitimation och lämna de uppgifter som är nödvändiga. Användaren ska underteckna ansökan i traditionell pappersbaserad form och intyga att lämnade uppgifter är riktiga och fullständiga.

1.87 Om en sökande redan har identifierats vid ett personligt besök för att få använda bank på Internet eller någon liknande tjänst för ekonomiskt eller rättsligt betydelsefulla mellanhavanden får han eller hon använda elektroniska rutiner enligt 1.60.

1.88 Innan ansökan sker ska den sökande ha beretts tillfälle att ta del av och spara utfärdarens villkor och information enligt 1.57 samt tydligt ange om han eller hon till någon del inte godtar villkoren. En innehavares ansvar mot utfärdaren och mot förlitande parter vid fel eller försummelse bör regleras i villkoren.

Identifiering

1.89 En användare som ansöker om e-legitimation ska vidta de åtgärder som behövs för att utfärdaren ska kunna

identifiera den sökande enligt 1.59 och 1.60.

Mottagande och användning av e-legitimation

1.90 Användaren ska behandla sin e-legitimation och sin personliga kod på ett tillförlitligt sätt enligt villkoren i användarens avtal med utfärdaren.

1.91 En användare som väljer sin personliga kod får inte använda en sådan som är enkel att lista ut.

1.92 En användare ska bruka de tekniska hjälpmedel som identitetsutfärdaren tillhandahåller enligt 1.78 – 1.80 så att legitimering och elektronisk underskrift sker med tillförlitliga rutiner.

Skydd för e-legitimationer och personliga koder m.m.

1.93 Användaren ska skydda sin e-legitimation så att ingen annan får tillgång till den och sin personliga kod så att ingen annan kan få reda på den. Dessa åtgärder består bl.a. i att

1) skydda datorer och annan utrustning där e-legitimationen förvaras eller används,

2) välja en personlig kod som inte är lätt att lista ut, och

3) hålla den personliga koden hemlig och inte anteckna koden på ett sätt eller på en plats som gör att den kan kopplas till e-legitimationen.

Anmälan om spärr

1.94 En användare av en e-legitimation ska göra en spärranmälan snarast efter att denne upptäckt att det finns anledning att spärra e-legitimationen.

Användare av e-tjänstelegitimation som innehavare

1.95 En användare av en e-tjänstelegitimation får använda den endast i enlighet med instruktioner från arbets- eller uppdragsgivaren.

Arbets- eller uppdragsgivare som sökande m.m.

1.96 En arbets- eller uppdragsgivare som anskaffar e-tjänstelegitimationer bestämmer inom ramen för sin arbetsledningsrätt hur e-tjänstelegitimationen får brukas av användaren.

1.97 En arbets- eller uppdragstagare ska göra en spärranmälan snarast efter att denne upptäckt att det finns anledning att spärra en e-tjänstelegitimation som denne tilldelat en arbets- eller uppdragstagare. Anledning att spärra kan föreligga bl.a. om arbets- eller uppdragsförhållandet upphört eller en personlig kod kan ha blivit tillgänglig för någon annan.

8. Regler för e-tjänsteleverantörer

E-tjänsteleverantörernas kontroller

1.98 E-tjänsteleverantören hanterar frågor om identitet och attribut med stöd av uppgifter i intyg utfärdade av identitets- och attributsutfärdare som är anslutna till Infrastrukturen för Svensk e-legitimation.

1.99 E-tjänsteleverantörer som är anslutna till Infrastrukturen för Svensk e-legitimation bör normalt godta identitets- och attributsintyg från anslutna utfärdare, om det inte finns skäl för en annan bedömning i ett ärende. E-tjänsteleverantören bedömer vilken tillitsnivå som krävs.

1.100 Om det i det enskilda fallet finns skäl att kontrollera den autentisering som identitetsutfärdaren utfört får myndigheten begära ytterligare uppgifter från identitetsutfärdaren eller begära att användaren ska bekräfta uppgiften om identitet eller den elektroniskt underskrivna handlingen.

Av 10 § tredje stycket förvaltningslagen (1986:223), 44 § tredje stycket förvaltningsprocesslagen (1971:291) och 33 kap. 3 § tredje stycket rättegångsbalken följer att behöriga handläggare från fall till fall får avgöra om en elektroniskt undertecknad eller stämplad handling ska godtas eller om en bekräftelse ska inhämtas.

1.101 Kontroller som e-tjänsteleverantören inte utför automatiserat ska utföras av behöriga handläggare hos e-tjänsteleverantören.

Interna regler för e-tjänsteleverantören

1.102 En e-tjänsteleverantör som är ansluten till Infrastrukturen för Svensk e-legitimation bör ha interna regler om hur identifiering, äkthetskontroll och kontroll av attribut utförs.

Underskrifter och stämplar

1.103 En elektronisk underskrift ska presenteras i anknytning till den text som skrivs under, så att underskriftens innebörd framgår av sammanhanget, på samma sätt som vid underskrift på traditionellt sätt. Behövs skriftlig information om denna innebörd, t.ex. en angivelse av en fullständig firma vid firmateckning enligt 26 § firmalagen (1974:156), bör detta anges i den text som undertecknas.

1.104 Presenteras flera underskrifter på samma sida eller presenteras en underskrift så att det finns risk för att läsaren missförstår vilken text som undertecknats bör åtgärder vidtas för att förenkla och förtydliga läsarens tolkning av det som presenteras. Detsamma gäller om både skyddad och oskyddad text presenteras tillsammans.

Rutiner för att ta emot, expediera, presentera, hantera och långtidslagra elektroniska handlingar

1.105 En myndighet som tar emot eller ställer ut undertecknade elektroniska handlingar ska säkerställa att de krav som de kryptografiska rutinerna för med sig beaktas från arkivsynpunkt. I Riksarkivets föreskrifter finns bestämmelser om framställning, hantering, förvaring och skydd av allmänna handlingar.

1.106 Myndigheter bör tydligt anvisa de mottagningsställen där myndigheten tar emot elektroniska handlingar. [Detta behövs dock inte inom ramen för t.ex. webbformulär och webbtjänster där adresseringen till mottagande myndighet sker automatiskt.]

1.107 Kvittenser bör utfärdas. Kvittenser och andra bekräftelser från myndigheter bör utformas så att det inte finns risk för att mottagaren vilseleds om vad som har undertecknats eller stämplats.

9. Persondataskydd

1.108 Utfärdare av Svensk e-legitimation, identitets- och attributsutfärdare och e-tjänsteleverantörer får inom Infrastrukturen för Svensk e-legitimation inhämta personuppgifter endast direkt från den som uppgifterna avser eller med dennes uttryckliga samtycke och endast i den utsträckning som det är nödvändigt för att utfärda eller upprätthålla funktioner för e-legitimationer och identitets- och attributsintyg. Uppgifterna får inte samlas in eller behandlas för andra ändamål utan uttryckligt samtycke från den som uppgifterna avser.

10. Bevarande, säkerhet och tillsyn

1.109 E-tjänsteleverantörer, identitets- och attributsutfärdare ska tillämpa ett ledningssystem för informationssäkerhet. Detta innefattar bl.a. att

1) upprätta en informationssäkerhetspolicy och andra styrande dokument som behövs för informationssäkerheten,

2) utse en eller flera personer som leder och samordnar arbetet med informationssäkerhet,

3) klassificera sin information med utgångspunkt i krav på sekretess, riktighet, tillgänglighet och spårbarhet,

4) utifrån risk- och sårbarhetsanalyser och inträffade incidenter avgöra hur risker ska hanteras, samt besluta om åtgärder för aktörens informationssäkerhet,

5) dokumentera vidtagna granskningar och säkerhetsåtgärder av större betydelse.

1.110 Ledningen inom en e-tjänsteleverantör, identitets- eller attributsutfärdare ska löpande informera sig om arbetet med informationssäkerhet samt minst en gång per år följa upp och utvärdera detta arbete.

1.111 E-tjänsteleverantör och identitets- och attributsutfärdare ska bedriva sitt arbete enligt 1.109 och 1.110 i former enligt följande etablerade svenska standarder för informationssäkerhet;

1) Ledningssystem för informationssäkerhet – Krav (SS-ISO/IEC 27001: 2006 fastställd 2006-01-19), och

2) Riktlinjer för styrning av informationssäkerhet (SS-ISO/IEC 27002:2005 fastställd 2005-08-12).

1.112 Revision och rapporteringsskyldighet[1].

[1] Utredningen arbetar vidare med att ta fram ett förslag till slutrapporten.

Förslag till riktlinjer för federationsoperatörer

1 Tillämplighet

Dessa förslag till riktlinjer för federationsoperatörer är tillämpliga för aktörer som avser tillhandahålla en identitetsfederation under E-legitimationsnämndens regelverk för identitetsfederationer inom ramen för Infrastrukturen för Svensk e-legitimation.

2 Inledning

En identitetsfederation består av ett antal leverantörer av identitetstjänster (identitetsutfärdare) och förlitande parter (e-tjänsteleverantörer) som samverkar inom ramen för vissa regler, standarder och tekniska lösningar så att identitetsutfärdare kan tillhandahålla trovärdig identitetsinformation till förlitande parter.

Medan en identitetsfederation med några få aktörer kan bygga på att alla deltagare ingår avtal med alla andra som deltar, måste en stor identitetsfederation styras av en federationsoperatör som kan samordna viktiga standarder, tillhandahålla grundläggande tjänster till alla deltagare i federationen och sluta avtal så att avtalsfloran begränsas.

I detta dokument ges förslag till riktlinjer för en federationsoperatör som ska svara för en identitetsfederation för e-legitimationer i Sverige. Begreppet e-legitimation används här som en samlingsbeteckning certifikat, säkerhetsdosor eller andra sådana identifieringslösningar som uppfyller kraven för anslutning till den svenska modellen för legitimering och underskrift i elektronisk miljö.

Federationsoperatören upprätthåller ett ramverk för tillit som deltagarna i federationen är beroende av och ska

- bestämma regler och tekniska standarder för den som är ansluten till federationen, bl.a. för hur

  - e-legitimationer utfärdas och hanteras;
  - användares personliga integritet ska skyddas,
- tillhandahålla regler för certifiering av deltagare i federationen, och
- samla in och tillhandahålla uppgifter som beskriver deltagares tjänster och tillhandahålla information och nycklar för säkert informationsutbyte och identifiering av federationens medlemmar (s.k. metadata).

Utöver dessa grundläggande uppgifter för att skapa tillit till federationen ska federationsoperatören

- tillhandahålla stöd för att lösa frågor när aktörerna inte är eniga (tvistlösning) och att testa överensstämmelse med tekniska normer och förmågan att samverka (s.k. interoperabilitet),
- upphandla och sluta avtal om vissa tjänster som ska vara tillgängliga för anslutna till Svensk e-legitimation.

För att federationsoperatören ska kunna utföra alla dessa uppgifter på ett effektivt sätt måste denna ha resurser, personal och förmåga att ingå de avtal och bestämma de regler för identitetsfederationen som faller inom ramen för federationsoperatörens kompetens.

3 Dokumentation och processer

Identitetsfederationen ska drivas i enlighet med bestämda regler och standarder för anslutning och användning. Hit hör bl.a.

- ett regelverk för identitetsfederationen som ska
  - definiera klasser av anslutna till federationen, såsom identitetsutfärdare, e-tjänsteleverantörer och vissa attributsutfärdare,
  - ange operativa rättigheter och skyldigheter för anslutna,
  - reglera deltagande i och ansvar för federationen,
  - bestämma en process för hur säkerhetsincidenter ska hanteras inom federationen,
- dokument som anger krav eller ger vägledning för anslutna till federationen beträffande de tekniska lösningar och de förfaranden och processer som anslutna ska använda för att delta i federationen; bl.a.

- ett tillitsramverk som anger
  - processer för att kontrollera användares identitet;
  - metoder och faser genom olika stadier av e-legitimationers livscykel för förvaring och skydd av dem,
- en tvistlösningsmekanism för anslutna till federationen,
- krav på informationssäkerhet i anslutna e-tjänste-leverantörers tjänster och skydd för personuppgifter och sekretess,
- tekniska specifikationer av
  - protokoll som ska stödjas vid informationsutbyte inom federationen,
  - attribut som kan ingå i identitets- eller attributsintyg;
  - metadata och åtkomst till sådana,
  - anvisningstjänster för att finna tjänster inom federationen,
- regler och förfaranden för att kontrollera att den som är ansluten till federationen följer de regler, processer och specifikationer som gäller för anslutna,
- avtal för anslutna till Svensk e-legitimation

4 Ansökan om deltagande

Federationsoperatören ska verka inom ramen för regler för att definiera och hantera ansökningar om deltagande i federationen.

5 Tillitsskapande åtgärder

5.1 Tillitsramverk och integritet

Ett grundläggande del i identitetsfederationen är att utarbeta regelverk och tekniska och operativa krav så att anslutna har förtroende för federationen. För identitetsutfärdare innefattar detta krav på identifiering av användare, utfärdande av e-legitimationer, e-legitimationers kvalitet och hantering samt säker lagring och kommunikation av identiteter och annan information. Detta arbete ska säkerställa en korrekt hantering av information och skydd för användares personliga integritet.

5.2 Samordning av regelverk och riktlinjer

Om en identitetsutfärdare som ska anslutas till identitetsfederationen redan har fastställda regler för identitetshantering, kan det dessa regler och hur de förhåller sig till reglerna för federationen kartläggas. Federationsoperatören ska i samverkan med identitetsutfärdaren svara för denna kartläggning.

5.3 Teknisk interoperabilitet och testning

Alla autentiseringsmekanismer och protokoll som används inom identitetsfederationen bör testas för att se till att de fungerar bland dem som är anslutna. Då protokoll som används för att förmedla information om identitet och tillitsnivå är avgörande för federationens funktion bör federationsoperatören definiera hur dessa protokoll ska testas för driftskompatibilitet, inklusive tester för e-tjänsters svar på felaktigt införande av protokoll hos identitetsutfärdare eller i attributstjänster. Även protokoll för distribution av metadata och respons vid felaktiga metadata bör testas.

6 Förhandlingar om avtal

Avtal om deltagande i identitetsfederationen ska ingås mellan federationsoperatören och de som ansluts. Dessa avtal ska vara likvärdiga för alla anslutna.

Behörighetshantering med stöd av attribut

Behörighetshantering med stöd av attribut 215

1.1 Funktioner med olika användningsområden..... 216

1.2 Juridisk behörighet – en granskning i flera led 216

1.3 Åtkomstkontroll och inre sekretess – gränsdragningar 217

1.4 Elektroniska registerutdrag..... 219

1.5 Behovet av kontroll – olika nivåer 221
1.5.1 Riskfördelning enligt lag 221
1.5.2 Ett balanserat risktagande 222

1.6 Processen för granskning och samverkan 225

1.7 En samordnad hantering av Attributsintyg..... 228
1.7.1 Bolagsverkets nuvarande tjänster 228
1.7.2 XML-paket..... 228
1.7.3 Automatiserade tolkningar 230

1.8 Kommuner 234

1.9 Landsting..... 235

1.10 En samordning kräver fortsatta analyser..... 236

1.1 Funktioner med olika användningsområden

Till den föreslagna Infrastrukturen för identifiering hör också hanteringen av attribut. Medan en beskrivning av Identitetsintyg och hur de används är relativt enkel att göra, i vart fall på ett övergripande plan, blir variationsmöjligheterna många så snart en samordnad infrastruktur för hantering av attribut ska övervägas för hela den offentliga sektorn. Även små myndigheter behöver smidigt kunna integrera, använda och administrera inte bara rena Identitetsintyg utan även intyg med attribut. Härvid uppkommer emellertid en spännvidd i juridiska och tekniska krav som saknar motsvarighet på området för identifiering och som inte kunnat genomlysas i erforderlig omfattning inom ramen för utredningens begränsade uppdrag.

I det följande ska dessa varierande förutsättningar belysas med exempel från Bolagsverkets hantering av registerutdrag och hälso- och sjukvårdens behov av attribut.

1.2 Juridisk behörighet – en granskning i flera led

En juridisk person kan inte agera själv – det krävs att organ såsom styrelse, verkställande direktör, befullmäktigade ombud eller liknande utför rättshandlingar för den juridiska personens räkning. Korrekta bedömningar förutsätter en genomgång i flera led – en slags process – som är allmänt vedertagen i pappersmiljö. Den består normalt av följande led.

1. Vilken *fysisk person* har företagit rättshandlingen?	Här används underskrifter, legitimationshandlingar, m.m. för att knyta en fysisk person till rättshandlingen.
2. Har personen agerat för egen eller *för annans räkning*?	I vems namn har rättshandlingen företagits? Här används t.ex. firmateckning för att klargöra att åtgärden vidtagits i egenskap av företrädare för annan.
3. Är den som agerat som företrädare för annan *behörig* att företa rättshandlingen?	Här används registreringsbevis (utvisande t.ex. firmateckningsrätt), fullmakter o.l.

En fullständig granskning av ovan nämnda omständigheter i varje enskilt fall blir tungrodd. I traditionell miljö har därför *förenklade förfaranden* vuxit fram, t.ex. att för vissa mindre transaktioner

godta en persons uttryckliga eller underförstådda påstående om behörighet.

Med en e-legitimation kan endast första steget i processen kontrolleras; dvs. (1) vilken fysisk person som agerar. Av e-legitimationen framgår inte om innehavaren (2) avser att agera för egen eller för annans räkning eller (3) är behörig att företräda en uppgiven huvudman vid rättshandlingar. Det är vanligt att tvister uppstår beträffande frågan om en viss rättshandling har företagits för *egen* räkning (t.ex. när ett bolag, som alternativt skulle kunna ses som huvudman, har försatts i konkurs) eller som *företrädare* för ett företag (vilket till skillnad från den fysiska personen har förmåga att betala).

1.3 Åtkomstkontroll och inre sekretess – gränsdragningar

Liknande frågor om roller och egenskaper uppkommer inom ett organ. Varje myndighet och varje företag av någon storlek styr numera åtkomsten till och rättigheter i egna informationssystem genom s.k. behörighetskontrollsystem (BKS). Föreskrifter om sådana begränsningar – i vissa sammanhang kallad inre sekretess – finns i patientdatalagen (2008:355; PDL), för vårdgivare. Här är det avgörande om en person är t.ex. läkare eller sjuksköterska och om personen deltar i vården av en viss patient eller av annat skäl behöver uppgifter om patienten för sitt arbete inom hälso- och sjukvården.[1] Begreppet ”behörighet” används emellertid även i det sammanhanget och enligt 4 kap. 2 § PDL ska en vårdgivare bestämma villkor för tilldelning av behörighet för åtkomst till sådana uppgifter om patienter som förs helt eller delvis automatiserat. Härvid föreskrivs att behörigheten ska begränsas till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården.

När sådan åtkomstkontroll införs blir det alltså inte fråga om kontroll av om en person *i juridisk mening* är behörig att företrädare ett rättssubjekt (t.ex. ett annat aktiebolag eller en annan myndighet). Det blir istället fråga om att *begränsa åtkomsten* till uppgifter och resurser i informationssystem inom en och samma

[1] Enligt 4 kap. 1 § PDL får den som arbetar hos en vårdgivare ta del av dokumenterade uppgifter om en patient endast om han eller hon deltar i vården av patienten eller av annat skäl behöver uppgifterna för sitt arbete inom hälso- och sjukvården.

vårdgivare.[2] Samtidigt aktualiseras emellertid en slags behörighetskontroll, dels genom att ett landsting eller en kommun som bedriver hälso- och sjukvård genom *flera myndigheter* får ha direktåtkomst till personuppgifter som behandlas av någon annan sådan myndighet i *samma landsting* eller kommun (5 kap. 5 § PDL), dels genom att en vårdgivare under vissa förutsättningar får ha direktåtkomst till personuppgifter som behandlas av *andra vårdgivare* (6 kap. 1 § PDL). Här aktualiseras alltså två olika typer av ”direktåtkomst” – den ena inom en vårdgivare, den andra mellan vårdgivare. För den senare typen av direktåtkomst krävs enligt huvudregeln att patienten lämnat sitt samtycke, att uppgifterna rör en patient som det finns en aktuell patientrelation med och att åtkomsten kan antas ha betydelse för att förebygga, utreda eller behandla sjukdomar och skador hos patienten inom hälso- och sjukvården.

Skillnaden mellan dessa olika typer av kontroller är alltså betydande. Endast några få personer ges *juridisk behörighet* att företräda en juridisk person medan *åtkomstkontroller* införs för alla anställda och uppdragstagare som ska ges åtkomst till informationssystem. En annan skillnad är att juridisk behörighet vanligtvis bestäms *grovmaskigt*; jfr att styrelsen enligt 8 kap. 39 § aktiebolagslagen (2005:551; ABL) får föreskriva att rätten att företräda bolaget och teckna dess firma får utövas endast av två eller flera personer i förening medan *andra inskränkningar* i en firmatecknares rätt att teckna bolagets firma *inte får registreras*. Denna grova avgränsning bör ställas mot åtkomstkontroll till informationssystem där användarnas rätt till åtkomst vanligtvis ges en finmaskig utformning.

Till detta kommer regleringen i patientdatalagen som innehåller en blandning av krav på *åtkomstkontroll* inom respektive mellan myndigheter och andra organ och krav på en slags juridisk behörighetskontroll mellan olika organ. Det finns risk för att dessa variationer i reglering och i hantering av åtkomst- respektive *behörighetskontroller* missförstås när tekniska och administrativa lösningar ska utarbetas för bl.a. Identitets- och Attributsintyg.

System för *åtkomstkontroll* ger alltså – utanför hälso- och sjukvårdsområdet – endast ett inre skydd som, till skillnad från juridisk behörighetskontroll, inte visar om en person äger rätt att

[2] Här finns också föreskrifter om att patienter får motsätta sig att personal vid en annan vårdenhet eller inom en annan vårdprocess hos samma vårdgivare gör personuppgifter som dokumenterats för vårdändamål tillgängliga genom elektronisk åtkomst (4 kap. 4 § PDL).

företräda annan vid rättshandlingar. Attributsintyg bör primärt utformas med tanke på juridiska behörighetskontroller. Det finns emellertid inget hinder mot att dessa Identitets- och Attributsintyg – när det visar sig lämpligt – används även inom en och samma juridiska person, t.ex. en vårdgivare, för att styra anställdas och uppdragstagares åtkomst utifrån relevanta attribut. Dessa användningsområden får emellertid inte blandas samman.

Dessa grundläggande skillnader kan därmed beskrivas så att det

- vid *juridisk behörighetskontroll* ska granskas om en person har sådan rätt att agera (t.ex. är ställföreträdare eller fullmäktig för ett aktiebolag) att *den som företräds* (i detta exempel aktiebolaget) *blir juridiskt bunden*, t.ex. av avtal eller andra åtaganden, men
- vid *åtkomstkontroll* ska granskas om personen *har rätt att få tillgång* till uppgifter eller andra resurser i informationssystem, och
- *inom hälso- och sjukvården* utförs kombinationer av kontroller för vilka en omfattande särreglering införts.

Utvecklingen av en Infrastruktur för Svensk e-legitimation får inte blandas samman med det utvecklingsarbete som utförs i annan ordning, t.ex. inom hälso- och sjukvården för att uppfylla patientdatalagens krav. E-legitimationsnämnden bör visserligen skapa förutsättningar för att de lösningar för identifiering och behörighetskontroller, som redan införts inom t.ex. hälso- och sjukvården, ska kunna tas tillvara även inom en ny Infrastruktur för identifiering. Åtkomstkontroll får härvid inte blandas ihop med juridiska behörighetskontroller. De måste också hållas isär från särskilda kontroller som krävs för att uppfylla patientdatalagens krav.

1.4 Elektroniska registerutdrag

Juridiska behörighetskontroller bör inom Infrastrukturen för identifiering kunna hanteras så att en Användare först legitimerar sig med e-legitimation och att E-tjänsteleverantören – efter att ha granskat identitetsintyget – ställer en attributsintygsfråga till en utfärdare inom Infrastrukturen för identifiering. För att förenkla framställningen utgår vi i det följande från att det är ett aktiebolag

som den identifierade personen påstår sig företräda och att det är Bolagsverket som ska lämna ett utdrag ur aktiebolagsregistret.

Lösningen kan utformas så att *Bolagsverket ställer ut* Attributsintyg med registerutdrag, som skyddas mot förfalskningar och andra angrepp med stöd av de infrastrukturcertifikat som tillgängliggörs i utfärdar- och e-tjänsteregistren för var och en som är ansluten. *E-tjänsteleverantören kontrollerar*, i egenskap av förlitande part, dels att Attributsintyget är äkta, dels att uppgifterna visar att angiven person är behörig att företräda angivet aktiebolag. E-tjänsteleverantörer bör ges möjlighet att tolka behörighetsinformationen såväl automatiserat (i maskinläsbar form) som manuellt (i vanlig läsbar form på t.ex. bildskärm eller i form av en utskrift). Det är emellertid inte Bolagsverkets uppgift att tillhandahålla sådant stöd och behovet av stöd varierar från E-tjänsteleverantör till E-tjänsteleverantör.

En myndighet som behöver göra många kontroller av juridisk behörighet, t.ex. Skatteverket, bör införa en automatiserad funktion för juridisk behörighetskontroll med stöd av Attributsintyg. Ansvars- och riskfördelningen kan bli densamma som idag genom att Bolagsverket endast lämnar registerutdrag. E-tjänsteleverantören (förlitande part) får därefter bedöma om de uppgifter som lämnats i utdraget ger tillräckligt underlag för att Användaren ska anses behörig att logga in eller skriva under i egenskap av företrädare för aktiebolaget. På samma sätt som idag får alltså E-tjänsteleverantören bedöma t.ex. om e-tjänsten endast används för sådant som utgör löpande förvaltningsåtgärder enligt 8 kap. 36 § ABL, så att den verkställande direktören är behörig att agera för bolagets räkning även om denne inte har ensam firmateckningsrätt. Det bör vidare krävas att varje e-tjänst utformas så att Användaren otvetydigt måste ange om tillträde, uppgiftslämnande, underskrift eller andra åtgärder i en e-tjänst utförs för egen eller för annans räkning och vem det är som i så fall företräds.

En lösning för automatiserade kontroller bör förenas med anpassningar för mindre myndigheter, antingen så att intyg kan granskas och bedöms manuellt eller så att de ges ett förenklat innehåll, t.ex. att en kod lämnas utifrån en klassificering som Bolagsverket stöder så att maskinella kontroller kan förenklas. En viss siffra i ett fält kan t.ex. visa att en individ (angiven med personnummer) är behörig att ensam teckna bolagets (angivet med organisationsnummer) firma.

För att inte riskera att rubba dagens ansvarsfördelning mellan Bolagsverket och den som litar på ett registerutdrag (här E-tjänsteleverantören) skulle sådana koder kunna införas enligt specifikationer som tillkommer efter samråd med berörda aktörer och fastläggs av Bolagsverket, t.ex. i en myndighetsföreskrift för tjänsten, där det framgår vad koderna står för och samtidigt klargörs att förlitande part själv får bedöma vilken verkan dessa uppgifter kan anses ha vid en juridisk behörighetskontroll.

En sådan hantering bör kunna utformas så att den blir tekniskt enkel att införa och använda. Den torde inte heller förutsätta några ändringar i lag eller förordning eftersom den endast innebär att Bolagsverket lämnar utdrag ur sina register. Utmaningen blir istället att finna en samsyn kring detaljer så att lösningen kan införas på ett samordnat och enhetligt sätt.

1.5 Behovet av kontroll – olika nivåer

1.5.1 Riskfördelning enligt lag

Att en fysisk person i juridisk mening är behörig att företräda annan innebär som framgått att huvudmannen, t.ex. ett aktiebolag, blir direkt bunden av en rättshandling som företrädaren företar. Det vilar emellertid på förlitande part att kontrollera att behörighet verkligen föreligger. Förlitande part står normalt också risken om det godtas att en person är behörig men detta senare visar sig felaktigt. Här bör nämnas att det av regler i bl.a.

- skuldebrevslagen (SkbrL), framgår att motparten står risken om
  - uppgiven företrädare för en part
    - inte är den han eller hon ger sig ut för att vara (kan kontrolleras med e-legitimation), eller
    - *saknar behörighet* att företräda uppgiven huvudman (kan kontrolleras med registreringsbevis),
  - urkunder, t.ex. skriftliga avtal, registreringsbevis eller fullmakter är falska (kan kontrolleras med e-legitimation om de försetts med elektronisk underskrift),[3]

[3] Enligt 17 § skuldebrevslagen (SkbrL) får förfalskning och bristande behörighet åberopas även mot den som är i god tro och i detta hänseende ger SkbrL uttryck för en allmän förmögenhetsrättslig princip som tillämpas analogt även utanför skuldebrevsrätten. Visserligen avser denna bestämmelse löpande skuldebrev men i lagmotiven har det, med avseende på enkla skuldebrev, uttalats att en gäldenär som regel har att på egen risk pröva

- rättegångsbalken (RB), framgår att resning kan beviljas sedan dom i tvistemål eller brottmål vunnit laga kraft, om en falsk skriftlig handling har åberopats till bevis och handlingen kan antas ha inverkat på utgången och att detsamma torde gälla om talan förts för en juridisk persons räkning där dennes anspråk t.ex. eftergivits helt utan behörighet att agera för denne,[4]
- aktiebolagslagen och aktiebolagsförordningen, framgår att register ska föras av Bolagsverket, att verket ska lämna utdrag men att verkets ansvar i princip är begränsat till att lämnade utdrag som rätt återger innehållet i aktiebolagsregistret – den som mottar och brukar utdrag avgör för vilka kontroller utdragen ska användas, hur kontrollerna ska utföras och står risken om behörighet felaktigt antas föreligga.

Författningsregleringen innebär alltså något förenklat att det är E-tjänsteleverantören (förlitande part) som står risken om det finns brister i behörighetskontrollerna.

1.5.2 Ett balanserat risktagande

Vissa ärenden rör känsliga uppgifter eller stora värden. I sådana fall görs vanligtvis en *fullständig kontroll* av juridisk behörighet, där det på ett tillförlitligt sätt granskas både vem som agerat och om denne var behörig att företa rättshandlingen för angiven huvudmans räkning. I praktiken gör emellertid förlitande parter riskbedömningar utifrån vilka de utformar sina kontroller. Sådana bedömningar kan i många fall leda till att *ingen kontroll* görs av t.ex. registreringsbevis eller fullmakter. Förlitande part utgår från att den som utger sig för att vara behörig företrädare verkligen är det. Skulle påståendet om behörighet vara felaktigt kan den som utgett sig för att ha behörighet bli skadeståndsskyldig mot förlitande part.

Som exempel på uttalanden rörande behovet av balanserade riskbedömningar kan nämnas att justitierådet Henrik Hessler i en äldre monografi ”Obehöriga förfaranden med värdepapper” uttalat att praktiskt taget alla transaktioner enligt sakens natur innebär att aktörerna måste ta vissa risker för att allt inte har gått rätt till och att det knappast är möjligt att helt eliminera dessa risker; ”i allt fall

huruvida den med vilken han har att skaffa är rätt borgenär eller behörig att på dennes vägnar uppbära betalning.

[4] Se 58 kap. 1 och 2 §§ RB.

skulle rigorösa försök i denna riktning sannolikt resultera i att verksamheten blev orimligt tungrodd". Hessler tillade bl.a. följande, som torde anses vara en självklarhet i pappersmiljö:

> I åtskilliga situationer kan dock (banken) blott genom utvisande av skälig aktsamhet och sålunda utan någon krävande försiktighetsapparat skydda sig mot förlustrisk. Ett klarläggande så långt möjligt av i vilka lägen en sådan aktsamhet är på sin plats samt kanske fram för allt vad den bör gå ut på och hur långt den behöver sträckas torde därför vara av praktiskt värde till underlättande av verksamhetens bedrivande; det förekommer väl icke blott att erforderlig aktsamhet eftersätts utan ej sällan också att man i brist på säker kännedom om rättsläget drivs att iakttaga en större försiktighet än nöden i själva verket kräver, vilket blir en onödig belastning på rörelsen.

Detta uttalande passar väl in på dagens hantering av kontroller i elektronisk miljö. E-tjänsteleverantörerna, som ska ställa upp de krav som en e-tjänst ska uppfylla bl.a. beträffande kontroll av behörighet, tenderar att ställa synnerligen höga krav så snart IT-stöd införs. En orsak kan vara en sammanblandning av de behov som finns av juridisk prövning av bl.a. identitet och behörighet med behov från informationssäkerhetssynpunkt av att skydda E-tjänsteleverantörens IT-miljö.[5]

Myndigheter kan emellertid i många fall – i vart fall initialt – förväntas införa e-tjänster utifrån enklare lösningar med manuella inslag. Här bör resonemang från pappersmiljön ofta kunna återanvändas så att förenklingar anses möjliga. I många fall bör en identifiering med t.ex. e-legitimation kunna räcka, utifrån enkla, närmast självklara resonemang. Som exempel kan nämnas att ärenden där t.ex. telefaxmeddelanden eller kanske till och med uppgiftslämnande per telefon godtas utan några behörighetskontroller knappast kan anses kräva fullständiga behörighetskontroller bara för att hanteringen har överförts till elektronisk miljö.

Begränsningar av behörighetskontroller godtas också enligt lag. Varken i förvaltningslagen (1986:223) eller lagen (1996:242) om domstolsärenden föreskrivs att en myndighet som handlägger ett ärende måste begära in och granska registreringsbevis eller fullmakt för ett ombud.[6] Däremot *får* myndigheten begära in behörighetshandlingar om myndigheten finner skäl för en sådan kontroll.

[5] En del i detta kan antas vara att automatiseringen medför att det saknas motsvarighet till den sociala kontroll som finns i pappersmiljö, så att handläggare reagerar om något verkar misstänkt. Vidare tar sig informationssäkerhetsarbetet ofta sådana uttryck att det inte görs några jämförelser med motsvarande riskbedömningar i pappersmiljö.

[6] Motsatsen gäller emellertid i tvistemål och brottmål enligt rättegångsbalken.

Visserligen innebär det ett risktagande när en myndighet använder sig av möjligheten att begränsa behörighetskontrollerna. Det har emellertid i praktiken visat sig fungera i pappersmiljö. På motsvarande sätt godtar företag ofta beställningar av varor per telefon, telefax o.l. – utan någon identitets- eller behörighetskontroll. Samma synsätt bör kunna tillämpas för e-tjänster. Har Användaren identifierats med stöd av e-legitimation och detta kontrollerats med hjälp av Identitetsintyg torde dessa åtgärder ofta räcka. Här bör motsvarande praktiska synsätt kunna tillämpas som i traditionell miljö – med de anpassningar som behövs till särskilda risker som IT kan föra med sig.

I traditionell miljö är det som framgått vanligt att identitets- och behörighetskontroller inte görs. För dessa fall skulle ett förenklat förfarande för IT-miljö där identifiering sker med Identitetsintyg men registerutdrag från Bolagsverket inte krävs innebära en noggrannare kontroll än den som görs i traditionell miljö när underskrifter godtas utan kontroller. Därmed bör det i många fall – i kombination med det skadeståndsansvar som följer av felaktiga påståenden om behörighet – räcka att den som agerar identifieras med stöd av Identitetsintyg samt att e-tjänsten utformas så att det otvetydigt framgår

- om personen agerar för egen eller för annans räkning, och
- för vem ett agerande för annans räkning sker.

I andra sammanhang kan en fullständig behörighetskontroll framstå som självklar, jfr de kontroller som görs av en ansökan om lagfart, i rättegång eller när betalning beordras av betydande belopp från ett konto i en bank. Vanligtvis finns inga särskilda regler om vilken dokumentation av behörighet som ska finnas och vilka kontroller som ska göra.[7] Det blir då upp till E-tjänsteleverantören att, utifrån det skyddsvärde som respektive e-tjänst anses ha, bedöma vilka krav som ska ställas på behörighetskontroller. Hanteringen av Attributsintyg får utformas utifrån dessa förutsättningar.

[7] Jfr dock rättegångsbalkens krav på bl.a. registreringsbevis och fullmakter och den redovisade särregleringen i patientdatalagen.

1.6 Processen för granskning och samverkan

När juridisk behörighet ska kontrolleras i elektronisk miljö bör hanteringen kunna förenklas med stöd av den föreslagna Infrastrukturen för identifiering. Denna hantering kan, som en följd av den *automatisering* som sker i IT-system, beskrivas som ett handlings- eller transaktionsmönster – i IT-sammanhang kallat en *process* (jfr avsnitt 1.1). Denna process kan beskrivas som ett antal steg där berörda aktörer har att

1. bedöma om registreringsbevis eller liknande behövs,
2. beställa registreringsbevis,
3. sända en beställning till rätt aktör,
4. motta beställningen,
5. se vilket intyg som ska lämnas enligt beställningen,
6. upprätta intyg,
7. sända intyget till rätt aktör,
8. motta intyget,
9. kontrollera att intyget är äkta, och
10. bedöma om intygets innehåll ska anses visa att behörighet föreligger.

När en person i traditionell miljö utger sig för att företräda att aktiebolag används vanligtvis registreringsbevis från Bolagsverket för en manuell granskning och bedömning. Bolagsverket tillhandahåller emellertid redan idag tjänster där elektroniska bevis med utdrag ur aktiebolagsregistret lämnas i XML-format. En förlitande part som mottagit ett sådant elektroniskt utdrag kan behandla det automatiserat enligt programmerade rutiner genom vilka det avgörs om behörighet anses föreligga för att t.ex. logga in i en e-tjänst, få del av uppgifter där eller lämna och skriva under uppgifter.

Skatteverket använder sig redan av denna elektroniska tjänst som fungerar som en del i den process som krävs för en helt automatiserad hantering; jfr processtegen i följande figur.

Skatteverket har också utformat en egen automatiserad procedur för att avgöra om uppgifterna i ett XML-baserat registreringsbevis visar att personen är behörig att företräda det aktuella bolaget.

Utformning och användning av vissa processteg i figuren bestäms i princip av respektive E-tjänsteleverantör, utifrån det skyddsvärde som leverantören anser att e-tjänsten har; se de steg som ligger utanför det röda fältet i följande figur. Däremot tar Bolagsverket emot beställningarna, ser vilka intyg som ska utfärdas samt upprättar och sänder dem.

Eftersom den föreslagna Infrastrukturen för identifiering avses användas, för dessa beställningar och svar, berörs även E-legitimationsnämnden som i denna del, i enlighet med sin instruktion, ska utveckla specifikationer och liknande krav som ska vara gemensamma för myndigheter under regeringen. Utformningen av juridiska behörighetskontroller med stöd av Attributsintyg kräver alltså samverkan mellan (A) E-legitimationsnämnden (som svarar för Infrastrukturen för identifiering via vilken begäran om intyg och utfärdade intyg distribueras), (B) Bolagsverket (som svarar för angivna delar i processen för att utfärda Attributsintyg) och de (C) E-tjänsteleverantörer som ansluts till Infrastrukturen för

identifiering och som ska kunna beställa, motta och använda Attributsintyg.

En del i denna samverkan är att utarbeta samordnade lösningar som är tillräckligt enkla och avgränsade för att kunna införas på bred front, så att även mindre aktörer, inom offentlig sektor kan nyttja dem. Målet bör vara en fullständig automatisering. Här behöver emellertid beaktas att myndigheter i många fall – i vart fall initialt – kan antas införa e-tjänster utifrån enklare lösningar med manuella inslag. I sådana fall bör resonemang från pappersmiljö ofta kunna återanvändas och förenklingar vara möjliga utifrån närmast självklara resonemang som var och en bör kunna förstå. Här kan som exempel nämnas ärenden där t.ex. telefaxmeddelanden eller kanske till och med uppgiftslämnande per telefon godtas. När samma ärenden handläggs i elektronisk miljö kan fullständiga behörighetskontroller knappast krävas, med e-legitimationer och attributsintyg, bara för att IT-stöd införts.

Här behöver också beaktas att kontroller av juridisk behörighet kan bli komplicerade i enskilda fall. Behörighetsfrågan behöver då – om en fullständig kontroll ska göras – bedömas manuellt. I undantagsfall kan rättsutredningar och bedömningar av expertis behövas. Sådana komplicerade juridiska bedömningar kan inte automatiseras eftersom de inte kan styras av på förhand programmerade lösningar.

Väljer den förlitande parten att ta en medveten risk kan automatisering dock ske även i sådana fall. Tolkningssvårigheterna uppdagas då inte förrän i ett senare skede när transaktionen redan utförts. Ett skäl för att godta sådana förenklingar kan vara ett en uppgiven företrädare har ett strängt personligt skadeståndsansvar gentemot den förlitande parten: Enkelt uttryckt, blir organisationen inte bunden av beställningen kan användaren av e-legitimationen bli skyldig att ersätta den skada som därmed drabbar den förlitande parten. Dessa regler gäller även för elektronisk miljö så länge inte annat föreskrivs.

Den infrastruktur som E-legitimationsnämnden inför för juridiska behörighetskontroller bör tillhandahålla de funktioner och kontrollnivåer som e-tjänstelevererande myndigheter och företag efterfrågar. Det får därefter bli upp till respektive E-tjänsteleverantör att utifrån beskrivna flöden avgöra vilket stöd för behörighetskontroller som ska införas i en e-tjänst. Denna infrastruktur får som framgått inte blandas samman med åtkomstkontroller inom en organisation eller de kombinationer av

kontroller för vilka särskild reglering har införts i patientdatalagen m.fl. författningar.

1.7 En samordnad hantering av Attributsintyg

1.7.1 Bolagsverkets nuvarande tjänster

Bolagsverket har dels en *myndighetsutövande funktion*, till vilken hör att registrera företag (bl.a. aktiebolag som här används som exempel), dels en *servicefunktion* som innefattar att *tillhandahålla företagsinformation* från verkets register (bl.a. Aktiebolagsregistret). Informationen tillhandahålls på flera olika sätt till förlitande parter, som t.ex. kan beställa ett traditionellt registreringsbevis på papper och få det översänt med vanlig post.[8] Den som behöver information om företag kan emellertid också söka fram samma uppgifter i verkets Näringslivsregister och ladda ned e-registreringsbevis i ett format som var och en kan läsa. Det är också möjligt att beställa eller ladda ned ett fullständigt eller tidsbegränsat historiskt bevis där alla ändringar, respektive de ändringar som skett under viss tid redovisas.

Den som inte nöjer sig med att få reda på vilka uppgifter som redan har registrerats i Aktiebolagsregistret kan beställa diariebevis eller ärendebevis, där det i det första fallet framgår om en handling som rör ett visst bolag har kommit in och i det andra fallet dessutom framgår vilket slags ärende som inkommen handling avser. Till detta kommer Bolagsverkets särskilda beställningsverksamhet där uppgifter lämnas ur register förpackade i enlighet med en beställares önskemål.

1.7.2 XML-paket

Leveranser i elektronisk miljö

Bolagsverket har även infört tjänster där s.k. XML-paket levereras. En av dessa produkter, betecknad ”FunktionarerFirmateckning-Vakanser”, visar bl.a. firmateckning; dvs. samtliga företrädare som är registrerade. Dessa XML-paket kan levereras även med historik. Automatiserade frågor efter sådana paket ställs med organisations-

[8] Beviset innehåller bl.a. företagets namn, registreringsdatum, verksamhet, firmatecknare, styrelse, företrädare samt adressen till företaget och till styrelsen.

nummer som sökbegrepp. Den som mottar XML-paket avses kunna låta egna datorprogram bearbeta och visa uppgifter i egna gränssnitt.

Dessa tjänster tar liksom de som beskrivits i avsnitt 1.6.1 s*in utgångspunkt* i det aktuella *aktiebolaget*. Bolagets organisationsnummer används som sökbegrepp. E-tjänsteleverantören avses därefter utifrån mottagna uppgifter om bolaget kunna sortera fram de uppgifter som rör den individ som legitimerat sig i e-tjänsten och att utifrån dem bedöma om denne är behörig att företräda aktuellt bolag.

Visserligen tillhandahåller verket också bevis om funktioner som tar sin utgångspunkt i en viss individ och visar vilka uppdrag denne har i olika företag eller föreningar. Dessa bevis utvisar emellertid inte i vilken mån individen är behörig firmatecknare i dessa företag och föreningar.

Mottagarens hantering

Den som beställt och mottagit XML-paket för behörighetskontroller måste emellertid sortera och tolka informationen. Eftersom XML-paketen tar sin utgångspunkt i företaget – inte i den individ som besöker en e-tjänst – blir informationen omfattande. Samtliga uppgifter om firmateckningsrätt finns med och en mängd andra uppgifter.

Materialet har visserligen försetts med koder, avsedda att förenkla en automatisering, men komplexiteten blir betydande och det behövs juridisk kompetens för att kravställa funktioner för kontroller. Det har visat sig svårt för E-tjänsteleverantörer att *sortera* sådan omfattande information och att göra de tolkningar och det utvecklingsarbete som krävs för att införa en automatiserad kontrollrutin i en e-tjänst.

Bolagsverket ska leverera utdrag – inte tolka innehållet

Till bakgrunden vid Bolagsverkets utveckling av dessa lösningar hör att verket inom ramen för sin servicefunktion endast ska lämna uppgifter ur registret – registerutdrag. Bolagsverket ska naturligtvis inte göra tolkningar av innehållet åt förlitande parter. E-tjänsteleverantörerna ska alltså själva granska och juridiskt bedöma om

den som använder e-tjänsten är behörig – alternativt välja att ta en viss risk.

I praktiken synes denna närmast självklara utgångspunkt emellertid ha lett till en alltför begränsad syn på vad som är ett registerutdrag till skillnad från en tolkning av registrets innehåll. Av regleringen i lag och förordning framgår nämligen endast följande. Enligt 8 kap. 43 § första stycket 3 ABL ska varje aktiebolag för registrering anmäla av vilka och hur bolagets firma tecknas. I paragrafens andra stycke sägs att anmälan ska innehålla uppgift om bl.a. postadress för de personer som anges i första stycket 3 och de angivna personernas personnummer. På liknande sätt föreskrivs i 1 kap. 3 § aktiebolagsförordningen (2005:559; ABF) att en anmälan för registrering enligt 2 kap. 22 § ABL ska innehålla uppgift om hur bolagets firma tecknas. I 2 kap. 14 § ABF sägs vidare att de uppgifter som avses i 8 kap. 43 § ABL ska antecknas när ett aktiebolag registreras. Cirkeln är därmed sluten och det finns inte några myndighetsföreskrifter på området

Kraven i författning på registreringens utformning går alltså inte längre än att det ska noteras ”av vilka och hur bolagets firma tecknas”. Dessa uppgifter registreras i maskinläsbar form. Varje presentation för vanlig läsning av en människa kräver alltså omvandling av digitala data till text på t.ex. papper eller bildskärm. Redan detta innefattar en tolkning från ett maskinspråk till ett uppfattbart språk. Dessutom görs vissa urval redan idag genom att fullständiga registerutdrag är ovanliga och att de begränsade utdragen innefattar viss sortering.

Även om det inte finns någon knivskarp gräns för samtliga fall mellan vad som utgör en juridisk tolkning av registrets innehåll, till skillnad från ett rent utdrag som begränsats till en delmängd av uppgifter, bör avgränsningar kunna ske så att även en träffsäkert begränsad mängd uppgifter ur t.ex. aktiebolagsregistret kan betraktas som utdrag ur registret; inte en juridisk tolkning.

1.7.3 Automatiserade tolkningar

Begränsade, kodade uppgifter i förfinade registerutdrag

Det har visat sig komplicerat för E-tjänsteleverantörer att tolka komplex information från Bolagsverket, särskilt när den ska användas automatiserat. Genom dessa utdrag överförs som fram-

gått betydligt mer information än E-tjänsteleverantören behöver. Informationen måste därför sorteras och tolkas. Den förlitande parten (E-tjänsteleverantören) har själv haft att sortera fram de uppgifter som behövs och har dessutom haft att utveckla ett automatiserat stöd för kontroller. Hittills synes endast Skatteverket ha infört en teknisk lösning för kontroller där det automatiserat bedöms om en person är behörig att företa en viss rättshandling. Dessutom är denna funktion begränsad till att ange om en person är behörig att ensam teckna firman.

Bolagsverket har därför inlett ett utvecklingsarbete för att förenkla hanteringen. Tanken är att Bolagsverket ska kunna lämna förfinade registerutdrag ur t.ex. aktiebolagsregistret, med endast *delmängder* av de uppgifter som idag lämnas i XML-paket. Utvecklingsarbetet är knutet till utredningens förslag om att införa en Infrastruktur för identifiering, där Identitetsintyg ska kunna kompletteras med Attributsintyg som tar sin *utgångspunkt i en individ* som t.ex. loggar in i en e-tjänst.

Från Bolagsverkets utgångspunkter blir frågan hur förfinade utdrag ska kunna utformas så att de endast blir att anse som registerutdrag – inte som juridiska tolkningar åt förlitande parter av om en viss individ är behörig företrädare för en juridisk person. Sådana intyg avses underlätta och förbättra verkets servicefunktion genom att E-tjänsteleverantörer enkelt, säkert och automatiserat ska kunna begära och få ut registrerade uppgifter samt utföra erforderliga kontroller. För E-tjänsteleverantörerna blir frågan istället hur de ska kunna hantera intyg för automatiserade bedömningar av juridisk behörighet.

Till nämndens uppgifter hör att skapa enighet och samordning mellan dessa aktörer inom ramen för en balanserad lösning. För att en sådan samordning ska kunna etableras måste, som ett första steg, ett förslag till en praktisk lösning tas fram. Här har Bolagsverket redan gjort ett omfattande arbete för att införa koder i sina register, bl.a. i Aktiebolagsregistret. Dessa koder finns redan med i de registerutdrag som lämnas i form av XML-paket. Tanken har varit att E-tjänsteleverantörer ska kunna programmera sina e-tjänster att godta de Användare som har kod(er) som visar att de är behöriga firmatecknare. Redan i denna del har emellertid vissa frågor aktualiserats. Koden ”FAVE” (= firman tecknas ensam av) kan enkelt förstås när den knyts till ett *personnummer* och en automatiserad tolkning av detta kan enkelt programmeras. När koden knyts till ”le” (=ledamöter) måste emellertid den automatiserade

granskningen kopplas till de fält där bolagets ledamöter anges. Eftersom ett utdrag ur Aktiebolagsregistret utgör en ögonblicksbild av registrets innehåll, även vid användning av XML-paket, kan det knappast hävdas att en angivelse av FAVE och le skulle utgöra ett registerutdrag, medan en användning av FAVE-koden så att den knyts till personnumret för varje ledamot som har ensam firmateckningsrätt skulle utgöra en tolkning. Uppgifterna kan inte missförstås utan utgör endast två olika språkliga sätt att säga samma sak.

Dessa exempel tydliggör den typ av frågor som behöver lösas.

Frågor för att få förfinade registerutdrag

När Bolagsverket funnit lämpliga lösningar rörande innehållet i förfinade registerutdrag behöver det klarläggas hur den standardiserade lösningen (SAML) ska kunna användas för att ställa frågor om juridisk behörighet. Denna standard används vanligtvis för att få svar rörande egenskaper som avser ett enda subjekt. En preliminär genomgång har emellertid visat att de avgränsningar som krävs till visst företag – är x firmatecknare i bolaget y – bör kunna ske genom att frågan innehåller t.ex. individens personnummer och företagets organisationsnummer.

Det behöver härvid genomlysas hur olika strukturer av svar ska kunna lämnas i Attributsintyg så att kontroller kan göras automatiskt i e-tjänsten. Även här aktualiseras frågor om roller. Lösningarna ska utformas så att E-tjänsteleverantörer eller andra inte kan få uppfattningen att Bolagsverket eller E-legitimationsnämnden utför juridiska tolkningar åt E-tjänsteleverantörer. Bolagsverket ska inte göra någon bedömning av en individs rätt att företa en viss rättshandling utan endast, genom den Infrastruktur för identifiering som E-legitimationen avses svara för, lämna svar elektroniskt med ett registerutdrag som avgränsats till uppgifter om den individ som agerat.

Stöd för automatiserade kontroller

För att en sådan lösning ska kunna få spridning behövs också funktioner för att E-tjänsteleverantörer ska kunna ta emot och tolka informationen. Denna samordning bör kunna ske inom

ramen för E-legitimationens uppdrag enligt myndighetens instruktion – att utveckla specifikationer och liknande krav som ska vara gemensamma för myndigheter under regeringen i deras användning av e-legitimationer.

Till denna användning hör inte bara e-legitimationerna utan även de Identitets- och Attributsintyg som behövs för att infrastrukturen ska fungera. I praktiken behöver någon programvara eller tjänst utvecklas, så att varje E-tjänsteleverantör enkelt kan automatisera kontroller av juridisk behörighet med stöd av Attributsintyg från Bolagsverket. Detta stöd bör kunna utvecklas i samverkan mellan Bolagsverket, E-legitimationsnämnden, Tillväxtverket, Skatteverket och Försäkringskassan m.fl. myndigheter som kommit långt i införandet av E-tjänster. Motsvarande lösningar bör i annan ordning tas fram för privat sektor.

Regleringen

Utvecklingstakten är hög. Det kan därför med kort varsel behövas anpassningar till nya behov eller risker. Till detta kommer att detaljeringsgraden kan bli hög. Regler i lag eller förordning är därför knappast ett lämpligt styrmedel. En reglering genom myndighetsföreskrifter kan däremot visa sig önskvärd, särskilt som avtal i många fall inte kan ingås mellan berörda aktörer eftersom de utgör en del av samma juridiska person (myndigheter under regeringen). En naturlig utgångspunkt för en fördelning av regelområdet finns också genom att

- Bolagsverket meddelar föreskrifter om vilka uppgifter som lämnas i förfinade registerutdrag och hur dessa uppgifter används (så att verket inte anses ha gjort tolkningar för annan), och
- E-legitimationsnämnden meddelar föreskrifter om Attributsintyg och deras funktioner och användning inom Infrastrukturen för Svensk e-legitimation.

En sådan normgivningskompetens för E-legitimationsnämnden ges enligt 40 § förslag till förordning om infrastrukturen för Svensk e-legitimation.

1.8 Kommuner

Samma användning i kommuners e-tjänster

Den beskrivna lösningen för *juridiska* behörighetskontroller har tagits fram med tanke främst på statliga myndigheter som behöver kontrollera om en fysisk person som uppger sig företräda en juridisk person är behörig att företräda denne, t.ex. ett aktiebolag eller någon annan organisation för vilken ett register förs enligt författning där uppgifter finns om firmatecknare.

Samma lösning bör fungera för kommuner som tillhandahåller sådana e-tjänster där användares juridiska behörighet att företräda en viss juridisk person måste kontrolleras. Här kan de kommunala myndigheternas behov av kontroll vara desamma som för statliga myndigheter – i den mån en fullständig behörighetskontroll verkligen behövs vid användning av den aktuella e-tjänsten.

Till detta kommer de samordnade lösningar som avses skapas för att även små myndigheter smidig ska kunna integrera, använda och administrera funktioner för Identitets- och Attributsintyg. Detta stöd kan antas bli betydelsefullt även inom kommunal sektor.

Publika register finns inte över behöriga handläggare

Kommunernas användning av registreringsbevis från Bolagsverket för att kontrollera juridisk behörighet att företräda t.ex. aktiebolag får emellertid inte förväxlas med kontroller av om en person är behörig handläggare hos *en myndighet* så att kontakter med en annan myndighet – t.ex. användning av en annan myndighets e-tjänst – sker behörigen. Skulle en sådan tjänst, för att kommunicera mellan myndigheter, anses kräva en fullständig kontroll av att den person som utger sig för att agera för en annan myndighets räkning verkligen är behörig att handlägga ärendet, kan den ovan beskrivna lösningen inte användas. Detta beror inte på att den tekniska lösningen skulle sakna tillräckliga funktioner utan på att det inte finns några *författningsreglerade register* över vilka handläggare vid kommuner eller andra myndigheter som är behöriga att handlägga en fråga. Det pågår emellertid ett arbete för att skapa sådana register och kataloger internt hos flera kommuner, där det tydligt och uppdaterat ska framgå vilka som är behöriga att handlägga olika kategorier av ärenden.

E-legitimationsnämnden bör i sitt fortsatta arbete agera för att myndigheter ska strukturera sina delegationsordningar m.m. på visst sätt och tillhandahålla dessa uppgifter elektroniskt så att det framgår vilka som är behöriga handläggare av olika kategorier av ärenden. Det är emellertid viktigt att hålla isär dessa behov av kontroller från de juridiska behörighetskontroller för vilka t.ex. Bolagsverket tillhandahåller registerutdrag.

1.9 Landsting

Landsting kan också tillhandahålla e-tjänster för företag och behöva kontrollera att den som loggar in är juridiskt behörig att agera för företagets, t.ex. ett aktiebolags räkning. Även här bör lösningen med Attributsintyg från Bolagsverket passa, förutsatt att landstingen kan godta den tekniska hanteringen inom den nationella Infrastrukturen för identifiering. I denna del torde det i praktiken kunna bli enkelt eftersom källan till den efterfrågade informationen finns på *ett enda ställe* för hela riket – hos Bolagsverket – och att den grundläggande hanteringen av dessa uppgifter är *reglerad* i lag och förordning utifrån syftet att sprida uppgifterna (s.k. publicitetsregister).

Inom kommunala och landstingskommunala myndigheter finns däremot som framgått inga lagreglerade publicitetsregister över vilka anställda och uppdragstagare som har olika behörigheter. På det område som regleras av patientdatalagen behövs uppgifter från olika register. Dessa register är inte publika och det finns inte någon sådan reglering av registerinnehåll och ansvar gentemot andra för registeruppgifter som vid användning av t.ex. aktiebolagsregistret eller fastighetsregistret.

Regleringen i patientdatalagen leder dessutom till blandade krav på dels *åtkomstkontroll* inom respektive mellan myndigheter och andra organ, dels en slags juridisk *behörighetskontroll* inom och mellan olika organ när åtgärder får vidtas endast av personer som har vissa roller. Det är nödvändigt att beakta dessa skillnader i reglering och hantering av *juridiska behörighetskontroller* av det slag som Bolagsverket avses stödja genom registerutdrag i form av Attributsintyg, respektive *blandade kontroller* enligt patientdatalagen av åtkomst och behörighet, inom respektive mellan myndigheter.

För hanteringen av Attributsintyg gäller olika juridiska förutsättningar vid behörighetskontroller med stöd av ett elektroniskt registerutdrag (Attributsintyg) från Bolagsverket och motsvarande intyg som lämnas inom det område som regleras av patientdatalagen. På det senare området tillkommer de roller och egenskaper inom ett organ, t.ex. ett landsting, som ska kunna kontrolleras enligt reglerna om inre sekretess och de register över ”behörigheter” som ska finnas och administreras hos varje vårdgivare.

1.10 En samordning kräver fortsatta analyser

De berörda särskilda reglerna för hälso- och sjukvårdsområdet och den hantering av attribut som krävs där får inte sammanblandas med generella kontroller av juridisk behörighet. Det är också viktigt att skilja frågan om vilka e-legitimationer ska få användas som Svensk e-legitimation från frågor om vilka attribut och Attributsutfärdare som ska finnas inom ramen för den Infrastruktur för identifiering (vilken även ska innefatta attributshantering) som E-legitimationsnämnden ska etablera. Exempelvis bör de e-tjänstelegitimationer som landstingen och flera kommuner infört och som uppfyller de högt ställda krav på identifiering kunna användas inom hela Infrastrukturen för Svensk e-legitimation medan all attributshantering för vilken sådana e-tjänstelegitimationer används kanske inte hör hemma inom den infrastruktur som E-legitimationsnämnden etablerar. En sortering behöver därför göras av vad som ska ingå i den Infrastruktur för identifiering som E-legitimationsnämnden enligt sin instruktion har att etablera och vad som bör utformas som särlösningar för t.ex. hälso- och sjukvårdsområdet.

Detta innebär naturligtvis inte att E-legitimationsnämnden ska bortse från behoven inom kommuner och landsting. Dessa behov bör så långt möjligt tillgodoses genom samordnade lösningar. Däremot bör lösningar som tillgodoser speciella krav, t.ex. inom hälso- och sjukvården, och som skulle föra med sig hinder eller begränsningar om de genomförs generellt, inte införas på områden där de inte behövs.

Genom att i det fortsatta arbetet närmare klargöra dessa skillnader och hur de bör hanteras kan sammanblandningar och missförstånd undvikas. Samtidigt kan de lösningar som E-legitima-

tionsnämnden respektive landstingen utvecklar tydligt avgränsas så att kravställning och samordning kan förenklas. En fråga i detta sammanhang är om det kan vara så att brister i samsyn som framträtt i det tekniska utvecklingsarbetet inte längre gör sig gällande om sammanblandningar med särlösningar för enskilda områden kan undgås. Här bör nämnas hur de förslag som utredningen tagit fram innebär att Användaren först legitimerar sig och att ett Identitetsintyg lämnas till E-tjänsteleverantören, som därefter beställer och får ett Attributsintyg från t.ex. Bolagsverket, medan det förslag som diskuterats inom hälso- och sjukvårdsområdet går ut på att i ett och samma intyg lämna uppgifter om såväl identitet som attribut, efter att Användaren legitimerat sig och systemet för utfärdande av intyg hämtat attribut från tillgängliga kataloger.

Det bör således genomlysas om skillnader i teknisk och administrativ syn på hur standarden (SAML) ska användas kan överbryggas när skilda förutsättningarna på dessa områden har klargjorts och beaktats. Den komplexa hanteringen av en mängd kataloger inom hälso- och sjukvårdsområdet och de särskilda kraven på tilldelade finmaskiga behörigheter för intern och extern åtkomst saknar motsvarighet vid de juridiska behörighetskontroller som görs med stöd av uppgifter ur t.ex. aktiebolagsregistret. Till detta kommer att attribut inom hälso- och sjukvårdsområdet styrs även utifrån användares angivelser av i vilken egenskap (uppdrag) de agerar i det enskilda fallet. Samma person kan ha flera uppdrag inom hälso- och sjukvården, vilket normalt inte blir fallet vid grovmaskiga juridiska behörighetskontroller där individen antingen är firmatecknare/fullmäktig eller saknar behörighet.

Härvid får sammanblandningar inte ske med kraven på t.ex. e-tjänstelegitimationer. Den Infrastruktur för Svensk e-legitimation som E-legitimationsnämnden ska införa bör harmoniera med existerande lösningar inom såväl hälso- och sjukvårdsområdets som andra kommunala redan existerande federationslösningar. Här kan olika tekniska och administrativa lösningar diskuteras för att säkerställa samverkande lösningar. En pusselbit för att åstadkomma en sådan samordning skulle kunna vara en genomtänkt anvisningstjänst som ger stöd även för användares val av uppdrag eller roll. En sådan angivelse skulle kunna läggas till grund för val av olika attributskällor, vilket blir intressant vid legitimering med bl.a. e-tjänstelegitimationer. I fall där en e-tjänst kräver intyg, som utöver identitet även behöver ange vilka rättigheter Användaren har i den

aktuella e-tjänsten, kan en på så sätt vidareutvecklad anvisningstjänst möjlige underlätta för fall där det redan finns attributskällor etablerade, t.ex. inom vård och omsorg. Dessa frågor behöver emellertid genomlysas närmare.

Genom att uppmärksamma och genomlysa dessa skillnader mellan rättsfrågor som har sin grund i patientdatalagens (finmaskiga) särreglering respektive generella regler om kontroller av en (grovmaskig) rätt att teckna en juridisk persons firma och tekniska val som görs för att tillgodose patientdatalagens särreglering respektive kontroller av juridisk behörighet, bör det alltså bli möjligt att finna en samsyn även kring tekniska frågor. Samtidigt bör missförstånd kunna undvikas.

Tillitsramverk

1 Tillitsramverk för e-legitimering 240

1.1 Svensk E-legitimation 241

1.2 Internationell samverkan 243

1.3 Tillitsnivåer 243
1.3.1 Nivå 1 (AL1) 244
1.3.2 Nivå 2 (AL2) 244
1.3.3 Nivå 3 (AL3) 245
1.3.4 Nivå 4 (AL4) 245

2 Kriterier för utfärdande av Svensk e-legitimation 247

2.1 Organisation och styrning 247

2.2 Information om villkor 247

2.3 Identifiering och registrering 248
2.3.1 Fastställande av sökandens identitet 249
2.3.2 Utfärdande av e-legitimation 250
2.3.3 Utformning av tekniska hjälpmedel 250

2.4 Operationella krav 251

2.5 Fysisk, administrativ och personorienterad säkerhet 253

2.6 Teknisk säkerhet 254

1 Tillitsramverk för e-legitimering

Detta tillitsramverk avses utgöra en central del i det regelverk som ska vara styrande för Infrastrukturen för identifiering. Utredningens arbete har emellertid inte nått så långt att det i alla delar kunnat bestämmas hur regelhierarkin ska se ut och på vilka nivåer i denna hierarki som närmare regler och krav ska finnas. I denna bilaga ges därför en första sammanställning och anpassning av de krav som kan ställas på utfärdare av Svensk e-legitimation. Infrastrukturen för identifiering bör ta sin utgångspunkt i ett tillitsramverk byggt på internationell standard och medge den flexibilitet som den föreslagna Infrastrukturen för Svensk e-legitimation och internationell samverkan kräver. Det måste emellertid säkerställas att dessa standarder är tillämpbara på och förenliga med svenska förhållanden.

Bilagan bör läsas som en vägledning inför en anpassning av Svensk e-legitimation till internationell standard, och de mer konkreta och detaljerade krav som en sådan anpassning kan komma att kräva.

För att konkretisera den diskussion som måste föras om ett tillitsramverks närmare utformning, har detta första utkast till en sammanfattning av de krav som kan förväntas ställas på Svensk e-legitimation tagits fram. Utkastet bör läsas som en vägledning inför en anpassning av Svensk e-legitimation till internationell standard, och de mer konkreta och detaljerade krav som en sådan anpassning kan komma att kräva.

De flesta av de internationella ansträngningar som gjorts för att definiera nivåer av tillit vid användning av e-legitimationer har sin grund i en publikation (SP 800-63) från det amerikanska National Institute of Standards and Technology (NIST). De riktlinjer som beskrivs där är emellertid relativt allmänt hållna. Fördjupande arbeten har därför bedrivits inom bl.a. Europeiska unionen, där det storskaliga s.k. STORK-projektet utgjort en viktig del[1].

[1] EU-kommissionen har tagit fram en handlingsplan som ska underlätta för medlemsstaterna att införa ömsesidigt godkända och kompatibla system för e-signaturer och e-legitimationer i syfte att göra det lättare att tillhandahålla elektroniska offentliga tjänster över gränserna [KOM(2008) 798]. Arbetet för ömsesidigt erkännande av elektronisk identifiering inom EU genomförs inom STORK-projektet.

Ett betydelsefullt arbete för att utarbeta ett internationellt tillitsramverk bedrivs nu också inom International Organization for Standardization och International Electrotechnical Commission (ISO/IEC). Det kommande resultatet av detta arbete, ISO/IEC 29115, som förväntas bli internationell norm på området, bygger på dokument som publicerats inom det s.k. Kantara Initiative Identity Assurance Framework (Kantara IAF).

Under förutsättning att det fortsatta arbetet inom ISO/IEC leder till resultat som är förenliga med behoven inom den föreslagna Infrastrukturen för identifiering bör Sverige följa denna internationella standard. E-legitimationsnämnden bör därför, liksom E-delegationen, verka för att resultatet av standardiseringsarbetet blir förenligt med svenska intressen på området.

I avvaktan på detta resultat bör ett tillitsramverk införas som har sin förankring i de tidigare nämnda publikationerna. De har alla gemensamt att de definierar fyra tillitsnivåer (AL)[2] för e-legitimering, i syfte att möta olika nivåer av risk och olika krav på användbarhet. Dessa tillitsnivåer svarar mot olika grader av teknisk och operationell säkerhet hos utfärdaren och olika grader av kontroll av att en person som tilldelas en elektronisk identitet verkligen är den han eller hon utger sig för att vara.

Något förenklat kan tillitsnivåerna beskrivas som en måttstock, där en lägre indikering på skalan motsvarar enklare användning och utgivning, lägre kostnader, men också en lägre skyddsnivå. Högre klassificering medför högre kostnader för såväl utgivande som användande, men leder till att en högre grad av tillit kan fästas vid identifieringen.

1.1 Svensk e-legitimation

Vid en tillämpning av dessa internationella normer har det, såvitt hittills framkommit, visat sig ändamålsenligt att för Svensk e-legitimation kräva en tillitsnivå som motsvarar nivå 3 (AL3) eller högre. Detta innebär att utgivare av Svensk e-legitimation ska ha dokumenterade och fungerande ledningssystem för informationssäkerhet i enlighet med erkända standarder, att innehavares identiteter verifieras på ett ändamålsenligt sätt, att metoden för

[2] AL är en förkortning av den internationella termen för tillitsnivå, ”Assurance Level”, som används såväl i Kantara IAF som i STORK-projektet.

legitimering baseras på starka kryptografiska mekanismer och utgivaren ska kunna påvisa att de når upp till och efterlever kraven enligt AL3.

Tillitsnivå 3 är också den nivå som ligger närmast de av ramavtalsleverantörerna idag utgivna e-legitimationerna. Den öppnar emellertid även nya typer av e-legitimationer som inte är certifikatbaserade. Detta förväntas kunna leda till en högre användbarhet och större spridning inom fler samhällsgrupper. Om det visar sig att en betydande del av de redan utgivna e-legitimationerna inte uppfyller kraven för nivå 3 i tillitsramverket kan det komma att bli nödvändigt att etablera övergångsregler så att dessa kan godtas inom infrastrukturen för Svensk e-legitimation till dess att en anpassning skett. Kvalificerade certifikat utgivna i enlighet med lagen (2000:832) om kvalificerade elektroniska signaturer kan, bland annat beroende på metod för utgivning, komma att uppfylla kraven för nivå 2, 3 eller 4, och därmed också användas inom infrastrukturen för Svensk e-legitimation. Då kraven i tillitsramverket är väsentligt mer specifikt framställda än de som återfinns i 4 kap. signaturlagen, följer att kvalificerade certifikat inte med automatik uppfyller någon tillitsnivå högre än 2.

En förutsättning för att en Svensk e-legitimation ska få utfärdas föreslås dessutom vara att användaren har svenskt person- eller samordningsnummer. En e-tjänsteleverantör kan därför, när Svensk e-legitimation använts, veta att det finns möjlighet att få sådan information, i ett identitetsintyg eller efter en manuell förfrågan om en sådan påkallas från persondataskyddssynpunkt. Dessa krav införs liksom regleringen i övrigt genom avtal mellan E-legitimationsnämnden och utfärdare för anslutning till Infrastrukturen för Svensk e-legitimation, i den mån detta inte följer av författningsreglering.

E-legitimationsnämnden ska utöva tillsyn över utfärdare av Svensk e-legitimation så att tillgänglighet, kvalitet och informationssäkerhet blir säkerställda i enlighet med ett regelverk för Infrastrukturen för Svensk e-legitimation. I enlighet med regelverket ska nämnden också kunna ingripa mot missförhållanden – ytterst avveckla en utfärdare om omständigheterna är sådana att de riskerar att leda till oacceptabla konsekvenser för användare, e-tjänsteleverantörer eller andra, eller i stort rubba förtroendet för Infrastrukturen för Svensk e-legitimation.

1.2 Internationell samverkan

Vid samverkan över nationsgränserna kan andra länders E-legitimationer översättas till AL1 eller AL2 i tillitsramverket. Om en utländsk E-legitimation erhållit klassificering enligt STORK-projektets modell, kan Nivå 2 eller högre översättas till AL2. Vid de fall det råder tveksamhet under vilka premisser en utländsk E-legitimation utfärdas, ska dessa istället översättas till AL1.

1.3 Tillitsnivåer

Fyra tillitsnivåer (AL1—AL4) definieras. Nivåerna indikerar hur stor tilltro man bör fästa vid en elektronisk identitet, och beskrivs enligt nedanstående skala:

AL1: ingen eller liten tilltro till identiteten
AL2: viss tilltro till identiteten
AL3: hög tilltro till identiteten
AL4: mycket hög tilltro till identiteten

För att kunna fastställa lägsta acceptabla tillitsnivå för en e-tjänst, bör de risker och konsekvenser som en felaktig identifiering kan medföra inom följande områden beaktas:

- Obehag, oro eller ryktesskada
- Finansiell skada
- Skada för myndighetens rykte
- Civilt- eller straffrättsligt brott
- Personsäkerhet

För höga krav på identifieringen kan medföra högre kostnader för e-tjänsten, men också resultera i mindre flexibilitet och användbarhet för användaren. Den högre kostnaden för identifiering uppstår på grund av att det vanligen är dyrare att utfärda och underhålla en identitet med en högre tillitsnivå än en med en lägre. Den minskade flexibiliteten för användaren visar sig t.ex. genom att användaren enbart kan använda viss utrustning eller viss programvara för att nå e-tjänsten, eller att identiteten i praktiken enbart kan utfärdas till och användas av vissa kategorier av befolkningen.

Som grundregel bör därför en e-tjänst kräva en lägsta tillitsnivå som står i proportion till de identifierade riskerna enligt ovan.

1.3.1 Nivå 1 (AL1)

På Tillitsnivå 1 finns ingen eller liten tilltro till angiven identitet. Användning av denna nivå är lämplig när resultat av en felaktig identifiering endast förväntas leda till marginella negativa konsekvenser, samtidigt som identifieringsmetoden ger viss tillit och underlättar för användaren och/eller e-tjänsten.

Felaktig identifiering i en e-tjänst som kräver denna nivå kan t.ex. innebära:

- små monetära förluster
- liten skada på rykte

Exempel: Uppgiftslämnande via en e-tjänst kan använda sig av AL1 i de fall när information endast flödar från individen till e-tjänsten, inga känsliga uppgifter delges uppgiftslämnaren och inga av de övriga kraven för högre tillitsnivåer blir tillämpliga.

Ett flertal olika tekniker för identifiering kan användas, t.ex. lösenord eller PIN-kod. Denna nivå kräver inte heller starkt kryptografiskt skydd av identiteten.

1.3.2 Nivå 2 (AL2)

På Tillitsnivå 2 finns viss tilltro till angiven identitet. Användning av denna nivå är lämplig när man kan se vissa negativa konsekvenser som resultat av en felaktig identifieringen.

Användning av starkt lösenord över öppet nätverk är en acceptabel identifieringsmekanism på denna nivå. AL2 kräver skydd mot avlyssning, återuppspelning och gissning av lösenord.

Fastställandet av sökandens identitet kan ske utan traditionell legitimering vid personligt besök, och istället baseras på metoder liknande de för utgivning av kreditkort.

Felaktig identifiering i en e-tjänst som kräver denna nivå kan t.ex. innebära:

- medelhöga monetära förluster

- att delvis känslig information kommer i orätta händer
- viss skada på rykte

Exempel: E-tjänster som tar emot och lämnar ut delvis känslig information, men där uppgifterna i sig kan verifieras eller inhämtas på annat sätt, kan använda sig av AL2 förutsatt att inga av de övriga kraven för högre tillitsnivåer blir tillämpliga.

1.3.3 Nivå 3 (AL3)

På tillitsnivå 3 finns hög tilltro till angiven identitet. Användning av denna nivå är lämplig när man kan se substantiella konsekvenser som resultat av en felaktig identifiering.

Denna nivå kräver flerfaktorsidentifiering som styrker både kännedom om personlig kod samt kontroll över e-legitimationshandling som baserats på starka kryptografiska mekanismer. Både mjuka och hårda e-legitimationshandlingar är tillåtna, inklusive metoder för att framställa engångslösenord.

Kraven på kontroll av den ursprungliga identifieringen är starkare än på AL2, och kräver att användaren legitimerat sig vid ett personligt besök hos utfärdaren eller utfärdarens ombud.

Felaktig identifiering i en e-tjänst som kräver denna nivå kan t.ex. innebära:

- viss skada på allmänna intressen
- substantiella monetära förluster
- att känslig information kommer i orätta händer
- substantiell skada på rykte

Exempel: Inhämtande och utlämnande av känsliga uppgifter som traditionellt kräver identifiering med godkänd fotolegitimation, kan använda sig av AL3.

1.3.4 Nivå 4 (AL4)

På tillitsnivå 4 finns mycket hög tilltro till angiven identitet. Användning av denna nivå är lämplig när man kan se mycket stora konsekvenser som resultat av en felaktig identifiering.

Denna nivå kräver starkast möjliga identifieringsmekanismer, och måste baseras på kryptografiska metoder som bevisar tillgång till nyckelmaterial lagrat i hårda bärare under innehavarens direkta kontroll.

Hög kryptografisk och fysisk säkerhet krävs för samtliga ingående komponenter som hanterar nyckelmaterial. All data-överföring måste skyddas och skyddet måste vara kryptografiskt kopplat till det nyckelmaterial som används vid identifieringen.

Felaktig identifiering i en e-tjänst som kräver denna nivå kan t.ex. innebära:

- hög fara för annans liv
- stor skada på allmänna intressen
- stora monetära förluster (> 10 M EUR)
- att mycket känslig information kommer i orätta händer
- stor skada på rykte

2 Kriterier för utfärdande av Svensk e-legitimation

2.1 Organisation och styrning

1.1 Utfärdare av Svensk e-legitimation ska drivas som ett registrerat svenskt aktiebolag eller motsvarande utländska företag inom Europeiska ekonomiska samarbetsområdet.

1.2 Utfärdare ska ha en etablerad verksamhet, vara fullt operationell i alla delar som berörs i detta dokument, och vara väl insatt i de regulatoriska, avtalsmässiga och juridiska krav som ställs på denne som utfärdare av Svensk e-legitimation.

1.3 Utfärdare ska förfoga över tillräckliga ekonomiska medel för att kunna bedriva verksamheten i minst 1 år och bära risken för skadeståndsskyldighet.

2.2 Information om villkor

2.1 Utfärdaren ska tillhandahålla uppgifter om avtal, villkor samt anknytande uppgifter och eventuella begränsningar i användandet av tjänsten till anslutna användare, arbets- och uppdragsgivare, e-tjänsteleverantörer och andra som kan komma att förlita sig på utfärdarens tjänst.

2.2 En utfärdare som vill införa villkor som inte finns med i ansökningshandlingen ska tydligt hänvisa till villkoren och utforma rutinerna så att villkoren kommer sökanden tillhanda innan denne undertecknar eller annars ingår avtal med utfärdaren.

2.3 Utfärdaren ska tillhandahålla en utfärdardeklaration som bl.a. innefattar:

a) bolagets identitet och kontaktuppgifter,

b) ägarstruktur och vilka principer för bolagsstyrning som tillämpas,

c) villkor förknippade med den tillhandahållna tjänsten (inklusive metod för utgivning, spärr och avveckling),

d) metod att ändra villkoren för den tillhandahållna tjänsten,

e) utfärdarens skyldigheter, utfästa garantier, utlovad tillgänglighet och finansiellt ansvar,

f) användarens skyldigheter att skydda sin elektroniska identitet,

g) information om insamling, registrering, lagring, bearbetning, och spridning eller samkörning av personuppgifter, och i vilken mån detta sker.

2.4 Utfärdare av Svensk e-legitimation ska inhämta användarens samtycke vid nyteckning eller ändring av tjänsten, samt regelbundet var 5:e år.

2.5 Utfärdare av Svensk e-legitimation ska tillhandahålla en tjänst där användaren kan ändra tilläggsinformation knuten till den elektroniska identiteten (t.ex. e-postadress) samt spärra sin e-legitimation (spärrtjänst). Tjänsten ska ha god tillgänglighet och utfärdaren ska behandla anmälan om spärr skyndsamt.

2.6 Den arbets- eller uppdragsgivare som ansöker om en Svensk e-legitimation knuten till organisationstillhörighet (e-tjänste-legitimation)

a) får bestämma hur e-tjänstelegitimationen får användas, t.ex. om den får användas även utanför tjänsten, och

b) får spärra e-legitimationen.

2.3 Identifiering och registrering

3.1 Utfärdare ska, beaktat reglerna för persondataskydd, föra register över anslutna användare och de tilldelade elektroniska identitetshandlingarna, och hålla detta register aktuellt.

3.2 Svensk e-legitimation får utfärdas endast efter skriftlig ansökan i traditionell form. Ansökan ska vara undertecknad på traditionellt sätt, med intyg om att lämnade uppgifter är riktiga och fullständiga.

3.3 Om en sökande redan har identifierats vid ett personligt besök (i enlighet med 3.8) för ekonomiskt eller rättsligt betydelsefulla mellanhavanden, och sökanden kan identifieras på annat tillförlitligt sätt som är likvärdigt med kraven för Svensk e-legitimation, får utfärdaren identifiera och ta emot ansökan genom denna tjänst i stället för enligt 3.2.

3.4 En ansökan om Svensk e-legitimation ska innehålla personnummer eller samordningsnummer, samt de uppgifter som i övrigt är nödvändiga för att identitetsutfärdaren ska kunna tillhandahålla sådan e-legitimation och utfärda identitetsintyg.

3.5 En Svensk e-legitimation knuten till organisationstillhörighet (e-tjänstelegitimation) får utfärdas endast efter skriftlig ansökan i traditionell form av en arbets- eller uppdragsgivare. Ansökan ska vara undertecknad på traditionellt sätt av arbets- eller uppdragsgivaren. Om denne är en juridisk person ska ansökan vara undertecknad av en behörig företrädare.

3.6 Om en arbets- eller uppdragsgivare eller en behörig företrädare för denne har legitimerat sig eller skrivit under med Svensk e-legitimation, eller enligt det förenklade förfarande som anges i 3.3, får en sådan underskrift eller legitimering för uppgiftslämnande ersätta ett förfarande enligt 3.5.

3.7 Utfärdare ska skyndsamt och på ett säkert sätt behandla och effektuera spärrbegäran och vidta sådana åtgärder för att förhindra missbruk av spärrtjänsten (eller andra handlingar som leder till spärr av en elektronisk identitetshandling) att användares e-legitimationer är tillgängliga när de behövs.

2.3.1 Fastställande av sökandens identitet

3.8 Utfärdare av Svensk e-legitimation ska kontrollera den sökandes identitet vid ett personligt besök, på likvärdigt sätt som vid en ansökan om en traditionell identitetshandling.

3.9 Utfärdare av en e-legitimation ska kontrollera att ansökan om e-legitimation är behörigen undertecknad på papper eller lämnad elektroniskt enligt 3.3, och att de uppgifter som den

sökande lämnat är fullständiga och stämmer överens med uppgifter som finns registrerade i ett officiellt register.

3.10 Utfärdare av en e-legitimation knuten till organisationstillhörighet (e-tjänstelegitimation) ska kontrollera att ansökan om e-legitimation är behörigen undertecknad på papper eller lämnad elektroniskt enligt 3.6, och att de uppgifter som den sökande lämnat är fullständiga och stämmer överens med uppgifter som finns registrerade i ett officiellt register.

2.3.2 Utfärdande av e-legitimation

3.11 Utfärdare av Svensk e-legitimation ska säkerställa att alla sökande tilldelas en unik elektronisk identitet och att de utfärdade elektroniska identitetshandlingarna är utformade så att de för användaren tydligt kan hänföras till den aktuella tjänsten.

3.12 Utfärdare av Svensk e-legitimation ska tillhandahålla den tilldelade elektroniska identitetshandlingen till sökanden på ett säkert sätt, och säkerställa att identitetshandlingen blir entydigt kopplad till sökandens elektroniska identitet.

3.13 En utfärdare som vid personligt besök eller via elektroniskt förfarande som är förenligt med 3.3, tillhandahåller både den elektroniska legitimationshandlingen som användaren ska inneha och personlig kod som användaren ska bruka för att aktivera e-legitimationen, ska bekräfta brevledes till sökandens folkbokföringsadress att överlämning av sådan e-legitimation skett.

3.14 Sökanden ska bekräfta att denne mottagit e-legitimationen innan den blir giltig.

2.3.3 Utformning av tekniska hjälpmedel

3.15 Tekniska hjälpmedel för identifiering genom Svensk e-legitimation ska utformas enligt sådan tvåfaktorsprincip att en del består i den elektroniska identitetshandlingen som användaren ska inneha, och en del i det som användaren ska bruka för att aktivera e-legitimationen (personlig kod).

3.16 Aktiveringsmekanismen och den personliga koden ska utformas så att det är osannolikt att en utomstående kan forcera aktiveringsskyddet, ens på maskinell väg.

3.17 Användare av Svensk e-legitimation ska på egen hand kunna byta personlig kod, och få hjälp att välja den personliga koden så att kraven i 3.16 upprätthålls.

2.3.4 Identitetsintyg

3.18 Utfärdare av Svensk e-legitimation ska tillhandahålla tjänst för utgivning av identitetsintyg till förlitande e-tjänster, enligt de tekniska specifikationer som E-legitimationsnämnden från tid till annan föreskriver. Utlämnande av identitetsintyg ska föregås av en tillförlitlig kontroll av den angivna elektroniska identiteten och den elektroniska identitetshandlingens giltighet.

3.19 Lämnade identitetsintyg ska vara giltiga endast så länge som det krävs för att användaren ska få tillgång till den efterfrågade e-tjänsten, samt skyddas så att informationen är läsbar endast för den avsedda mottagaren och att den som tar emot intyget kan kontrollera att mottagna intyg är äkta.

2.4 Operationella krav

4.1 Utfärdare ska ha ett ledningssystem för informationssäkerhet (LIS) som i tillämpliga delar baseras på ISO/IEC 27001 eller motsvarande erkända och vedertagna standarder, omfattande bl.a. organisation, resurser samt tekniska respektive administrativa säkerhetsåtgärder och utgöra en kvalitetsprocess som kontinuerligt ska utvärderas och anpassas till aktuella verksamhets- och omvärldskrav:

a) Samtliga säkerhetskritiska administrativa och tekniska processer ska dokumenteras och vila på en formell grund, där roller, ansvar och befogenheter finns tydligt definierade.

b) Utfärdare ska säkerställa att denne vid var tid har tillräckliga personella resurser till förfogande för att uppfylla sina åtaganden.

c) Utfärdare ska inrätta en process för riskhantering som på ett ändåmålsenligt sätt, kontinuerligt eller minst var sjätte månad, analyserar hot och sårbarheter i verksamheten, och som genom införande av säkerhetsåtgärder balanserar riskerna till acceptabla nivåer.
d) Utfärdare ska inrätta en process för incidenthantering som systematiskt säkerställer kvaliteten i tjänsten, former för vidarerapportering och att lämpliga reaktiva och preventiva åtgärder vidtas för att lindra eller förhindra skada vid händelser som lett till eller kunnat leda till en incident.
e) Utfärdare ska upprätta och testa en kontinuitetsplan som tillgodoser verksamhetens tillgänglighetskrav genom en förmåga att återställa kritiska processer vid händelse av katastrof eller allvarliga incidenter.

4.2 Ledningssystemet för informationssäkerhet och efterlevnaden av de krav som ställs på utfärdare av Svensk e-legitimation ska årligen vara föremål för internrevision, utförd av oberoende intern kontrollfunktion, såvida inte organisationens storlek eller annan försvarbar orsak motiverar annat.

4.3 Ledningssystemet för informationssäkerhet och efterlevnaden av de krav som ställs på utfärdare av Svensk e-legitimation ska vara föremål för extern revision minst var 24:e månad, och utföras av opartisk och självständig revisor med dokumenterad erfarenhet av IT-revisioner och kontrolltestning. Resultatet av revisionen ska redovisas i en revisionsrapport, och som på begäran ska ges in till E-legitimationsnämnden.

4.4 En utfärdare som på annan part har lagt ut utförandet av en eller flera säkerhetskritiska processer, ska genom avtal definiera vilka kritiska processer som underleverantören är ansvarig för och vilka krav som är tillämpliga på dessa, samt tydliggöra avtalsförhållandet i utfärdardeklarationen så att underleverantörens uppfyllelse av kraven för Svensk e-legitimation kan verifieras oberoende av huvudmannen.

2.5 Fysisk, administrativ och personorienterad säkerhet

5.1 Verksamhetens centrala delar ska skyddas fysiskt mot skada som följd av miljörelaterade händelser, otillåten åtkomst eller andra yttre störningar. Tillträdeskontroll ska tillämpas så att åtkomst till känsliga utrymmen är begränsad till behörig personal, att flyttbart datamedia och pappersdokument förvaras på ett säkert sätt, och att dessa utrymmen kontinuerligt övervakas för obehörigt tillträde.

5.2 Innan en person antar någon av de roller som identifierats i enlighet med 4.1a, och som är av särskild betydelse för säkerheten, ska utfärdaren ha genomfört bakgrundskontroll i syfte att förvissa sig att personen kan anses vara pålitlig samt att personen har de kvalifikationer och den utbildning som krävs för att utföra de arbetsuppgifter som följer av rollen på ett tillfredställande, korrekt och säkert sätt.

5.3 Utfärdare av Svensk e-legitimation ska bevara

a) ansökningshandlingar och handlingar som rör utlämnande, mottagande eller spärr av e-legitimationer.

b) avtal, policydokument och utfärdardeklarationer, och

c) övrig dokumentation som stöder efterlevnaden av de krav som ställs på utfärdare av Svensk e-legitimation, och som visar att de säkerhetskritiska processerna fungerar.

5.4 Tiden för bevarande ska inte understiga tio år och material ska kunna tas fram i läsbar form under hela denna tid, såvida inte krav på gallring påkallas från integritetssynpunkt och har stöd i lag eller annan författning.

5.5 En utfärdare av Svensk e-legitimation som upphör med sin verksamhet ska informera sina användare och E-legitimationsnämnden. Utfärdaren ska hålla arkiverat material tillgängligt.

2.6 Teknisk säkerhet

6.1 Utfärdare ska kunna visa att de tekniska kontroller som finns införda är tillräckliga för att uppnå den skyddsnivå som bestämts genom riskanalysen, och att dessa kontroller fungerar och är effektiva.

6.2 Kommunikation mellan systemkomponenter över allmänna telekommunikationsnät eller andra kommunikationslänkar som inte är fysiskt skyddade i enlighet med 5.1, ska begränsas och ömsesidigt identifieras med en styrka som minst motsvarar kraven för Svensk e-legitimation, samt skyddas mot insyn, manipulation och återuppspelning.

6.3 Känsligt kryptografiskt nyckelmaterial ska skyddas så att:

a) åtkomst begränsas, logiskt och fysiskt, till de roller och de tillämpningar som oundgängligen kräver det,

b) nyckelmaterialet aldrig lagras i klartext på beständigt lagringsmedia,

c) aktiveringsdata för skydd av nyckelmaterial hanteras genom flerpersonkontroll,

d) nyckelmaterialet skyddas när det inte är under användning, direkt eller indirekt, via kryptografisk hårdvarumodul med aktiva säkerhetsmekanismer mot både fysiska och logiska försök att röja nyckelmaterialet,

e) säkerhetsmekanismerna för skydd av nyckelmaterial är genomlysta och baserade på erkända och väletablerade standarder.

6.4 Utfärdaren ska kunna påvisa att tekniska säkerhetskontroller införts vid identifiering av användare och utfärdande av identitetsintyg, så att det är osannolikt att utomstående genom gissning, avlyssning, återuppspelning eller manipulation av kommunikation kan forcera skyddsmekanismerna.

6.5 Utfärdaren ska ha en dokumenterad och fungerande process for styrning och ändring av IT-system i enlighet med vedertagna principer, och som innefattar kontinuerlig omvärldsbevakning av de produkter och teknologier som används i tjänsten samt ändåmålsenlig beredskap för förändrade risknivåer.

Kvalificerade certifikat

Analys av konsekvenser om identitetsleverantörer tvingas tillhandahålla endast kvalificerade certifikat.

1 Sammanfattande slutsatser 256

2 Uteslutning av e-legitimationslösningar 256

3 Hur svårt är det att konvertera 257

4 Övergångsproblem 258

5 Säkerhetsvinster med kvalificerade certifikat 259

6 Internationell samverkan 261

7 Juridiska frågor om säkerhetsnivå 262

8 Ekonomi Affärsmodell 263

9 Realistiska alternativ 264

1 Sammanfattande slutsatser

Ett krav på att endast kvalificerade certifikat är godkända som e-legitimationer i Sverige garanterar inte en högre säkerhetsnivå än om även icke kvalificerade certifikat accepteras.

Ett krav på kvalificerade certifikat skapar stora övergångsproblem för såväl dagens utfärdare av e-legitimationer som utfärdare av tjänstelegitimationer och tvingar nuvarande e-legitimationsutfärdare att stå utanför federationen om de inte helt ändrar sin affärsmodell och avtalsstruktur.

Ett krav på kvalificerade certifikat strider mot normer som utarbetats inom EU projektet STORK om det inte kombineras med ett krav på hårda nyckelbärare (Smarta Kort).

Ett krav på kvalificerade certifikat utesluter alternativa tekniker som anses vara acceptabla inom EU projektet STORK, ex användning av koddosor och kan medföra mer långtgående krav än vad som ofta behövs i praktiken.

2 Uteslutning av e-legitimationslösningar

Ett krav på att e-legitimationer ska baseras på kvalificerade certifikat reducerar drastiskt mängden godkända e-legitimationer.

I Sverige finns bara en aktör som är registrerad som utfärdare av kvalificerade certifikat. Detta krav utesluter därför bl.a. följande övriga aktörer:

- Samtliga ramavtalsleverantörer i infratjänsten, d.v.s. e-legitimationer från BankID, Nordea, SEB, Telia, Posten och Steria. Därmed utesluts i stort sett samtliga e-legitimationer som idag accepteras av svenska myndigheter.
- Befintliga tjänstelegitimationer som ex SITHS och enskilda myndigheters e-tjänstekort (Skatteverket, Polisen m.m.)

Vidare utesluts även alternativa tekniker så som koddosor, kodkort och diverse mobiltelefonbaserade e-legitimeringslösningar som inte

är certifikatbaserade eller som av andra skäl inte knyts till ett kvalificerat certifikat.

3 Hur svårt är det att konvertera

Av lagen (2000:832) om kvalificerade elektroniska signaturer (signaturlagen) följer att kvalificerade elektroniska signaturer skapas med certifikat som ska ges ut till allmänheten (s.k. öppna system). Innebörden av detta kan sammanfattas enligt följande:

> För slutna system ska parternas avtalsfrihet respekteras i den utsträckning det är förenligt med övrig lagstiftning. Vissa svårigheter finns dock att avgöra vad som utgör slutna respektive öppna system. *Storleken på den grupp till vilken ett certifikat har erbjudits anses inte vara avgörande*. I stället kan det, enligt lagmotiven, vara rimligt att som huvudregel utgå från att *det rör sig om utfärdande till allmänheten när certifikaten avses användas vid kommunikation med andra än utfärdaren, alltså en tredje part, och det inte föreligger något kontraktsförhållande mellan utfärdaren och denne tredje part.* Anger en certifikatutfärdare att certifikaten är kvalificerade, utan att i certifikaten begränsa kretsen av möjliga mottagare på ett mer precist sätt, kan det finnas anledning att anse att certifikatutfärdaren omfattas av lagens tillämpningsområde. Den närmare tolkningen av begreppet "till allmänheten" har överlämnats till rättstillämpningen (prop. 1999/2000:117 s. 35–36).

Nuvarande e-legitimationsutfärdare är i dag bundna till en affärsmodell där man tar betalt för spärrkontroll. Detta förutsätter ett kontraktsförhållande med förlitande part och får till följd att spärrinformation inte kan tillhandahållas öppet till andra förlitande parter som inte omfattas av sådant kontraktsförhållande.

Dagens e-legitimationsutfärdares tjänster kan därför inte uppfylla kraven på att vara kvalificerade med mindre än att nuvarande affärsmodell och kontraktsförhållande med förlitande parter ändras och systemet öppnas för allmän användning.

Av 6 § signaturlagen följer vidare att ett certifikat – för att få kallas kvalificerat – ska innehålla uppgift om att det utfärdats som ett kvalificerat certifikat. Det är inte tillräckligt att certifikatutfärdaren anger detta i sin marknadsföring eller på annat sätt; det måste framgå av själva certifikatet (prop. 1999/2000:117 s. 71).

Detta innebär att även om man överger sin nuvarande affärsmodell och registrerar sig som utfärdare av kvalificerade certifikat, så kommer inte de certifikat som redan utfärdats att räknas som kvalificerade. Endast nya certifikat som innehåller uppgift om att de utfärdats som kvalificerade certifikat uppfyller rekvisiten för att vara kvalificerade.

Här finns en övergångsperiod där alla nuvarande innehavare av e-legitimationer aktivt måste ansöka om nya certifikat efter det att man övergett sin gamla affärsmodell.

Dessa problem drabbar inte bara nuvarande utfärdare av privata e-legitimationer utan drabbar lika hårt dagens tjänstekort. De certifikat som finns utfärdade på tjänstekort blir inte kvalificerade bara för att utfärdaren blir registrerad som utfärdare av kvalificerade certifikat. Innan tjänstekorten kan användas måste nya tjänstekort utfärdas alternativt förses med nya certifikat.

Sammantaget blir en konvertering av befintliga e-legitimationssystem till utfärdande av kvalificerade certifikat mycket kostsam. Detta är en kostnad som sannolikt kommer att drabba svenska myndigheter som i slutändan ska betala för användningen av dessa e-legitimationer.

4 Övergångsproblem

Det är inte rimligt att anta att alla myndigheter byter e-legitimationssystem samtidigt. Under en övergångstid tvingas dagens e-legitimationsutfärdare därför att kvarstå som utfärdare av icke kvalificerade certifikat tills alla e-tjänster har konverterat till den nya federativa infrastrukturen. Först då kan man börja om och ge ut kvalificerade certifikat. Under denna tid måste tjänsteleverantörer vara anslutna till båda systemen samtidigt.

I teorin kan e-legitimationsutfärdaren erbjuda alternativ till användarna,

1. kvalificerade certifikat för legitimering mot myndigheter som är anslutna till federationen, och/eller
2. icke kvalificerade certifikat för legitimering mot myndigheter som är anslutna till nuvarande infratjänst.

I praktiken är en sådan uppdelning mindre hållbar eftersom det blir svårt för användare att välja både vilken e-legitimation de ska skaffa och vilken e-legitimation de ska använda för legitimering mot en viss e-tjänst.

En annan övergångsmöjlighet är att godkänna icke kvalificerade certifikat under en övergångsperiod som är så lång att samtliga myndigheter och utfärdare av e-legitimationer har kunnat konvertera till att använda identitetsfederationen samt att samtliga användare har bytt ut sina e-legitimationer mot nya.

Detta är dock inte helt okomplicerat om det innebär att e-legitimationerna därmed byter tillitsnivå.

Problem uppstår även om någon av dagens utfärdare inte anser att det är tillräckligt lönsamt att registrera sig som utfärdare av kvalificerade certifikat eller om e-tjänster inte kan acceptera kostnaden för den ändrade tillitsnivån.

5 Säkerhetsvinster med kvalificerade certifikat

Identitetsfederationens hanterar kvalitetskrav på identifiering genom att definiera olika tillitsnivåer. Varje tillitsnivå definieras av en rad ingående faktorer så som krav på registrering och verifiering av användares identiteter, legitimeringstekniker och krav på nyckelbärare. De säkerhetskrav som ställs för utfärdare av kvalificerade certifikat i signaturlagen är dock allmänt hållna:

> 9 § En certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten ska bedriva verksamheten tillförlitligt och
>
> 1. ha personal med tillräcklig kompetens och erfarenhet för verksamheten, särskilt vad avser ledning, teknik och säkerhetsrutiner,
> 2. använda sådana rutiner för administration och ledning som uppfyller erkända standarder,
> 3. använda pålitliga system och produkter som är skyddade mot ändringar och se till att teknisk och kryptografisk säkerhet upprätthålls,
> 4. förfoga över tillräckliga ekonomiska medel för att kunna bedriva verksamheten enligt denna lag och bära risken för skadeståndsskyldighet,

5. ha säkra rutiner för identitetskontroll av de undertecknare som kvalificerade certifikat utfärdas till,

6. förfoga över ett snabbt och säkert system för registrering och omedelbar återkallelse av kvalificerade certifikat, och

7. vidta åtgärder mot förfalskning av kvalificerade certifikat och i förekommande fall se till att framställandet av signaturframställningsdata sker konfidentiellt.

Kraven i första stycket 3 ska anses uppfyllda för sådan maskin- eller programvara som överensstämmer med sådana standarder för produkter för elektroniska signaturer som Europeiska gemenskapernas kommission fastställt och offentliggjort referensnummer till i Europeiska gemenskapernas officiella tidning.

10 § En certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten ska

1. omedelbart återkalla ett certifikat när undertecknaren begär det eller när det annars finns anledning till det,

2. säkerställa att exakt tidpunkt kan anges för utfärdande och återkallelse av certifikat, och

3. säkerställa att av utfärdaren framställda signaturframställningsdata och signaturverifieringsdata kan användas som komplement till varandra.

Det finns inget som hindrar att identitetsfederationen ställer krav på utfärdare av e-legitimationer som motsvarar dessa krav utan att för den sakens skull kräva att e-legitimationen baseras på ett kvalificerat certifikat i lagens mening.

Därmed kan man inte förutsätta att en e-legitimation som baseras på ett kvalificerat certifikat är säkrare bara på grundval av att det är kvalificerat. Förtroendenivå avgörs av den definierade tillitsnivån.

I tillitsramverket kan federationen ställa olika krav på säkerhetsnivåer som både är högre och lägre än kvalificerade certifikat, vilket också är fallet i EU projektet STORK (se nedan under internationell samverkan). Tillitsramverket är vidare mycket mer detaljerat än lagens krav på utfärdare av kvalificerade certifikat.

En annan viktig aspekt som avgör graden av tillförlitlighet är kvaliteten på den nyckelbärare som certifikatet är kopplat till. Kravställningarna runt kvalificerade certifikat ställer inga specifika krav på nyckelbärarens kvalitet. En e-legitimation utgiven av en bank med smart kort som nyckelbärare kan anses vara mer tillförlitlig än ett kvalificerat certifikat med mjuk nyckelbärare

utfärdat av en identitetsutfärdare som inte har en tidigare relation med e-legitimationsinnehavaren.

6 Internationell samverkan

Internationell samverkan runt identifiering baseras inom ramen för dagens aktiviteter inom Europa på federationsteknik och dess ramverk för tillitsnivåer.

Inom ramen för STORK-projektet har ett ramverk definierats för tillitsnivåer med 4 nivåer som i stora drag är kompatibelt med det internationella ramverket ”Kantara Identity Asurance Framework” som även ligger till grund för de tillitsnivåer som vi avser definiera i Sverige.

Nivå 4 av STORK-projektets tillitsnivåer förutsätter kvalificerade certifikat samt hårda nyckelbärare. Nivå 3 och lägre förutsätter inte att kvalificerade certifikat används och tillåter mjuka nyckelbärare.

Det är värt att notera att det inte räcker med att ett certifikat är kvalificerat för att uppnå STORK tillitsnivå 4. Även om dagens leverantörer av e-legitimationer konverterar och ger ut kvalificerade certifikat så uppnås därmed inga fördelar inom ramen för internationell samverkan med mindre än att man även kräver att alla nyckelbärare ska vara hårda (ex smarta kort).

Enligt STORK uppfyller såväl certifikat med mjuk nyckelbärare som koddosor utan certifikat kraven för nivå 3. Även om vi i Sverige kräver kvalificerade certifikat men tillåter mjuka nyckelbärare, samtidigt som vi inte tillåter icke kvalificerade certifikat eller icke certifikatbaserade lösningar, så är vi därmed i klar disharmoni med det Europeiska ramverket eftersom vi har dragit en linje rakt igenom tillitsnivå 3.

Om Sverige vill harmonisera med STORK-ramverket så ska nivå 4 kräva kvalificerade certifikat och hårda nyckelbärare medan nivå 3 ska tillåta icke kvalificerade certifikat och alternativa autentiseringsmetoder med motsvarande säkerhetsnivå.

Om vi i Sverige inte avser kväva nivå 4 för alla e-tjänster (vilket torde vara orimligt) så måste även icke kvalificerade certifikat tillåtas i federationen om Sveriges tillitsramverk (för nivå 3) ska harmonisera med övriga Europa.

7 Juridiska frågor om säkerhetsnivå

I ett beslut den 16 oktober 2009 av Europeiska kommissionen (2009/767/EG) om åtgärder för att underlätta användningen av förfaranden på elektronisk väg genom gemensamma kontaktpunkter har kommissionen uttalat sig bl.a. angående användande av elektroniska signaturer (artikel 1). Där framgår att medlemsstaterna ska kräva att en användning av avancerad elektronisk signatur baserad på ett kvalificerat certifikat, endast om det är motiverat på grundval av en ändamålsenlig bedömning av berörda risker.

En identitetsfederation har ingen direkt koppling till elektroniska underskrifter eftersom den är till för identifiering. Krav på elektroniska underskrifter kan hanteras i en separat signeringstjänst.

Det kan därför vara mindre lämpligt att motverka eller utmönstra identifiering med alternativa metoder.

Till saken hör också att det inte någonstans i svensk lagstiftning eller författningsreglering krävs en kvalificerad elektronisk signatur (se 2 § signaturlagen där ”kvalificerad elektronisk signatur” definieras som en avancerad elektronisk signatur som är baserad på ett kvalificerat certifikat och som är skapad av en säker anordning för signaturframställning).

Hur lätt det är att blanda samman dessa begrepp framgår emellertid av bl.a. Karnovkommentaren till lagen (2005:807) om ersättning för viss mervärdesskatt för kommuner och landsting. Där sägs följande i not 15 till 9 §:

> Bestämmelsen är utformad efter mönster av 10 kap. 26 § skattebetalningslagen (1997:483) och 4 kap. 4 § lagen (2001:1227) om självdeklarationer och kontrolluppgifter, se prop. 2005/06:7, s. 29 f. Att kravet på underskrift får uppfyllas med elektroniska medel innebär att det finns en kvalificerad elektronisk signatur (kursiverat här). Detta följer av 17 § lagen (2000:832) om kvalificerade elektroniska signaturer. De aktuella blanketterna finns normalt endast som ifyllnadsbara pdf-blanketter på Skatteverkets hemsida.

Ett studium av regeringens proposition 2005/06:7 Vissa kommunalekonomiska frågor visar på samma missförstånd. Där sägs följande:

> I andra stycket anges vad som är ett elektroniskt dokument. Att kravet på underskrift ska anses som uppfyllt med elektroniska medel innebär att det finns en kvalificerad elektronisk signatur. Detta följer av 17 § lagen (2000:832) om kvalificerade elektroniska signaturer.

Påståendena är felaktiga. I 9 § andra stycket nämnda lag föreskrivs nämligen att med ett elektroniskt dokument avses en upptagning som har gjorts med hjälp av automatiserad databehandling och vars innehåll och utställare kan verifieras genom ett visst tekniskt förfarande. Denna definition kräver inte att den elektroniska signaturen ska vara kvalificerad; jfr motsvarande misstag i prop. 2001/02:25 s. 172.

En näraliggande slutsats – från juridiska och praktiska utgångspunkter – är därmed att det kan vara lämpligt att undvika en begreppsapparat som missförståtts av så många och som bygger på en teknikstyrd terminologi som genererar ständiga diskussioner och behov av klargöranden. Ett praktiskt alternativ är att bygga på sådana tillitsnivåer och anslutning till en identitetsfederation som övervägs inom detta projekt.

8 Ekonomi Affärsmodell

Identitetsutfärdare kommer att klassas i enlighet med den tillitsnivå de erbjuder och varje tjänstetyp för varje e-tjänsteleverantör kommer att deklarera vilken tillitsnivå de kräver. Det är därför väldigt enkelt att hantera flera tillitsnivåer i federationen.

Inom ramen för den fördelning av pengar som sker till identitetsutfärdare borde det finnas utrymme för olika ersättningsnivåer beroende på vilken tillitsnivå man tillhandahåller, alternativt viktad mot vilken tillitsnivå som e-tjänsten krävt.

9 Realistiska alternativ

Ett realistiskt alternativ till att kräva kvalificerade certifikat för medlemskap i federationen är att vi i Sverige definierar tillitsnivåer som harmoniserar med internationella standarder och Europeiska normer med eventuella tillägg för Svenska förhållanden inom ramen för de internationella ramverken.

Nivå 3 kan då inte kräva kvalificerade certifikat medan nivå 4 troligen gör detta i kombination med krav på hårda nyckelbärare.

Inom ramen för den upphandlingsmodell för identifieringstjänster som tas fram bör man vidare ha möjlighet att anpassa ersättningsnivå till identitetsutfärdare beroende på vilken tillitsnivå de tillhandahåller.

Teknisk sammanfattning av infrastrukturen för Svensk e-legitimation

1 Sammanfattning

Denna sammanfattning av Infrastrukturen för Svensk e-legitimation är riktad till läsare som är bekanta med federationsteknik enligt SAML 2.0 och de tekniker som i övrigt ligger till grund för utfärdande och användning av e-legitimationer för identifiering och signering.

2 Grundstruktur och skillnader mot dagens infrastruktur

Infrastrukturen för identifiering inom ramen för Svensk e-legitimation bygger på en federativ modell enligt protokollet SAML 2.0.

Detta innebär inga skillnader för utfärdande och utformning i förhållande till dagens e-legitimationer. Samma e-legitimationer som används inom nuvarande infrastruktur kommer att kunna användas inom ramen för en federativ modell.

Den stora skillnaden är att ”Service Providers” SP (i utredningen kallade E-tjänsteleverantörer) inte kommer i direkt kontakt med användarnas e-legitimationer utan istället får ett identitetsintyg i form av en SAML assertion från e-legitimationsutfärdarens Identity Provider (IdP).

I en traditionell SAML-relation innebär detta att myndigheters e-tjänster intar rollen som service provider (SP) och att e-legitimationsutfärdarna intar rollen som Identity Provider (IdP) och därmed den part för vilken användaren identifierar sig, oavsett vilken e-tjänst som användaren avser att logga in på.

Övergången från att hantera e-legitimationer direkt till att konsumera Identitetsintyg i form av SAML assertions innebär även

att de identitetsuppgifter som förmedlas till e-tjänsten kan anpassas efter e-tjänstens behov. När e-tjänsten kräver personnummer ska denna information ingå i identitetsintyget men om e-tjänsten istället kräver andra uppgifter som exempelvis organisationsnummer och ID inom organisationen kan informationen i identitetsintyget anpassas till e-tjänstens behov oavsett vilken e-legitimation som användaren använt för att legitimera sig.

För de fall där e-tjänsten behöver mer information om användaren som loggar in, exempelvis uppgift om juridisk behörighet kan en fråga ställas till en Attribute Authority – AA (I utredningen benämnd Attributsutfärdare) som genom en attribute query (attributsförfrågan) kan erhålla nödvändig kompletterande information.

Härvid kan teoretiskt sett alla typer av e-legitimationer, även de som inte innehåller några specifika personuppgifter så som koddosor för generering av engångslösenord, användas för inloggning mot en myndighet som kräver såväl personnummer som ytterligare information om juridisk behörighet.

3 Tillitsramverk och Säkerhetsnivåer

Grunden för vilken säkerhetsnivå som tillämpas när en användare legitimerar sig är den tillitsnivå som e-tjänsten kräver. För att dessa säkerhetsnivåer ska kunna vara jämförbara inom ramen för federationen definieras fyra tillitsnivåer (assurance levels) för federationen genom ett tillitsramverk. Alla IdP som utfärdar Identitetsintyg till anslutna e-tjänster måste visa att hela den process som ligger till grund för utfärdandet av identitetsintyg uppfyller kraven i den efterfrågade tillitsnivån, detta innefattar bl.a.

- Krav på utfärdandeprocessen.
- Krav på själva e-legitimationen och dess användning.
- Krav på utfärdaren av e-legitimationen.

Mer information om tillitsramverket tillhandahålls i *Bilaga 9*.

4 Metadata

För att infrastrukturen ska kunna erbjuda identifiering med hög säkerhetsnivå måste bl.a. Identitetsintyg med identitetsuppgifter signeras och krypteras från IdP till e-tjänst. Detta kräver att parterna har tillgång till varandras publika nycklar dels för verifiering av signaturer och dels för kryptering av data.

Vidare behöver e-tjänsters krav på attribut och tillitsnivåer finnas tillgängliga så att en IdP kan leverera ett identitetsintyg med lämplig information om användare till e-tjänsterna.

För att underlätta spridning av denna information på ett tillförlitligt sätt lagras sådan information i ett centralt register med s.k. metadata. Dessa metadata hålls tillgänglig för de aktörer som behöver den. Varje IdP måste ha tillgång till information om alla e-tjänster och e-tjänsterna behöver information om varje IdP och attributstjänst. Metadatainformationen tillhandahålls i signerad form, signerad av den federationsoperatör som administrerar federationen och dess tillhörande registeruppgifter.

5 Discovery service

5.1 Grundläggande syfte och funktion

Genom federationens metadata vet varje e-tjänst vilken IdP som ska identifiera en användare med en specifik typ av e-legitimation och som ska utfärda ett Identitetsintyg för användaren.

För att detta ska kunna ske måste dock e-tjänsten veta vilken e-legitimation som användaren kan och vill använda. E-tjänsten kan så som sker idag låta en användare välja vilken av alla tillgängliga e-legitimationer som användaren vill använda men detta blir opraktiskt i takt med att antalet alternativ ökar.

En discovery service (i utredningen benämnd Anvisningstjänst) kan i samarbete med varje användare komma ihåg vilken e-legitimation som användaren använt tidigare mot andra e-tjänster och därmed skapa förenklade dialoger där användarens tidigare val av e-legitimation kommer upp som förval.

Utredningen förordar att en discovery service ska erbjudas i två versioner, en där användaren omdirigeras till discovery service

enligt standardiserat SAML protokoll och ett där en dynamisk webbsida från e-tjänsten kan anpassas till användarens förval genom s.k. AJAX anrop till discoverytjänsten. Dessa alternativ finns närmare beskrivna i *bilaga 16*.

5.2 Förhållande mellan IdP och utfärdare av e-legitimation

Det är viktigt att användarens val av e-legitimation blir begriplig för användaren. Detta innebär att användaren endast ska behöva välja typ av e-legitimation för att e-tjänsten ska kunna hänvisa användaren till rätt IdP för identifiering.

Samtidigt är det viktigt att användaren inom ramen för Infrastrukturen för svensk e-legitimation känner igen sig vid varje identifieringstillfälle. Det är därför betydelsefullt att användaren alltid identifierar sig för samma IdP oberoende av vilken e-tjänst inom infrastrukturen som kräver legitimering.

Varje typ av e-legitimation från en specifik utfärdare måste vidare kopplas till ett namn på e-legitimationen som användaren känner igen och kan relatera till i det gränssnitt för val av e-legitimationer som skapas i samverkan med infrastrukturens discovery service. Detta namn återfinns även i federationens metadata för respektive IdP. Det är dessa metadata som utgör grunden för att såväl skapa val-gränssnitt för användare som att koppla användarens val till en viss IdP.

För att garantera att varje typ av e-legitimation representeras av ett för användaren begripligt namn och att detta endast kopplas samman med en IdP, är e-legitimationsutfärdaren ansvarig för definition av namn för dennes olika typer av e-legitimationer samt att specificera en och endast en godkänd IdP för vare typ av e-legitimation.

6 Integration i e-tjänster

Hantering av SAML Assertions är i dag väldigt enkelt då de stöds av en lång rad färdiga produkter och i allt större utsträckning stöds som standard i olika miljöer och verktyg för att införa webb-tjänster.

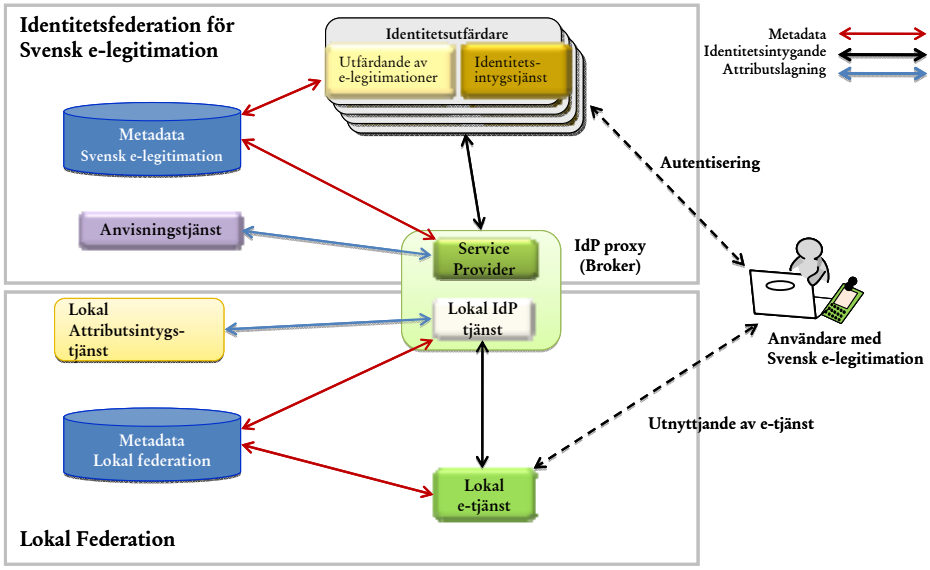
Eftersom Identitetsintyg följer ett standardiserat format behöver e-tjänster i den federativa modellen inte anpassas ytterligare om nya aktörer i egenskap av identitetsutfärdare tecknar avtal med federationsoperatören (E-legitimationsnämnden).

Integrationen av färdiga e-tjänster mot den nya infrastrukturen är därför förhållandevis enkel. För de parter som avser att skapa en ny e-tjänst, utgör integration med den federative infrastrukturen en generellt sett försumbar kostnad i jämförelse med vad det kostar att skapa själva e-tjänsten.

6.1 Integration med lokala federationer

Idag existerar många befintliga identitetsfederationer som är uppbyggda på liknande sätt som identitetsfederationen för Svensk e-legitimation. En sådan "lokal" identitetsfederation kan innefatta e-tjänster som nyttjar en IdP inom den lokala federationen för att erhålla identitetsintyg som följer lokala konventioner, men där denna e-tjänst likväl vill tillåta att användare ska kunna identifiera sig via identitetsfederationen för Svensk e-legitimering.

Detta kan enkelt lösas genom att den lokala IdP:n i den lokala federationen uppträder som en IdP Proxy enligt följande modell:



En IdP Proxy agerar som en IdP inom en lokal federation mot e-tjänster i den lokala federationen men utgör samtidigt en registrerad Service Provider (e-tjänst) i federationen för Svensk e-legitimation. En användare med Svensk e-legitimation som loggar in på en e-tjänst som är ansluten till den lokala federationen överförs till IdP Proxy som i enlighet med lokala konventioner konstaterar att användaren ska identifieras genom federationen för Svensk e-legitimation. Användaren anvisas till och identifieras av den IdP som är kopplad till användarens e-legitimation och ett identitetsintyg returneras till IdP Proxy. IdP Proxy aggregerar vid behov ytterligare information om användaren och returnerar sedan ett lokalt identitetsintyg till e-tjänsten i den lokala federationen.

För att underlätta discovery i den lokala federationen så att användaren kan ges en korrekt uppsättning val av e-legitimationer för inloggning som även inkluderar e-legitimationer som bara hanteras inom federationen för Svensk e-legitimation, kan lämplig metadata om IdP tjänster i federationen för Svensk e-legitimation inkluderas i den lokala federationens metadataregister.

7 Signering

I nuvarande infrastruktur sker signeringen i användarens klient av den information som skickas från e-tjänsten. Detta kräver dels att e-tjänsten kan skicka information som ska signeras på ett sätt som är anpassat till användarens lokala klientprogramvara och e-legitimation, dels att användarens e-legitimation är certifikatbaserad och kan användas för att skapa en elektronisk signatur enligt gällande standards.

Elektroniska signaturer som skapas i dagens modell kan endast verifieras av parter som har avtal med e-legitimationsutfärdaren för åtkomst till spärrinformation. Detta omöjliggör i praktiken för utländska myndigheter att verifiera en signatur skapad med en svensk e-legitimation.

I en ny modell där det kan förekomma e-legitimationer som inte kan användas för signering krävs en annan lösning som

- inte kräver att e-tjänsten inför anpassningar mot varje typ av e-legitimation och klientprogramvara, och
- gör det möjligt

- för alla användare att signera, även de som innehar en icke certifikatbaserade e-legitimationer, och
- för utländska aktörer att verifiera en signatur som är skapad med stöd av en svensk e-legitimation.

Utredningen har föreslagit att en central signeringstjänst ska övervägas för att tillgodose dessa behov. Olika förslag på lösningar presenteras i *Bilaga 17*.

Tekniskt ramverk

Teknisk beskrivning av infrastrukturen för Svensk e-legitimation

1 Introduktion

Det tekniska ramverket beskriver hur identitetsfederationen implementeras tekniskt. Identitetsfederationen är baserad på den internationella standarden SAML v2.0 specificerad i [SAML2Core].

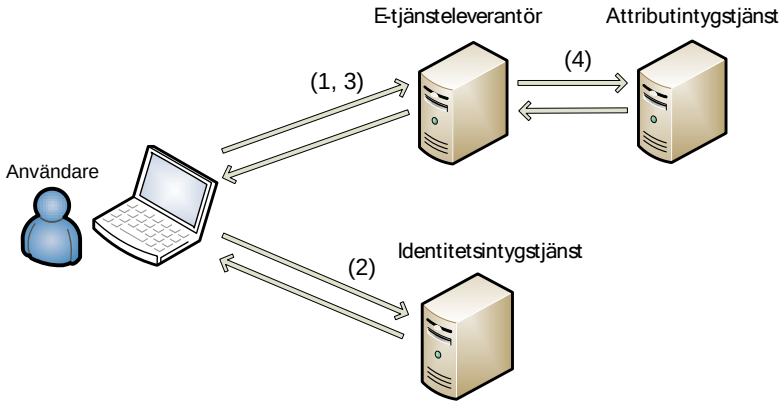
SAML är en flexibel standard som inte reglerar implementationen av aktuella identitetsfederationer på detaljnivå. För att kunna federera med SAML på ett effektivt sätt behöver ett antal vägval göras och dokumenteras. Den tekniska dokumentationen utgörs av dessa vägval och närmare reglering av hur standarden används.

Grundtanken vid framtagandet av det tekniska ramverket har varit att i så stor utsträckning som möjligt använda internationellt vedertagna tekniska profiler för federering och SAML.

2 Teknisk bakgrund

2.1 Elektroniska intyg

Det är viktigt att noggrant specificera format och innehåll för de elektroniska intyg som kommuniceras mellan identitetsintygstjänst (IdP), e-tjänsteleverantör (SP), och attributintygstjänst. Syftet är att förenkla kommunikationen mellan parter i identitetsfederationen utan att skapa onödiga begränsningar. Som bakgrund presenteras nedan det tänkta informationsflödet vid en inloggning till en webbtjänst i identitetsfederationen.



1. Användaren ansluter till e-tjänsten.

2. E-tjänsteleverantören skickar användaren vidare till ett inloggningsformulär hos identitetsintygstjänsten med hjälp av en identitetsförfrågan.

3. Efter framgångsrik autentisering utfärdas ett identitetsintyg som skickas tillbaka till e-tjänsteleverantören. Detta intyg beskrivs ingående i avsnitt 2 i attributspecifikation [AttrSpec].

4. Om e-tjänsteleverantören behöver ytterligare information om användaren kan denna hämtas från en attributintygstjänst via en attributförfrågan. Denna process beskrivs närmare i avsnitt 3 i attributspecifikationen.

Attributintyg används för att e-tjänsteleverantörer ska kunna hämta användarattribut som inte är kända för identitetsintygstjänsten. Exempel på sådana attribut kan vara organisationstillhörighet, roll, behörighetsinformation etc.

Det finns ingen teoretisk begränsning i vilken information som kan kommuniceras via attribut. Det är dock viktigt att påpeka att en attributsförfrågan skiljer sig från en auktorisationsfråga.

En attributsförfrågan besvarar frågan: ”Vilka egenskaper har detta subjekt?”

En auktorisationsförfrågan besvarar frågor av typen: ”Får detta subjekt genomföra åtgärd X”.

Rena auktorisationsfrågor kan inte besvaras med ett attributsintyg.

2.2 Tillit och metadata

Identitetsfederering via SAML är baserat på att identitetsintygsgivarna och e-tjänsteleverantörerna litar på varandra och därmed kan verifiera de signaturer som används i SAML-kommunikationen. Rent tekniskt så baseras denna tillit på att respektive parter litar på varandras URL:er och tillhörande servercertifikat.

Tillitsprocessen automatiseras via användning av SAML metadata [SAML2Meta]. Specifikationen av metadata är framtagen av OASIS för att underlätta administration av större federationer. Federationen definieras då av ett register i XML-format som är signerat med federationsoperatörens certifikat. Filen innehåller information om identitetsfederationens medlemmar inklusive deras servercertifikat. Eftersom metadatafilen är signerad räcker det med att jämföra ett servercertifikat med dess motsvarighet i metadatat.

En infrastruktur baserad på ett centralt federationsregister förutsätter att registret uppdateras kontinuerligt samt att federationsmedlemmarna alltid använder den senaste versionen av filen.

För att kunna använda metadata krävs en central aggregator som kontinuerligt hämtar lokal metadata från federationsdeltagarna och uppdaterar och signerar federationsregistret. Mjukvarukrav på hantering av lokal metadata beskrivs i federationens implementationsprofil [ImpProf].

2.3 Federationsregister

Inom identitetsfederationen används federationsregister definierade av metadatafiler publicerade av federationsoperatören. Registren kommer att innehålla följande typer av information:

- Information om identitetsintygsgivare och attributintygsgivare
- Information om e-tjänsteleverantörer, såväl offentliga som kommersiella från näringslivet.

Hantering och innehåll i metadata specificeras i [MetaSpec].

2.4 Användning av SAML

Svensk eID-federation använder SAML, version 2.0 eller högre. SAML v2.0 är en mycket omfattande standard som definierar ett antal så kallade användningsprofiler. Av de tillgängliga profilerna används följande.

- *SAML Web Browser SSO Profile* definierad i [SAML2Prof]. Profilen används för federerad autentisering mot e-tjänster.
- *SAML Assertion Query/Response Profile* definierad i [SAML2Core] och [SAML2Prof]. Profilen används för attributförfrågningar och attributsintyg.
- *IdP Discovery Profile* definierad i [IdPDisco].

Profilerna är relativt generellt hållna och lämnar många beslut öppna till de faktiska implementationerna.

3 Normativ dokumentation

Dokumenten listade i detta avsnitt reglerar normativt hur förloppen beskrivna i kapitel 1 och 2 realiseras inom svensk eID-federation. Samtliga dokument förutom SAML2Int är framtagna som del av utredningens arbete.

3.1 SAML2Int

SAML2Int är en samling av större akademiska identitetsfederationer vilka tillsammans tagit fram en profil [SAML2Int] som reglerar typisk användning av *Web Browser SSO Profile*. Istället för att göra om deras arbete väljer vi att istället peka på denna profil som riktlinje för användning av *Web Browser SSO*.

3.2 Attributspecifikation

Det är nödvändigt att specificera format och innehåll på de elektroniska intyg som skickas mellan identitetsintygstjänst, e-tjänsteleverantörer och attributintygstjänst. Detta regleras i attributspecifikationen [AttrSpec].

Attributspecifikationen pekar tillbaka på *Web Browser SSO* för hantering av identitetsintyg och *Assertion Query/Response Profile* för attributsintyg.

3.3 Specifikation av metadata

Federationen hålls samman av tre stycken federationsregister. Innehåll, uppdatering och publicering av dessa register beskrivs i specifikation av metadata [MetaSpec].

3.4 Anvisningstjänst

En anvisningstjänst tillhandahåller en tjänst till e-tjänsteleverantörer som underlättar processen att fastställa vilken identitetsintygstjänst som ska autentisera en användare. Anvisningstjänsten beskrivs närmare i [AnvTj].

3.5 Krav på mjukvara

Mjukvara som ska användas inom Infrastrukturen för Svensk e-legitimation förväntas leva upp till kraven i implementationsprofilen [ImpProf].

4 Referenser

[AnvTj] Utredningen kring bildandet av en ny e-legitimationsnämnd FI 2010:05, ”Anvisningstjänst”, 2010

[AttrSpec] Utredningen kring bildandet av en ny e-legitimationsnämnd FI 2010:05, ”Attributspecifikation”, 2010

[IdPDisco] OASIS Committee Specification, ”Identity Provider Discovery Service Protocol and Profile”, March 2008.

[ImpProf] Utredningen kring bildandet av en ny e-legitimationsnämnd FI 2010:05, ”Implementation Profile”, 2010

[MetaSpec] Utredningen kring bildandet av en ny e-legitimationsnämnd FI 2010:05, ”Specifikation av metadata”, 2010

[SAML2Core] OASIS Standard, “Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0”, March 2005.

[SAML2Int] SAML2Int, ”Interoperable SAML 2.0 Profile”, <http://saml2int.org/profile/current>

[SAML2Prof] OASIS Standard, “Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0”, March 2005

Attributspecifikation

Specifikation av innehåll och format på identitets- och attributsintyg

1 Identitetsintyg

Varje deltagande identitetsintygstjänst eller e-tjänsteleverantör i identitetsfederationen måste uppfylla de identitetsprofiler som presenteras i denna specifikation. Det står identitetsintygstjänst fritt att kommunicera ytterligare information i intygen förutsatt att intygen följer det i detta dokument fastlagda formatet.

1.1 Användningsfall

Inom infrastruktur för Svensk e-legitimation hanteras tre olika identitetsprofiler eller användningsscenarier; personlig, anonymiserad samt organisationsanknuten identitet. Nedan följer exempel på användar-fall som motsvaras av de tre identitetstyperna. Närmare specifikation av attributen ges i avsnitt 1.4.

1.1.1 Personlig identitet

Personlig identitet används när en medborgare behöver identifiera sig mot en e-tjänst med personnummer. Detta kan liknas vid inloggning med certifikatsbaserad e-legitimation innehållande personnummer.

Obligatoriska attribut: pseudonym, personnummer, namn
Valfria attribut: tillitsnivå, adress, telefonnummer, e-post

1.1.2 Organisationsidentitet

För vissa tillämpningar är det intressant att basera användarens identitet på organisationstillhörighet. Information om identitet hos den aktuella organisationen kan även kompletteras med personlig identitet (personnummer).

Obligatoriska attribut: pseudonym, organisationstillhörighet(er) och namn
Valfria attribut: personnummer, adress, telefonnummer, e-post

Flera samtidiga organisationstillhörigheter representeras i intyget som en sekvens av attribut av samma typ.

1.1.3 Pseudonym identitet

En pseudonymiserad identitet används för att skydda den personliga integriteten. En sådan identitet kan användas närhelst en e-tjänst inte kräver koppling av användaren till en specifik fysisk individ. Många enklare webbtjänster som används idag utanför offentlig sektor lämpar sig för denna typ av inloggning.

Obligatoriska attribut: pseudonym
Valfria attribut: adress, telefonnummer, e-post

1.2 Identitetsintyg

Format och hantering av identitetsintyg beskrivs i [SAML2Core].

Inom identitetsfederationen måste alla identitetsintyg av säkerhets- och anonymitetskäl skickas i krypterad form. Det är valfritt för e-tjänsteleverantörerna att signera identitetsförfrågningar men obligatoriskt att signera attributförfrågningar. Kryptering och signering sker med respektive parts publika nyckel vilken publicerats i metadata.

1.2.1 Format på identitetsintyget

Regler för utgivande av identitetsintyg ges nedan.

1. Om identitetsintygstjänsten önskar returnera ett fel ska svaret <saml2p:Response> inte innehålla någon <Assertion>.
2. Om autentiseringen är lyckad ska identitetsintyget innehålla åtminstone:

- Utfärdaren av identitetsintyget som elementet <Issuer>.
- En <Assertion> innehållande exakt en <AuthnStatement> som innehåller ett <NameId> med en persistent pseudonym. Intyget innehåller även ett flertal attribut i enlighet med avsnitt 2.1.
- Tillitsnivå kommuniceras som del av <AuthnContext> enligt specifikation i [IdAssurProf] och [AuthCtx]. Faktiska tillitsnivåer och namnrymd är definierade i tillitsramverket [TillRamverk].

Det är valfritt men rekommenderat att utöver tillitsnivå även kommunicera använd autentiseringsmetod som del av <AuthnContext>.

1.2.2 Kodning av attribut

- XML-attributet `NameFormat` på elementet `Attribute` måste vara `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`
- Attributnamn måste vara en URI som beskrivet ovan.
- XML-attributet `FriendlyName` är valfritt.
- Alla attribut måste ha en OID och ska använda denna som namn.
- Alla attributvärden måste vara av typen "`xs:string`".

Ett exempelattribut formaterat enligt ovanstående regler ges nedan:

```
<saml:AttributeNameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
        Name="urn:oid:2.5.4.4" FriendlyName="displayName">
        <saml:AttributeValue xsi:type="xs:string">John
Smith</saml:AttributeValue>
</saml:Attribute>
```

1.3 Pseudonymisering

Pseudonymisering består i att ersätta identifierbar data såsom personnummer med en artificiell identifierare. Av anonymitetskäl är den unika användaridentifieraren i identitetsintyget en pseudonym.

Pseudonymen genereras av IdP baserat på EntityID för IdP, SP samt en unik användaridentifierare endast känd av IdP:n. Det är viktigt att pseudonymen är genererad på ett sådant sätt att den inte kan användas för att härleda användarens identitet.

I samtliga användarfall beskrivna i avsnitt 2.1 kommuniceras pseudonymen som SAML `NameID` i identitetsintyget.

1.4 Attributdefinitioner

Endast attribut med befintlig allokerad OID (objektidentifierare se [RFC3061]) är tillåtna. Följande obligatoriska attribut hanteras som del av identitetsintyg inom federationen.

Beskrivning	Attributnamn	OID
Personnummer*	personalIdentityNumber	1.2.752.29.4.13
Org-identifierare	orgAffiliation	Allokeras av nämnden
Namn**	displayName	2.16.840.1.113730.3.1.241
Namn (alternativ)	Sn	2.5.4.4
	givenName	2.5.4.42
Nåbarhetsadress	postalAddress	2.5.4.16
Folkbokföringsadress	Street	2.5.4.9
	postOfficeBox	2.5.4.18
	postalCode	2.5.4.17
	l	2.5.4.7
	c	2.5.4.6
Telefon	telephoneNumber	2.5.4.20
Mobil	Mobile	0.9.2342.19200300.100.1.41
Epost	Mail	0.9.2342.19200300.100.1.3

*Attributet används även för samordningsnummer [Samord].

** Fördelen med displayName är att attributet är av ”single value” typ.

1.4.1 Organisationsidentifierare

Identifieraren ska identifiera en organisation (svenskt organisationsnummer) med möjlighet att specificeras en inom organisationen lokal identifierare, t.ex. anställningsnummer eller användarnamn. Roll inom organisationen specificeras inte genom denna identifierare. Syntax:

http://id.gov.se/org/< se-org-no > [/< local-part >]

Exempel på organisationsidentifierare för en organisation med organisationsnummer 123456-7890 skulle kunna vara:

http://id.gov.se/org/123456-7890
http://id.gov.se/org/123456-7890/svensvensson
http://id.gov.se/org/123456-7890/9823

1.4.2 Egendefinierade attribut

Inom infrastrukturen för identifiering kan det uppstå behov attribut som endast några få deltagare i infrastrukturen behöver känna till. Om en attributstjänst exempelvis tillhandahåller ett attribut som är anpassat till en viss tjänst, så är det bara användare av den tjänsten som behöver känna till hur detta attribut ska hanteras.

Definition av attribut som används inom ramen för svensk e-legitimation kan därför hanteras olika beroende på attributets användningsområde:

Attribut som måste kunna hanteras av alla deltagare i infrastrukturen – Information om dessa attribut införs i infrastrukturens attributspecifikation

Attribut som är av allmänt intresse – Information om dessa attribut kan ingå i infrastrukturens attributsspecifikation men kan även definieras i separata dokument som godkänns och publiceras av e-legitimationsnämnden.

Privata attribut som bara behöver förstås av några få aktörer inom ramen för ett avgränsat användningsområde - Definition av dessa attribut kan göras oberoende av e-legitimationsnämnden. Om ett sådant attribut listas i något av federationens register (metadata) så måste dock

attributets definition godkännas och publiceras av e-legitimationsnämnden.

En aktör som behöver definiera ett nytt attribut med begränsat användningsområde kan göra så och fritt förmedla information om detta attribut till berörda parter utan att ansöka om tillstånd.

2 Attributsintyg

2.1 Användningsfall

Ett exempel på en tjänst som begagnar attributsförfrågan skulle kunna vara att Skatteverket vill låta privatpersoner se skattekonton för de företag respektive person företräder. För att ta reda på denna information gör Skatteverket en attributförfrågan till Bolagsverket.

2.2 Format på attributsintyg

Attributsintyg använder SAML-profilen *Attribute Query / Response* definierad i [SAML2Prof] och [SAML2Core].

Attributsförfrågningar använder en så kallad `<saml2p:AttributeQuery>` och attributsintyget kommuniceras inom ramen för ett `<saml2p:Response>`.

Attributförfrågningar autentiseras mot attributintygstjänsten med e-tjänsteleverantörens certifikat (enligt metadata) som klientcertifikat.

2.3 Attributdefinitioner

I denna specifikation görs ingen reglering av vilken information som får eller måste kommuniceras inom attributsintyg inom federationen.

Däremot ges i följande tabell rekommendationer för vilka faktiska attribut som bör användas för att representera vissa vanliga egenskaper. Nedanstående tabell kompletterar attributdefinitionerna i avsnitt 1.4.

Beskrivning	Attributnamn	OID
Organisationsnamn	organization	2.5.6.4
Organisationsenhet	organizationalUnit	2.5.6.5

3 Referenser

[AuthCtx] OASIS Standard, "Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0", mars 2005.

[IdAssurProf] OASIS Standard, "SAML V2.0 Identity Assurance Profiles Version 1.0", juli 2010.

[RFC3061] RFC 3061, "A URN Namespace of Object Identifiers", IETF Proposed Standard, februari 2001.

[Samord] Samordningsnummer, SKV 707, utgåva 2, Skatteverket, oktober 2006

[SAML2Core] OASIS Standard, "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0", mars 2005.

[SAML2Prof] OASIS Standard, "Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0", mars 2005.

[TillRamverk] Utredningen kring bildandet av en ny e-legitimationsnämnd FI 2010:05, *Tillitsramverk, 2010*

Specifikation av metadata

Användning av SAML metadata för svensk eID-federation

1 Introduktion

Hanteringen av federationsregister och förtroende inom identitetsfederationen ska följa *OASIS Metadata Interoperability Profile* [MetaIOP]. Profilen är framtagen för att standardisera upprättande av förtroende via metadata. Federationsregister signeras av federationsoperatören.

1.1 Gemensamma regleringar

Attribut refererade i metadata identifieras unikt av sin OID. Obligatoriska attribut och hantering av aktörerna egendefinierade attribut beskrivs i attributspecifikationen [AttrSpec].

Såväl identitets- som attributsintyg ska både krypteras och signeras. Ingen reglering görs av identitetsförfrågningar medan attributsförfrågningar måste signeras.

För att på ett enkelt sätt garantera global unicitet för `EntityID` rekommenderas federationsaktörerna använda ett URI-baserat format involverande den egna organisationen.

1.2 Identitets- och attributintygsgivare

Utöver `EntityID` förväntas Identitetsintygsgivare kommunicera följande information via metadata i enlighet med [MetaIOP]:

- Läsbart namn som unikt identifierar e-legitimationsutfärdaren. Lämpligt attribut är `orgFriendlyName`.
- URL till tjänsten
- certifikat för SAML-kommunikation
- tillgängliga tillitsnivåer, se avsnitt 1.3.1.

Ovanstående kan kompletteras med tillgängliga attribut representerat som en sekvens av `<saml:Attribute>` element.

Attributintygsgivare behöver endast kommunicera URL samt certifikat.

1.3 E-tjänsteleverantörer

E-tjänsteleverantörer förväntas kommunicera följande information via metadata i enlighet med [MetaIOP] och [SAML2Meta]:

- Namn på e-tjänsten
- URL till tjänsten
- certifikat för SAML-kommunikation
- efterfrågade användarattribut som en sekvens av `<RequestedAttribute>` element.
- efterfrågad tillitsnivå, se avsnitt 2.3.

En e-tjänsteleverantör kan tillhandahålla flera e-tjänster förutsatt att tjänsterna har unika URL:er.

1.4 Utvidgningar av metadata

I och med att metadata används i praktiken har det uppstått ett behov av att kunna lägga in godtyckliga attribut. Detta regleras i *SAML V2.0 Metadata Extension for Entity Attributes* [MetaAttr].

1.4.1 Tillitsnivå

Nedan ges ett exempel på hur man lägger till en tillitsnivå för antingen en identitetsintygsgivare eller en e-tjänsteleverantör.

```
<EntityAttributes xmlns="urn:oasis:names:tc:SAML:metadata:attribute">
  <saml:Attribute Name="urn:oasis:names:tc:SAML:attribute:assurance-certification">
  <saml:AttributeValue>http://id.gov.se/AL_X.pdf</saml:AttributeValue>
  </saml:Attribute>
 </EntityAttributes>
```

Attributnamnet `Name` ska som i exemplet ovan vara:
urn:oasis:names:tc:SAML:attribute:assurance-certification

1.4.2 Gränssnitt

För att göra det möjligt för identitetsintygsgivare att kontrollera sin grafiska representation hos anvisningstjänsten är det möjligt att använda metadata UI extensions beskrivna i [MetaUI]. Användningen av gränssnittsutvidgningen är frivillig inom federationen.

2 Centralt register

Federationens tre register sammanställs, signeras och publiceras av federationsoperatören. Federationsoperatören ansvarar för att innehållet i respektive register är korrekt. Medlemsinformation kan inhämtas till registret med valfri metod förutsatt att äktheten kan garanteras.

För att garantera en god tillgänglighet till anvisningstjänsten rekommenderas e-tjänsteleverantörer att lagra en lokal kopia av federationsregistret för identitetsintygsgivare.

3 Referenser

[AttrSpec] Utredningen kring bildandet av en ny e-legitimationsnämnd FI 2010:05, ”Attributspecifikation”, 2010

[MetaAttr] OASIS Committee Specification, ”SAML V2.0 Metadata Extension for Entity Attributes Version 1.0”, August 2009.

[MetaIOP] OASIS Committee Specification, “SAML V2.0 Metadata Interoperability Profile Version 1.0”, August 2009.

[MetaUI] OASIS Committee Specification, “SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0”, September 2010.

[SAML2Core] OASIS Standard, “Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0”, March 2005.

[SAML2Meta] OASIS Standard, “Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0”, March 2005

Implementation Profile

Software requirements for the Swedish Infrastructure for eID

This document is directly based on the InCommon implementation profile for SAML interoperability [InCommon]. Some modifications and additions have been made to adjust to special requirements of the Swedish Infrastructure for eID. The major adjustments relate to the use of pseudonyms and attribute queries.

1 Implementation profile

This profile specifies behavior and options that implementations of the SAML v2 Web Browser SSO Profile and Assertions Query/Request Profile [SAML2Prof] are required to support for use within the Swedish eID-federation. The requirements specified are in addition to the requirements of the original profiles, and readers should be familiar with all relevant reference documents. Any such requirements are not repeated here except where deemed necessary to highlight a point of discussion or draw attention to an issue addressed in errata, but remain implied.

SAML leaves substantial latitude to implementations with regard to how software is architected and combined with authentication and application infrastructure. Where the terms "Identity Provider" and "Service Provider" are used, they should be understood to include the total software footprint intended to provide the desired functionality; no specific assumptions are made as to how the required features are exposed to deployers, only that there is some method for doing so.

2 Metadata and Trust Management

Identity Provider, Service Provider, and Discovery Service implementtations MUST support the use of SAML v2.0 Metadata [SAML2Meta] in conjunction with their support of the SAML V2.0 Web Browser SSO Profile [SAML2Prof]. Additional expectations around the use of particular metadata elements related to profile behavior may be encountered in subsequent sections.

Implementations MUST support the SAML V2.0 Metadata Interoperability Profile Version 1.0 [MetaIOP]. It is OPTIONAL for implementations to support the generation, publication, or exportation of metadata, but implementations MUST support the following mechanisms for the importation of metadata:

- local file
- remote resource at fixed location accessible via HTTP 1.1 [RFC2616] or HTTP 1.1 over TLS/SSL [RFC2818]

In the case of HTTP resolution, implementations MUST support use of the "ETag" header for cache management; other cache control support is OPTIONAL. Implementations SHOULD support the use of more than one fixed location for the importation of metadata, but MAY leave their behavior unspecified if a single entity's metadata is present in more than one source.

In accordance with [MetaIOP], importation of multiple entities' metadata contained within an <*md:EntitiesDescriptor*> element MUST be supported.

Verification of metadata MUST include XML signature verification at least at the root element level, and SHOULD support the following mechanisms for signature key trust establishment:

- direct comparison against known keys
- some form of path-based certificate validation against one or more trusted root certificates and certificate revocation lists

The latter mechanism does not impose a particular profile for certificate validation, as no such profile has wide enough adoption across tools and libraries to warrant such a requirement, but should be understood as being consistent with the "usual" practices encountered in the implementation of certificate validation. Where possible, implementations SHOULD document known limitations of the mechanisms they employ.

Implementations SHOULD support the SAML V2.0 Metadata Extension for Entity Attributes Version 1.0 [MetaAttr] and provide policy controls on the basis of SAML attributes supplied via this extension mechanism.

Finally, implementations SHOULD allow for the automated updating/reimportation of metadata without substantial disruption of services.

3 Identity Provider Discovery

Service Provider and Discovery Service implementations MUST support the Identity Provider Discovery Service Protocol Profile in conformance with section 2.4.1 of [IdPDisco].

4 Pseudonyms

Identity Provider and Service Provider implementations MUST support the following SAML V2.0 name identifier formats, in accordance with the normative obligations associated with them by [SAML2Core]:

- urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
- urn:oasis:names:tc:SAML:2.0:nameid-format:transient

Support for other formats is OPTIONAL.

5 Attributes

Identity Provider and Service Provider implementations MUST support the generation and consumption of <*saml2:Attribute*> elements that conform to the MACE-Dir Attribute Profile for SAML 2.0 [MACEAttr], with the exception that the ability to support <*saml2:AttributeValue*> elements whose values are not simple strings (e.g., <*saml2:NameID*>, or other XML values) is OPTIONAL.

As a non-normative summary, this requirement primarily implies the capability to ensure the use of particular *Name* and *NameFormat* values when generating and consuming <*saml2:Attribute*> elements, rather than relying on hard-wired assumptions or proprietary sets of attribute identifiers.

6 Authentication Requests

6.1 Binding and Security Requirements

Identity Provider and Service Provider implementations MUST support the use of the HTTP-Redirect binding [SAML2Bind] for the transmission of <*saml2p:AuthnRequest*> messages, including the generation or verification of signatures in conjunction with this binding.

Because verification of signatures by Identity Providers cannot be guaranteed in deployments, Service Provider implementations MUST NOT rely on the integrity of a signed request for the enforcement of requirements derived from options such as the *ForceAuthn* attribute or the <*saml2p:RequestedAuthnContext*> element. Rather, Service Providers MUST enforce such requirements based on the content of the <*saml2p:Response*> messages they receive.

Support for other bindings is OPTIONAL.

6.2 Message Content

In addition to standard core- and profile-driven requirements, Service Provider implementations MUST support the inclusion of at least the following <*saml2p:AuthnRequest*> child elements and attributes (when appropriate):

- AssertionConsumerServiceURL
- ProtocolBinding
- ForceAuthn
- IsPassive
- AttributeConsumingServiceIndex
- <saml2p:RequestedAuthnContext>
- <saml2p:NameIDPolicy>

Identity Provider implementations MUST support all <*saml2p:AuthnRequest*> child elements and attributes defined by [SAML2Core], but MAY provide that support in the form of returning appropriate errors when confronted by particular request options. However, implementations SHOULD fully support the options enumerated above. Implementations MAY limit their support of the <*saml2p:RequestedAuthnContext*> element to the value "exact" for the Comparison attribute.

7 Authentication Responses

7.1 Binding and Security Requirements

Identity Provider and Service Provider implementations MUST support the use of the HTTP-POST binding [SAML2Bind] for the transmission of <*saml2p:Response*> messages.

Support for other bindings is OPTIONAL.

Identity Provider and Service Provider implementations MUST support the signing of <*saml2:Assertion*> elements in responses; support for signing of the <*saml2p:Response*> element is OPTIONAL.

Identity Provider and Service Provider implementations MUST support the use of XML Encryption via the <*saml2:EncryptedAssertion*> element; support for the <*saml2:EncryptedID*> and <*saml2:EncryptedAttribute*> elements is OPTIONAL.

7.2 Message Content

The Web Browser SSO Profile allows responses to contain any number of assertions and statements. Identity Provider implementations MUST allow the number of <*saml2:Assertion*>, <*saml2:AuthnStatement*>, and <*saml2:AttributeStatement*> elements in the <*saml2p:Response*> message to be limited to one.

In turn, Service Provider implementations MAY limit support to a single instance of those elements when processing <*saml2p:Response*> messages.

It is OPTIONAL for Identity Provider implementations to support the inclusion of a Consent attribute in <*saml2p:Response*> messages.

Service Provider implementations that provide some form of session semantics MUST support the <*saml2:AuthnStatement*> element's *SessionNotOnOrAfter* attribute.

8 Attribute Queries

Identity Provider and Service Provider implementations MUST support the Assertion Query/Request Profile as defined in [SAML2Prof] and [SAML2Core].

8.1 Binding and Security Requirements

Identity Provider and Service Provider implementations MUST support the use of the SOAP binding [SAML2Bind] for the transmission of attribute query and response messages.

8.2 Message Content

Identity Provider and Service Provider implementations MUST support <*saml2p:AttributeQuery*> requests with accompanying <*saml2p:Response*> and corresponding responses.

Support for other assertion request types is OPTIONAL.

9 Referenser

[RFC2616] RFC 2616, "Hypertext Transfer Protocol – HTTP/1.1", June 1999.

[RFC2818] RFC 2818, "HTTP Over TLS", May 2000

[IdPDisco] OASIS Committee Specification, Identity Provider Discovery Service Protocol and Profile, March 2008.

[InCommon] "InCommon Federation SAML 2.0 Profiles", InCommon Federation Technical Advisory Committee. February 2010

[MACEAttr] MACE-Dir Working Group Publication, "MACE-Dir SAML Attribute Profiles", April 2008.

[MetaAttr] OASIS Committee Specification, "SAML V2.0 Metadata Extension for Entity Attributes Version 1.0", August 2009.

[MetaIOP] OASIS Committee Specification, "SAML V2.0 Metadata Interoperability Profile Version 1.0", August 2009.

[SAML2Core] OASIS Standard, "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0", March 2005.

[SAML2Meta] OASIS Standard, "Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0", March 2005.

[SAML2Bind] OASIS Standard, "Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0", March 2005.

[SAML2Prof] OASIS Standard, "Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0", March 2005.

Anvisningstjänst

Teknisk specifikation för anvisningstjänst inom infrastukturen för Svensk e-legitimation

1 Sammanfattning

Detta dokument utgör teknisk specifikation för en anvisningstjänst (Discovery Service) som upprättas inom ramen för infrastukturen för Svensk e-legitimation.

Anvisningstjänstens funktion är att underlätta användarens val av e-legitimation vid utnyttjande av en e-tjänst.

Genom anvisningstjänsten ges användaren en möjlighet att informera om vilken e-legitimation användaren brukar använda så att ett förenklat gränssnitt, där användarens tidigare använda e-legitimation kommer upp som förvalsalternativ, kan skapas vid legitimering. Användarens tidigare val av e-legitimationer kommuniceras inte med e-tjänsten utan hanteras uteslutande mellan användaren och anvisningstjänsten genom en s.k. ”cookie” som lagras i användarens webbläsare. Denna cookie innehåller ingen information om användarens aktiviteter eller identitet och anvisningstjänsten har ingen information om vilken individ som utnyttjar tjänsten för att välja e-legitimation. Genom att lagra senaste val lokalt hos användaren genom denna metod behöver inte anvisningstjänsten lagra någon information om användares senaste val i anvisningstjänsten mellan användarens nyttjande av e-tjänster.

Anvisningstjänsten tillhandahålls i två utförande. I det ena utförandet överförs användaren till anvisningstjänsten som tillhandahåller gränssnitt för användarens val av e-legitimation. I det andra utförandet tillhandahåller e-tjänsten ett eget gränssnitt mot användaren genom en dynamisk webbsida som automatiskt anpassas till tidigare val av e-legitimation genom kommunikation med anvisningstjänsten.

I detta utförande är inte tillgång till anvisningstjänsten kritisk. Om anvisningstjänsten inte är tillgänglig innebär detta bara att användaren inte får upp sin e-legitimation som förval. En e-tjänst som tillämpar det första utförandet är dock beroende av att

anvisningstjänsten är tillgänglig för användaren för att en legitimering ska kunna genomföras.

I inget utförande är det kritiskt att användaren accepterar en cookie från anvisningstjänsten. En användare som inte accepterar att lagra en cookie, eller av andra orsaker inte har en cookie med förvalsinformation lagrad, får göra ett förnyat val.

E-tjänster måste inte använda anvisningstjänsten. Ett tredje alternativ för e-tjänsten är att skapa en helt egen dialog med användaren för val av e-legitimation genom att hämta nödvändig information från federationens metadata (federationsregistret). Detta alternativ kan även kombineras med alternativ 2 så att gränssnittet fungerar även om anvisningstjänsten av någon anledning inte är tillgänglig. Det är rekommenderat att alltid använda anvisningstjänsten i någon form där detta är möjligt för att kunna erbjuda användarna ett förenklat gränssnitt.

2 Definitioner och förkortningar

Följande begrepp används som synonymer

Begrepp	Synonymer
Anvisningstjänst	Discovery Service
E-tjänst	E-tjänsteleverantör
Identitetsutfärdare	Identity Provider

Förkortningar

Förkortning	Betydelse
DS	Discovery Service (Anvisningstjänst)
SP	Service Provider (E-tjänst)
IdP	Identity Provider (Identitetsutfärdare)

3 Förutsättningar

Denna specifikation är uteslutande definierad för Anvisningstjänst inom ramen för Infrastukturen för Svensk e-legitimation. Anvisningstjänstens funktion förutsätter att varje typ av e-legitimation som representeras av ett unikt namn i användargränssnitt för val av e-legitimation representeras av en specifik IdP och att denna unika relation mellan e-legitimation och IdP är dokumenterad i federationens metadata (federationsregistret).

Anvisningstjänsten måste kunna identifiera en och endast en Identitetsutfärdare utifrån det val av e-legitimation som användaren gör. Detta innebär att användaren aldrig först ska behöva välja e-legitimation för att sedan behöva göra ytterligare att val av vilken Identitetsutfärdare som ska utföra autentisering.

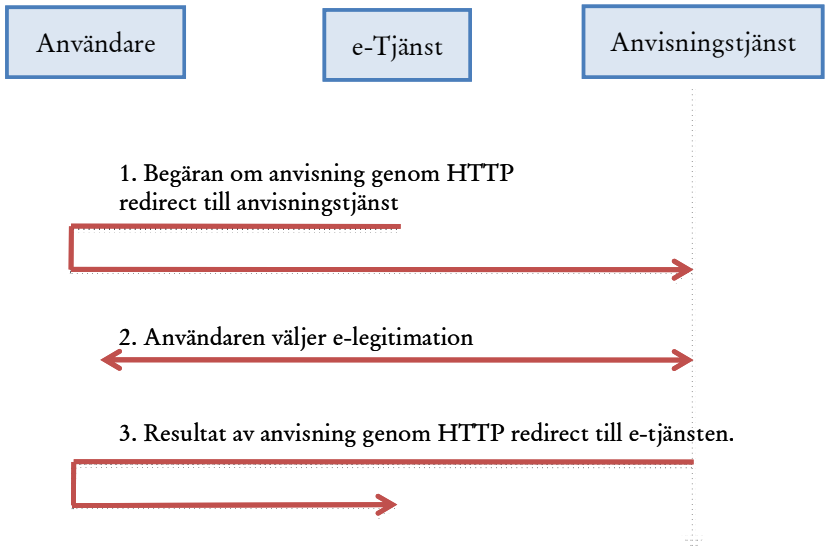
4 Utförandealternativ

Anvisningstjänst som upprättas enligt denna specifikation ska tillhandahålla tjänst till e-tjänster som underlättar processen att fastställa vilken Identitetsutfärdare som ska autentisera en användare. Anvisningstjänsten ska erbjuda tjänsten i två utförande avsedda för

1. E-tjänster som inte tillhandahåller eget gränssnitt för användarens val av e-legitimation, och
2. E-tjänster som själva tillhandahåller att gränssnitt för användarens val av e-legitimation.

5 Utförande 1 – e-tjänst utan gränssnitt för val av e-legitimation

Detta utförande av Avisningstjänsten ska implementeras enligt SAML ”Identity Provider Discovery Service Protocol and Profile” [SAML-Discovery].



Enligt detta utförande sker anvisning av Identitetsutfärdare enligt följande förfarande:

1. E-tjänsten skickar en begäran om anvisning som en HTTP Get request enligt [SAML-Discovery] till Anvisningstjänsten i en HTTP redirect.
2. Anvisningstjänsten (DS) returnerar en webbsida där användaren ges möjlighet att välja e-legitimation. Anvisningstjänsten använder federationens metadata för att fastställa vilken Identitetsutfärdare som användarens e-legitimation är kopplad till i federationen.
3. Anvisningstjänsten returnerar uppgift om Identitetsutfärdare (IdP) som en HTTP Get request enligt [SAML-Discovery] till e-tjänsten i en HTTP redirect.

Utformning av webbgränssnitt där användaren väljer e-legitimation är inte specificerad.

Avisningstjänsten bör erbjuda användarens klient en cookie enligt [rfc2965] för att spara användarens val av e-legitimation för att underlätta framtida val av e-legitimation. Denna cookie ska vara identisk med den cookie som användaren erbjuds i utförande 2 (se avsnitt 6)

Följande avgränsningar gäller för implementering av [SAML-Discovery]

Parameter	Avgränsning
isPassive	Måste vara satt till ”false” i alla request till anvisningstjänsten
returnIDParam	Ska utelämnas från request till anvisningstjänsten (Anvisningstjänsten returnerar ett ”entityID”)
return	Denna parameter ska alltid medfölja en request till anvisningstjänsten och ska identifiera den URL som anvisningstjänsten ska returnera användaren till efter val av e-legitimation.

Om anvisningstjänsten erhåller en request som bryter mot någon av reglerna ovan, eller om anvisningstjänsten av annan anledning inte kan fastställa vilken Identitetsutfärdare som användaren ska anvisas till för autentisering, så ska anvisningstjänsten returnera användaren till e-tjänsten till den URL som anges i returnIDParam, men utan att returnera någon entityID för Identitetsutfärdare.

5.1 Krav på kontroll av mottagande e-tjänst

För att förhindra att någon som inte är en registrerad e-tjänst kan vidarebefordra användaren till anvisningstjänsten för att utröna användarens val av e-legitimation så måste anvisningstjänsten kontrollera att e-tjänstens internetadress som specificeras av ”return” parametern överensstämmer med en internetadress för en legitim e-tjänst i metadataregistret.

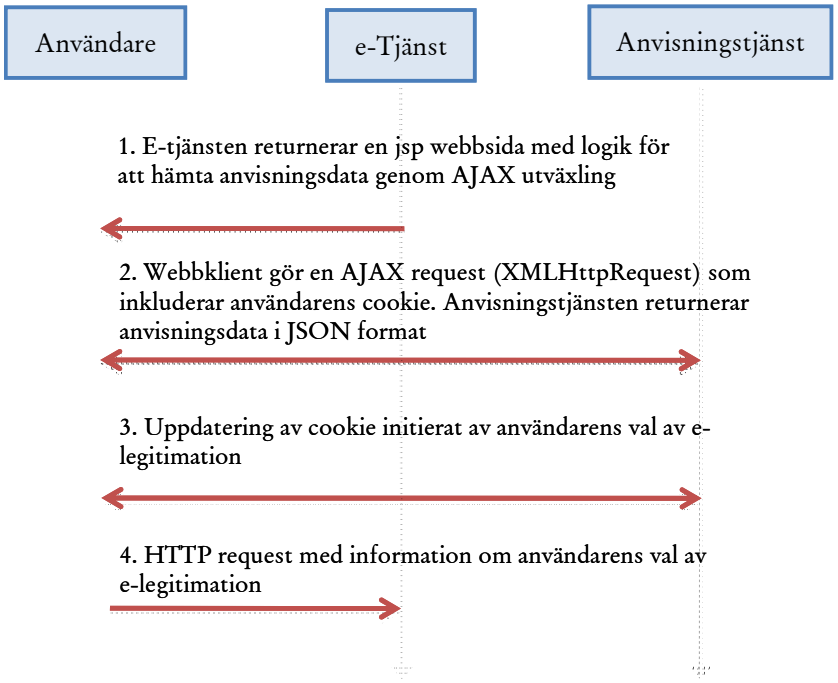
6 Utförande 2 – e-tjänst med eget gränssnitt för val av e-legitimation

Det saknas i dag någon standardiserad lösning för en Anvisningstjänst som tillhandahålls till e-tjänster som själv implementerar gränssnittet för val av e-legitimation. Den lösning som presenteras i detta avsnitt utgör ett grundförslag som beskriver en av många möjliga lösningar.

I detta utförande tillhandahåller e-tjänsten en dynamisk webbsida (Java Server Pages) för val av e-legitimation som implementerar AJAX (Asynchronous JavaScript and XML) kommunikation med anvisningstjänsten för att hämta hem anvisningsinformation i JSON (JavaScript Object Notation) format.

Då användarens webbsida hämtar JSON informationen genom AJAX anrop så skickas även användarens cookie med förvalsinformation till anvisningstjänsten som därmed anpassar den returnerade JSON informationen efter användarens förval.

Java script i den dynamiska webbsidan anpassar användarens gränssnitt för val av e-legitimation baserat på JSON informationen från anvisningstjänsten.



Enligt detta utförande sker anvisning av Identitetsutfärdare enligt följande förfarande:

1. E-tjänsten tillhandahåller en dynamisk webbsida (Java Server Pages) med AJAX instruktioner

2. Användarens webbläsare gör ett AJAX anrop (XMLHttpRequest) för att hämta ett JSON objekt med anvisningsdata. Användarens cookie med information om användarens preferenser (om sådan finns) medföljer anropet. JSON objektet anpassas av anvisningstjänsten utifrån användarens preferenser. Användarens gränssnitt skapas utifrån mottagen information från anvisningstjänsten.
3. Användarens val initierar uppdatering av användarens cookie med information om användarens senaste val.
4. Ett HTTP request skickas till e-tjänsten med information om vilken Identitetsutfärdare som ska legitimera användaren.

6.1 Cookie format och användning

Cookie med information om användarens preferenser konsumeras endast av anvisningstjänsten. Det är upptill anvisningstjänsten att utforma cookie så att den tillhandahåller nödvändig information men ska utformas i enlighet med RFC 2965 [rfc2965].

För det fall en användare använder flera e-legitimationer, eller samma webbläsare används av flera användare med olika e-legitimationer, ska en cookie kunna lagra information om flera valda e-legitimationer.

Livslängd för cookie ska sättas så att den består mellan en typisk användares utnyttjande av e-tjänster. Detta bör inte överstiga en tid av tre månader.

En cookie bör innehålla information om tidpunkt för senaste val av respektive e-legitimation så att ett förval kan tas bort om denna e-legitimation inte används mer men att cookien ändå förnyas regelbundet genom val av annan e-legitimation.

6.2 Format för JSON data

Format för JSON data måste följa ett väl definierat format så att e-tjänsters dynamiska webbsidor kan tolka informationen från anvisningstjänsten och dynamiskt uppdatera användarens gränssnitt.

Detta format bör utarbetas och vid behov uppdateras av e-legitimationsnämnden i samråd med federationens e-tjänster.

7 Referenser

[SAML-Discovery]	Identity Provider Discovery Service Protocol and Profile, OASIS Committee Specification 01, 27 March 2008
[HTTP]	RFC 2616, ”Hypertext Transfer Protocol -- HTTP/1.1”, IETF Draft Standard, June 1999.
[TLS]	RFC 5246, ”The Transport Layer Security (TLS) Protocol Version 1.2”, IETF Proposed standard, August 2008.
[RFC2965]	RFC 2965, ”HTTP State Management Mechanism”, IETF Proposed Standard, October 2000.

Central signeringstjänst

Central signering för myndigheters e-tjänster med stöd av identitetsfederationen för svensk e-legitimation

1 Sammanfattning

Detta dokument beskriver en möjlig utformning av en svensk central signeringstjänst som kan användas av svenska myndigheter och offentlig sektor för att låta användare av Svensk e-legitimation signera elektroniska handlingar.

Den lösning som beskrivs är avsedd att om möjligt skapa kvalificerade elektroniska signaturer enligt svensk lag (2000:832) om kvalificerade elektroniska signaturer. Syftet är inte att ta ställning till om detta är ett nödvändigt krav för svenska myndigheter, utan för att beskriva vad som krävs för att detta ska kunna realiseras.

Materialet i detta dokument har som syfte att fungera dels som beslutsunderlag men även som arkitekturförslag för ett implementeringsprojekt. Ytterligare tekniska specifikationer krävs för en komplett specificerad lösning.

En viktig slutsats är att de krav som identifierats för en signeringstjänst inte kan uppfyllas av en och samma utförande av signeringstjänsten. Därför beskrivs två alternativa utföranden med respektive fördelar och nackdelar. Ytterligare utredning av myndigheters och offentlig verksamhets behov krävs för att besluta om inget, ett eller båda dessa alternativa utföranden ska implementeras.

Som ytterligare del i ett sådant beslutsunderlag bör tillfogas myndigheters och offentlig verksamhets behov av elektroniska signaturfunktioner där detta ställs mot alternativa lösningar, som exempelvis att en användare godkänner information enbart genom legitimering, utan att signera informationen.

För det fall att inget av de föreslagna alternativen bedöms vara genomförbara förs en diskussion om möjliga övriga alternativ med begränsad funktionalitet som kan realiseras inom ramen för en federativ infrastruktur för identifiering.

Denna tekniska del av utredningen av en signeringstjänst tar inte ställning till hur många signeringstjänster som ska kunna finnas, affärsmodeller eller olika konkurrensaspekter.

2 Terminologi

2.1 Synonymer

Följande termer används med gemensam innebörd:

- elektronisk underskrift, underskrift, elektronisk signatur, signatur och avancerad elektronisk signatur
- dokument, handling och information

2.2 Begrepp

I detta dokument används följande begrepp:

Begrepp	Betydelse
Hash	Även ofta benämnt ”fingeravtryck” är en kontrollsekvens av data som beräknas från ett dokument med hjälp av en hashalgoritm. Hashalgoritmer är så beskaffade att ett varje dokument har ett unikt hash. När ett dokument signeras så är det dokumentets hash som signeras och inte själva dokumentet.
Elektronisk signatur	Data, knutet till ett elektroniskt dokument som kan användas för att verifiera vem som signerat dokumentet och att dokumentet inte förvanskats. **Not:** Det generella begreppet ”elektronisk signatur” används i detta dokument ekvivalent med begreppet ”avancerad elektronisk signatur” enligt signaturlagen [Sig].
Certifikat	Data som utfärdats till en användare och signerats av en certifikatutfärdare vars användningsområde i detta dokument är begränsat till att verifiera en användares signaturer. Certifikatet innehåller information om användarens identitet, nyckel för att verifiera användarens signaturer samt information om certifikatets användningsområde. **Not:** Det finns certifikat som har andra användningsområden än signaturverifiering men i detta

	dokument diskuteras endast certifikat som används för att verifiera innehavarens elektroniska signaturer.
Kvalificerat certifikat	Ett certifikat som utfärdats som kvalificerat certifikat i enlighet med signaturlagen [Sig]. Kvalificerade certifikat ställer särskilda krav på utfärdare och dess ansvar för utfärdade certifikat
Säker signeringsfunktion	En kryptografisk modul för skapande av elektroniska signaturer som uppfyller signaturlagens [Sig] krav på en ”säker anordning för signaturframställning”.
Kvalificerad elektronisk signatur	En elektronisk signatur enlig definition ovan som framställts av en säker signeringsfunktion och som kan verifieras med ett kvalificerat certifikat
Tidsstämpel	Kryptografiska data knutet till ett elektroniskt dokument som intygar att ett dokument existerade i ett specifikt utförande vid en specificerad tidpunkt. **Not:** Det dokument som tidsstämplas innefattar vanligtvis även en elektronisk signatur. På så sätt intygar tidsstämpeln såväl att dokument som dess signatur existerade vid den specificerade tidpunkten.

3 Nulägesanalys

I dagsläget kan myndigheter låta en användare signera elektroniska handlingar med sin e-legitimation. Vid detta förfarande signerar användaren den elektroniska handlingen lokalt i sin dator med hjälp av sin egen e-legitimation. E-tjänsteleverantören ombesörjer kommunikation med klienten som resulterar i att användaren accepterar och signerar en elektronisk handling.

Inom den så kallade ”Infratjänsten” tillhandahålls ett gemensamt gränssnitt OSIF (Offentligt Sammanhållen Identifierings Funktion) mot e-legitimationsutfärdarna för att underlätta legitimering och signering med användarnas e-legitimation. Vid tillämpning av OSIF-protokollet för signering skickas den information som ska signeras först till OSIF-servern för att anpassas till respektive typ av klientprogramvara som ombesörjer signering i användarens dator. Om denna OSIF-server tillhandahålls av en extern infratjänst så innebär detta att alla dokument som signeras passerar en central tjänst. I ett senare led av signeringen verifierar samma OSIF-server att användarens signatur överensstämmer med den information som e-tjänsten begärde få signerad.

Även om OSIF-protokollet är gemensamt för samtliga aktuella utfärdare av e-legitimationer så skickas olika data i skilda dataformat beroende på vilken klientprogramvara som installerats i användarens dator. Detta innebär att dagens tillämpning av OSIF-protokollet är direkt knuten till den funktionalitet och de dataformat som nuvarande klientprogramvaror kräver.

Elektronisk signering enligt denna modell innebär sammanfattningsvis följande:

- Signeringen sker i användarens dator
- Endast de e-legitimationer som är certifikatbaserade kan användas för signering. Andra former av e-legitimationer, ex kryptografiska kod-dosor, kan inte användas.
- Användare måste ladda hem en särskild programvara som ombesörjer signering av information som skickas från e-tjänsten, en s.k. klientprogramvara. Nuvarande protokoll för att understödja e-tjänsters hantering av legitimering och signering är knuten till nuvarande klientprogramvaror.
- Verifiering av användares elektroniska signatur förutsätter teknisk anpassning mot samt avtal med e-legitimationsutfärdarna. Den information om spärrning av certifikat som krävs för en oberoende verifiering av signatur, är inte öppet tillgänglig. Detta innebär exempelvis att signaturer inte kan verifieras av utländska aktörer som saknar avtal med e-legitimationsutfärdarna.
- Vid tillämpning av OSIF-protokollet mot en central OSIF-server så görs handlingen som ska signeras tillgänglig för en central tjänst.

I en framtida infrastruktur för Svensk e-legitimation som bygger på en SAML baserad federativ modell, innebär detta en rad problem:

- Den nuvarande modellen för signering är i grunden knuten till dagens leverantörer av e-legitimationer och kan inte med automatik utökas till att omfatta nya typer av e-legitimationer, särskilt inte de där användaren inte innehar certifikat för signering. Det finns visserligen leverantörer inom dagens Infratjänst som kan stödja legitimering och signering även med andra utfärdare av certifikatbaserade e-legitimationer, men detta kräver tillpassningar i de e-tjänster som ska acceptera e-

legitimationerna vilket försvårar anslutning av nya e-legitimationer.

- Den nuvarande modellen bygger på infrastruktur-komponenter och tjänster som inte återfinns i den federativa modellen. Fortsatt signering enligt nuvarande modell innebär därför att man tillämpar två olika infrastrukturer med olika affärsmodeller, dvs. en federativ modell för identifiering och den nuvarande infrastrukturen för signering.
- Den nuvarande modellen tillåter inte att vem som helst, som inte har avtal med e-legitimationsleverantörerna, kan verifiera elektroniska signaturer. Dessa signaturer kan därför inte användas exempelvis vid internationell informationsutväxling.

De mest signifikanta skillnaderna mellan en central signeringstjänst enligt avsnitt 0 och dagens modell och är att:

- Användaren behöver inte installera någon specialkonstruerad klientprogramvara. Hela processen att signera kan utföras med en vanlig webbläsare.
- Innehavare av alla typer av e-legitimationer ges möjlighet att skriva under elektroniskt. Även användare som inte innehar certifikatbaserade e-legitimationer[1].
- Nya e-legitimationsutfärdare kan adderas till infrastrukturen utan att tillpassning av protokoll och implementering i e-tjänster.
- Alla enheter som kan hantera en e-legitimation och en webbläsare kan användas för signering, ex mobiltelefoner.
- Signaturer kan skapas som kvalificerade elektroniska signaturer och signaturerna kan verifieras av oberoende tredje part som inte har avtal med e-legitimationsutfärdarna.
- Även de som inte har förlitandeavtal gentemot e-legitimations-utfärdarna kan verifiera underskriften på signerade handlingar.

[1] Användare använder endast sin e-legitimation för att legitimera sig mot signeringstjänsten som utför själva signeringen. Det som är avgörande är den tillitsnivå som e-legitimationen erbjuder, inte vilken teknik den tillämpar för legitimeringen.

4 Central signering och kvalificerade elektroniska signaturer

En central fråga för beslut om genomförande är om en central signeringstjänst kan uppfylla signaturlagens krav på en kvalificerad elektronisk signatur.

De mest relevanta kraven i detta hänseende utgörs av 3 § signaturlagen gällande ”Säkra anordningar för signaturframställning”

> **3 §** En anordning för signaturframställning som anges vara säker ska säkerställa att signaturen är tillfredsställande skyddad mot förfalskning.
>
> Anordningen ska även säkerställa att signaturframställningsdata
> 1. i praktiken kan förekomma endast en gång,
> 2. med rimlig säkerhet inte kan härledas, och
> 3. på ett tillfredsställande sätt kan skyddas av den behörige undertecknaren, så att andra inte kan komma åt eller använda dem.
>
> Anordningen får inte förändra de uppgifter som ska signeras elektroniskt eller hindra att de presenteras för undertecknaren före den elektroniska signeringen.

Den viktigaste frågeställningen i detta sammanhang är om signaturframställningsdata (privat signeringsnyckel) i en central signeringstjänst kan skyddas av den behörige undertecknaren, så att andra inte kan komma åt eller använda dem.Uppfyllelse av detta och övriga krav underlättas av om användarens privata signeringsnyckel, så som föreslås, endast existerar vid signeringstillfället i en för ändamålet säker hårdvara samt att signeringsnyckeln förstörs direkt efter användning. En sådan hårdvara utformasäven på ett sådant sätt att signaturnyckeln inte kan läsas ut ur hårdvaran.

Vid ett sådant förfarande bygger kravuppfyllelse på att signeringssystemet på ett betryggande sätt kan legitimera användaren vid signeringstillfället och därmed på ett rimligt sätt säkerställa att ingen annan än användaren själv kan signera i användarens namn med hjälp av signeringstjänsten.

För att belysamöjligheterna för en central signeringstjänst att tillgodose detta krav är det relevant att jämföramöjligheterna med en central signeringslösning i förhållande till en traditionell lokal lösning där själva signaturframställningen sker i användarens dator eller motsvarande lokal enhet (ex mobiltelefon).

Båda lösningarna kräver att användaren som ska signera har tillgång till sin e-legitimation. Skillnaden ligger i att lokal signering bygger på att användarens datormiljö ger ett tillförlitligt skydd mot missbruk medan den centrala signeringstjänsten bygger på att den centrala signeringsmiljön kan ge ett skydd i minst motsvarande grad.

Största hotet mot användarens lokala miljö utgörs av att skadlig kod (virus, trojaner, maskar mm) som användare installerat av oaktsamhet, eller som på annat sätt infiltrerat användarens dator kan ha potential att missbruka användarens signeringsfunktion. Detsamma gäller dock även i motsvarande grad en fientlig programvaras möjlighet att missbruka användarens e-legitimation vid legitimering mot en signeringstjänst. Dock finns många fler möjligheter att uppdaga problem av detta slag vid en central signeringstjänst, dels genom att legitimering vid signering loggas både av identitetsutfärdare som utfärdar identitetsintyget och av signeringstjänsten som legitimerar användaren samt möjlighet att bekräfta signering genom separat kanal, ex genom e-post eller SMS.

Följande tabell redovisar en samanställning av olika säkerhetsaspekter och hot samt en uppskattning av vilken lösning (lokal eller central signering) som erbjuder fördelar (+) respektive sämre förutsättningar (-).

	Fördelar och nackdelar	
Uppgift	**Lokal signering**	**Central signering**
Beroende av en trovärdig central signeringsfunktion	+	-
Hot från virus och annan fientlig programvara i användarens dator	-	+ (p.g.a. bättre spårbarhet)
Förhindrande av attlagrad signeringsnyckel missbrukas	-	+ (raderas efter signering)
Möjlighet att spåra vad som hänt genom loggar och trovärdig registrering av tidpunkt för signering	-	+
Möjlighet att spärra enskilda	-	+

signaturer vid missbruk		
Tredje parts bevittnade av användarens acceptans att signera presenterad handling	-	+ vid alternativ 1
Möjlighet att underrätta användaren om signering genom meddelande i separat kanal	-	+

4.1 Internationella krav

Tjänstedirektivet från EU kommissionen ställer krav på elektroniska tjänster som ska verka över landsgränser. Inom ramen för tjänstedirektivet kan medborgare behöva kommunicera elektroniskt signerade handlingar. Inom ramen för EU kommissionens stödjande aktiviteter för att underlätta utbyte av elektroniskt signerad information i samband med tjänstedirektivet har EU kommissionen i samverkan med medlemsstaterna utfärdat ett kommittologibeslut (”Kommissionens Beslut 2010/425/EU av den 28 juli 2010 om ändring av beslut 2009/767/EG”). I artikel 1 av detta beslut (som står oförändrat sedan 2009/767/EG) framgår följande:

> ”Om det är motiverat på grundval av en ändamålsenlig bedömning av berörda risker och i enlighet med artikel 5.1 och 5.3 i direktiv 2006/123/EG, får medlemsstaterna kräva att tjänsteleverantören för fullgörandet av vissa förfaranden och formaliteter genom de gemensamma kontaktpunkterna i enlighet med artikel 8 i direktiv 2006/123/EG ska använda avancerade elektroniska signaturer baserade på ett kvalificerat certifikat, **med eller utan en säker anordning för skapande av signaturer**, enligt vad som fastställs och regleras genom direktiv 1999/93/EG.”

Genom detta beslut framgår tydligt att grunden för internationell samverkan i fråga om signerade handlingar utgörs av elektroniska signaturer baserat på kvalificerade certifikat men att kravet på en säker anordning för skapande av signaturer inte är obligatoriskt.

Man kan därför förvänta sig at en lösning för elektroniska signaturer med central signeringstjänst enligt detta dokument kan fylla in viktig funktion inom ramen för införande av

tjänstedirektivet även om vi i Sverige inte väljer att godkänna den centrala signeringstjänsten som en säker anordning för skapande av signaturer i enlighet med avsnitt 4.

De signaturer som skapas inom ramen för dagens infratjänst kan endast verifieras av de myndigheter som är anslutna till infratjänsten (har förlitande avtal med e-legitimationsutfärdarna och därmed tillgång till aktuell spärrinformation). Detta gör dagens signaturlösning, eller motsvarande lösning där dokument signeras lokalt i användarens dator med e-legitimationer från dagens ramavtalsleverantörer, olämplig för utväxling av elektroniskt signerade handlingar inom ramen för internationell samverkan.

EN stor fördel i detta hänseende med en central signeringstjänst kombinerat med en federativ infrastruktur för identifiering är främst om befintliga e-legitimationer signaturerna kan användas internationellt genom att signaturerna kan kopplas till ett kvalificerat certifikat samt genom att certifikatens spärrinformation är öppet tillgänglig.

En viktig förutsättning för detta är att signeringstjänstens certifikatutfärdarfunktion kan godkännas och registreras hos PTS och att tjänsten tas med i Sveriges lista över certifikatutfärdare. Vad gäller möjligheten att ge ut kvalificerade certifikat baserat på nycklar som genererats centralt av certifikatutfärdaren, eller att identifiera den som ansöker om ett certifikat med hjälp av medel som i sig inte utgörs av kvalificerade certifikat så finns klart stöd från både internationell standard såväl som implementationer i Europa. Den allmänt accepterade standarden för utgivning av kvalificerade certifikat ETSI TS 101 456 [TS101456] ger tydligt utrymme för en sådan utfärdandeprocess.

5 Krav

Följande kravlista har utgjort grunden för utformning av en signeringstjänst. Kravlistan är utarbetad inom ramen för utredningen om bildandet av en e-legitimationsnämnd och är resultatet av såväl diskussioner inom utredningen som diskussioner med representanter från myndigheter och offentlig verksamhet.

- Användarna ska kunna signera dokument med en standard dator och en standard webbläsare som kör under marknadens vanligt

förekommande operativsystem (Windows, Mac OSX, Linux, Symbian, Android, iPhone, Blackberry, m.m.).

- E-tjänster ska kunna få tillgång till signeringstjänsten för att låta användare underteckna elektroniska dokument med minimala anpassningar av sin e-tjänst.
- E-tjänster måste kunna signera dokument som innehåller data enligt interna format som inte kan visas direkt i användarens webbläsare.
- E-tjänster måste kunna signera data som inte delges annan än användaren själv. I dessa fall får inte den signerade handlingens innehåll överföras till signeringstjänsten.
- Anslutna e-tjänster ska inte behöva befatta sig med skapande av elektronsikt signerade handlingar. Följande hantering ska kunna överlåts till signeringstjänsten:
  - Presentation av handlingen som ska signeras
  - Presentation av innebörden av att signera
  - Användarens godkännande av att signera handlingen
  - Utfärdande av signeringscertifikat[2]
  - Signering av elektronisk handling
  - Tidstämpling av dokument och signatur
  - Framställa signerad handling enligt överenskommet signaturformat
- Signaturen ska om möjligt kunna uppfylla lagens krav på en kvalificerad elektronisk signatur.

[2] Det är nödvändigt att signeringstjänsten utfärdar certifikat eftersom dessa kopplas till den signeringsnyckel som signeringstjänsten skapar för användaren. Dessa certifikat konkurrerar inte med andra certifikat på marknaden då dess enda funktion är att användas för att verifiera den specifika signatur som skapas. Eftersom signaturnyckeln förstörs efter signering kan certifikatet inte kopplas till eller användas för andra ändamål.

6 Användningsfall

Användningsfallen nedan är hypotetiska framtidsscenarier och utgör inte nödvändigtvis en korrekt beskrivning av de myndigheters e-tjänster som nämns. Dess syfte är uteslutande att beskriva situationer som belyser olika tillämpningar av en central signeringstjänst.

6.1 Signering av handling från e-tjänst som presenteras av signeringstjänsten

Anna besöker Skatteverkets webbplats för att deklarera. För att komma åt deklarationstjänsten loggar Anna in på skatteverkets webbplats med sin e-legitimation.

När alla uppgifter matats in vill Anna godkänna sin deklaration. Skatteverkets webbplats skapar då ett elektroniskt dokument som innehåller Annas deklaration med alla lämnade uppgifter införda varefter Anna dirigeras om till signeringstjänsten.

I signeringstjänsten får Anna information av att Skatteverket vill att Anna ska skriva under sin deklaration elektroniskt. Deklarationen som sammanställts av Skatteverket visas upp för Anna som kan gå igenom uppgifterna med sin webbläsare.

Anna väljer funktionen ”Jag skriver under” hos signeringstjänsten varvid Anna dirigeras till sin Identitetsutfärdare för legitimering för underskrift. Anna godkänner underskriften genom att legitimera sig med sin e-legitimation.

Dokumentet signeras av signeringstjänsten och förses med en kvalificerad elektronisk signatur enligt det signaturformat som e-tjänsten begärt.

Anna returneras tillbaks till skatteverkets webbtjänst (via signeringstjänsten) som meddelar att deklarationen nu är underskriven.

6.2 Signering av handling från e-tjänst som presenteras av e-tjänsten

Johan besöker Försäkringskassans webbplats och loggar in för att ansöka om föräldrapenning.

Försäkringskassans webbplats presenterar information som ska undertecknas varvid Johan accepterar att skriva under elektroniskt med sin e-legitimation genom funktionen ”Jag skriver under”.

Johan dirigeras till sin Identitetsutfärdare som begär legitimering för underskrift. Johan godkänner underskrift genom att legitimera sig med sin e-legitimation.

Johan returneras till Försäkringskassan med en signatur som framställts av signeringstjänsten. Försäkringskassan meddelar att ansökan har signerats.

6.3 Signering av handling vald av användaren

Petter ska signera en ansökan om tillstånd att få leverera tjänster i Portugal. Petter har fyllt i ett formulär som sparats i PDF format.

Petter kontaktat signeringstjänsten och presenterar det dokument som ska signeras samt väljer att dokumentet ska tidsstämplas.

Signeringstjänsten presenterar via webbgränssnitt det dokument som kommer att signeras. Petter verifierar dokumentet och väljer funktionen ”Jag skriver under” varvid Petter dirigeras till sin Identitetsutfärdare för legitimering för underskrift. Petter godkänner underskriften genom att legitimera sig med sin e-legitimation.

Petter returneras till signeringstjänsten där Petter får ladda hem det signerade dokumentet som försetts med en kvalificerad elektronisk signatur samt en kryptografisk tidsstämpel.

Utförandealternativ

För att uppfylla alla funktionella krav måste signeringstjänsten ha utförandealternativ som både kan hantera fall där presentation av information som ska signeras hanteras av signeringstjänsten och fall där detta hanteras av e-tjänsten.

I detta avseende innefattar hanteringen av information som ska signeras:

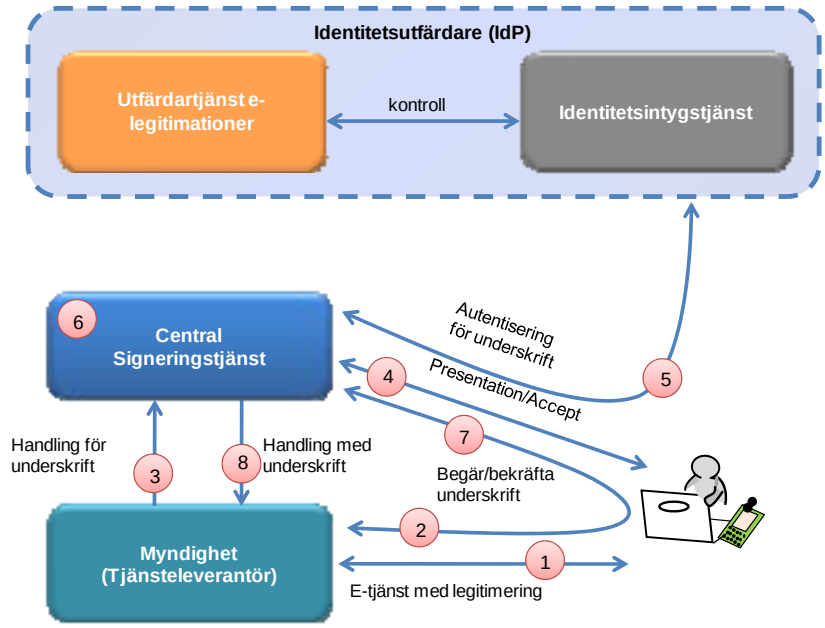
- Presentation av information som ska signeras
- Presentation av innebörden av att signera (detta kan framgå av informationen som signeras eller genom annan information)
- Funktion genom vilken användaren kan acceptera

För att uppfylla dessa krav presenteras två olika utförandealternativ som presenteras i detta avsnitt.

Utförandealternativen representerar främst skillnader mellan användningsfallen i avsnitt 6.1 och 6.2. Användningsfallet i avsnitt 6.3, där handlingen som signeras väljs av användaren, går att realisera inom ramen för båda alternativen genom att skapa en tjänst där användaren kan ladda upp ett dokument som ska signeras. Denna tjänst kan fylla funktionen av en e-tjänst i enlighet med både alternativ 1 och alternativ 2.

6.4 Alternativ 1 – Dokument som ska signeras hanteras av signeringstjänsten

I detta alternativa utförande överlåter e-tjänsten hela signeringsförfarandet till signeringstjänsten.



4. Användaren identifierar sig för en e-tjänst genom sin e-legitimation och utnyttjar en tjänst som kräver användarens elektroniska underskrift (signatur)
5. Användaren överförs till signeringstjänsten med en begäran om signering från e-tjänsten.
6. Signeringstjänsten inhämtar elektronisk handling för underskrift från e-tjänsten.
7. Signeringstjänsten presenterar handlingen som ska signeras för användaren och användaren accepterar att signera
8. Användaren överförs till sin identitetsutfärdare med begäran om legitimering. Användaren legitimeras med stöd av sin e-

legitimation och ett identitetsintyg returneras till signeringstjänsten.

9. Signeringstjänsten skapar användarens nyckelpar, utfärdar ett certifikat för användaren samt signerar den elektroniska handlingen. Vid behov tidsstämplas handlingen. Handling med underskrift skapas genom att foga samman handlingen med certifikat, signatur och eventuell tidsstämpel enligt efterfrågat signaturformat.
10. Användaren returneras till e-tjänsten med en bekräftelse på att handlingen är underskriven.
11. E-tjänsten hämtar hem den signerade handlingen från signeringstjänsten från angiven plats.

Genom detta förfarande kan en e-tjänst få tillgång till en signeringsfunktion som enkelt kan integreras med en e-tjänst med minimala insatser. En viktig fördel är att en tredje part (Signeringstjänsten) står som garant för att användaren verkligen accepterat att signera handlingen och att den information som användaren fått presenterat för sig och accepterat överensstämmer med den signatur som skapats. En annan fördel är att signeringstjänsten kan hantera alla de olika signaturformat som kan komma i fråga, särskilt om signaturen ska kunna användas/verifieras internationellt.

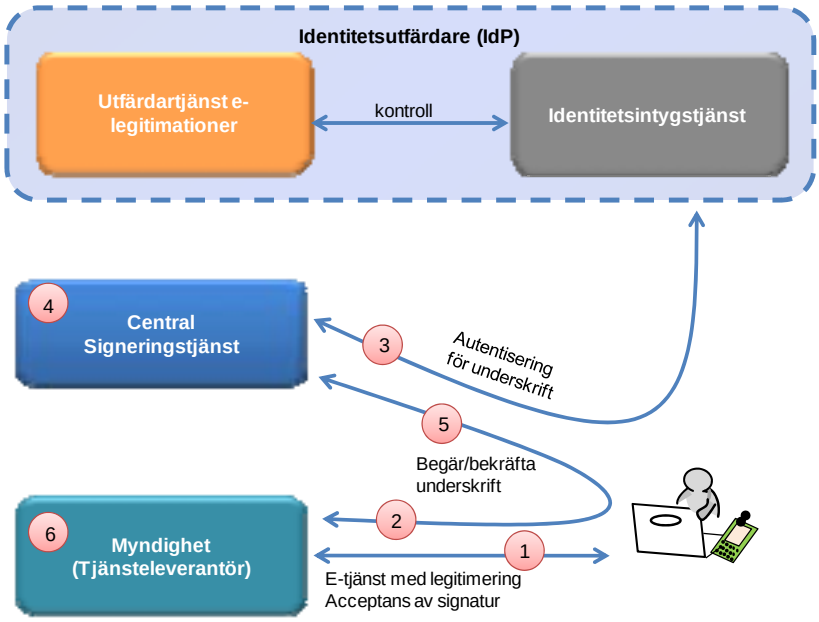
Den stora nackdelen med detta alternativ är att den handling som ska signeras måste hanteras av signeringstjänsten. Detta alternativ kan därför inte tillämpas om:

- E-tjänsten av något skäl inte kan eller får lämna ut handlingen som ska signeras till signeringstjänsten
- Handlingen som ska signerats inte förekommer i ett format som signeringstjänsten kan presentera för användaren på ett för användaren meningsfullt sätt endast med stöd av användarens webbläsare.

Då någon av dessa omständigheter gäller för signeringen så måste alternativ 2 tillämpas.

6.5 Alternativ 2 – Dokumentet som ska signeras hanteras av e-tjänsten

I detta alternativa utförande av signeringstjänsten hanterar signeringstjänsten inte den elektronisk handling som ska signeras. Gränssnittet mot användaren vid signering hanteras i sin helhet av signeringstjänsten



1. Användaren identifierar sig för en e-tjänst genom sin e-legitimation och utnyttjar en tjänst som kräver användarens elektroniska underskrift (signatur). E-tjänsten presenterar den elektroniska handling som ska signeras för användaren och användaren accepterar att skriva under handlingen.
2. Användaren överförs till signeringstjänsten med en begäran om signering från e-tjänsten. Begäran om signering innehåller bl.a. en hash representation av dokumentet som ska signeras.
3. Användaren överförs till sin identitetsutfärdare med begäran om legitimering. Användaren legitimeras med stöd av sin e-legitimation och ett identitetsintyg returneras till signeringstjänsten.

4. Signeringstjänsten skapar användarens nyckelpar, utfärdar ett certifikat för användaren samt signerar den elektroniska handlingen. Vid behov skapas en tidsstämpel.
5. Användaren returneras till e-tjänsten med en bekräftelse på att handlingen är underskriven. Bekräftelsen innefattar bl.a. signatur, certifikat och eventuell tidsstämpel.
6. Handling med underskrift skapas av e-tjänsten genom att foga samman handlingen med certifikat, signatur och eventuell tidsstämpel enligt efterfrågat signaturformat.

Genom detta förfarande kan e-tjänsten få en handling signerad utan att lämna ut uppgifter om den elektroniska handlingen till signeringstjänsten. Detta gör det även möjligt för e-tjänsten att signera handlingar som innehållsmässigt är strukturerade enligt att dataformat som inte signeringstjänsten kan presentera på ett för användaren meningsfullt sätt.

6.6 Fördelning av roller och uppgifter

Sammantaget innebär alternativ 1 och 2 följande skillnader i roller och vem som i praktiken utför väsentliga steg i signeringsprocessen.

	Tjänst som hanterar förfarandet	
Uppgift	**Alternativ 1**	**Alternativ 2**
Presentation av dokument som ska signeras för användaren	Signeringstjänsten	e-tjänsten
Skapande av en hash representation av dokumentet för signering	Signeringstjänsten	e-tjänsten
Motta användarens acceptans att signera	Signeringstjänsten	e-tjänsten
Identifiering av användaren	Signeringstjänsten	Signeringstjänsten
Generera nycklar för användaren samt utfärda certifikat till användaren	Signeringstjänsten	Signeringstjänsten
Tidsstämpling av dokument (Endast om detta begärs av e-tjänsten)	Signeringstjänsten	Signeringstjänsten
Signering av dokument	Signeringstjänsten	Signeringstjänsten
Skapa signerat dokument (*Foga samman dokument, certifikat ev. tidsstämpel samt signatur till ett signerat dokument enligt vedertagen standard*)	Signeringstjänsten	e-tjänsten

7 Krav på E-tjänster

De e-tjänster som utnyttjar signeringstjänsten enligt alternativ 2 kommer att bära ett viktigt ansvar för att signaturen är tillförlitlig. Om e-tjänsten är oärlig kan denne skicka med ett hash till signeringstjänsten som inte motsvarar det som e-tjänsten visat upp för användaren. Varken signaturtjänsten eller användaren har någon möjlighet att kontrollera att hash värdet som signeras överensstämmer med den information som användaren väljer att signera innan signering sker. Detta kan i viss mån motverkas om användarens får tillgång till den signerade handlingen efter signering för kontroll men detta förutsätter att den signerade handlingen har ett format som användaren lätt kan tillgodogöra sig.

Denna problemställning är dock inte ny för central signering. Även vid lokal signering är det svårt att uppnå en hög tillförlitlighet av att användaren faktiskt ser det som signeras då användaren måste förlita sig på den information som kan utläsas från lokal programvara för presentation av information och för signering. Även i många av dagens lösningar är användaren i slutändan tvungen att lita på att e-tjänsten inte beter sig bedrägligt.

Det bör klargöras, mot bakgrund av denna hotbild, vilka typer av e-tjänster som kan tillåtas utnyttja signeringstjänsten enligt alternativ 2, exempelvis om detta bör begränsas till statliga myndigheter.

8 Krav på signeringstjänstens organisation och driftsmiljö

Det är avgörande för förtroendet för utfärdade signaturer att signeringstjänsten hanteras under en organisation som har samhällets förtroende.

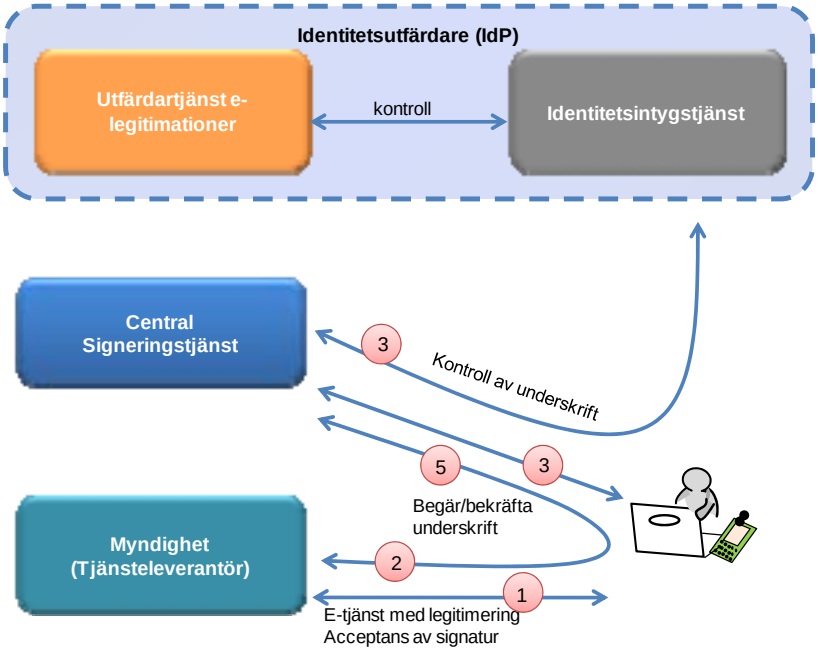
Driftsmiljö och säkerhetsrutiner måste på ett tillförlitligt sätt garantera systemets integritet och förhindra att enskilda administratörer kan missbruka systemet för egna syften.

Signeringstjänsten realiseras i grunden som en webbtjänst. Signeringstjänsten kommunicerar med användaren via HTTP samt kommunicerar vid behov med e-tjänsten via lämpligt gränssnitt.

9 Alternativ till central signering

Om en framtida utvärdering central signering kommer till slutsatsen att ingen form av central signering är acceptabelt, så finns andra alternativ till signering i samverkan med en federativ infrastruktur för identifiering i enlighet med utredningens förslag.

Som exempel kan följande lösning etableras:



1. Användaren identifierar sig för en e-tjänst genom sin e-legitimation och utnyttjar en tjänst som kräver användarens elektroniska underskrift (signatur).
2. Användaren överförs till signeringstjänsten med en begäran om signering från e-tjänsten.
3. Signeringstjänsten överför den information som ska signeras till användaren som signerar informationen med stöd av sin e-legitimation och sin klientapplikation för signering som

användaren erhållit från utfärdaren av användarens e-legitimation.

4. Signeringstjänsten verifierar att rätt användare signerat handlingen genom en kontroll mot identitetsutfärdaren (Förslagsvis genom att tillämpa standarden [SAMLX509].
5. Signeringstjänsten överför användaren tillbaks till e-tjänsten samt överför nödvändigsigneringsinformation.

Genom detta förfarande kan en e-tjänst befrias helt från såväl integration med användarens funktioner för signering, som tolkning av användarens e-legitimation för att fastställa användarens identitet. Signeringstjänsten sköter all integration med olika signeringslösningar i användarnas klienter och information om identitet ges i enlighet med federationens gemensamma attributsprofil i det attributsintyg som erhålls i samband med kontroll av signaturcertifikat (steg 4 enligt [SAMLX509].

Dock är en lösning av detta slag behäftat med i stort sett samma tidigare nämnda svagheter jämfört med dagens lösning på så sätt attanvändarens e-legitimation fortsatt måste vara certifikatbaserad samt att dessa signaturer inte kan verifieras av förlitande part i utlandet som inte har tillgång till aktuell spärrinformation eller den svenska infrastrukturen för identifiering.

Av detta skäl förs inte denna typ av lösning fram som ett primärt förslag.

10 Övergripande arkitektur

I de utförande exempel som anges i detta avsnitt sker även kommunikation mellan signeringstjänst och e-tjänst via HTTP.
Följande funktioner ingår i signeringstjänsten utöver webbgränssnittet mot användare och kommunikation med e-tjänster

- Certifikatutfärdare
- Tidsstämplingsfunktion
- Signeringsfunktion

Beskrivningarna i detta avsnitt utgör exempel på utförande som uppfyller ställda krav. De utgör ett grundförslag på utförande och

specificerar inte en komplett design för implementering. Olika aspekter av arkitekturen kan komma att ändras vid ett slutgiltigt genomförandeprojekt.

10.1 Informationsflöden

Grunden för kommunikation mellan e-tjänst och signeringstjänst samt mellan signeringstjänst och identitetsutfärdare är att kommunicera information via användaren så samma sätt som sker vid SAML authentication request och respons.

Utgångspunkten är att denna kommunikation sker i enlighet med SAML HTTP Post binding [SAML-Bindings].

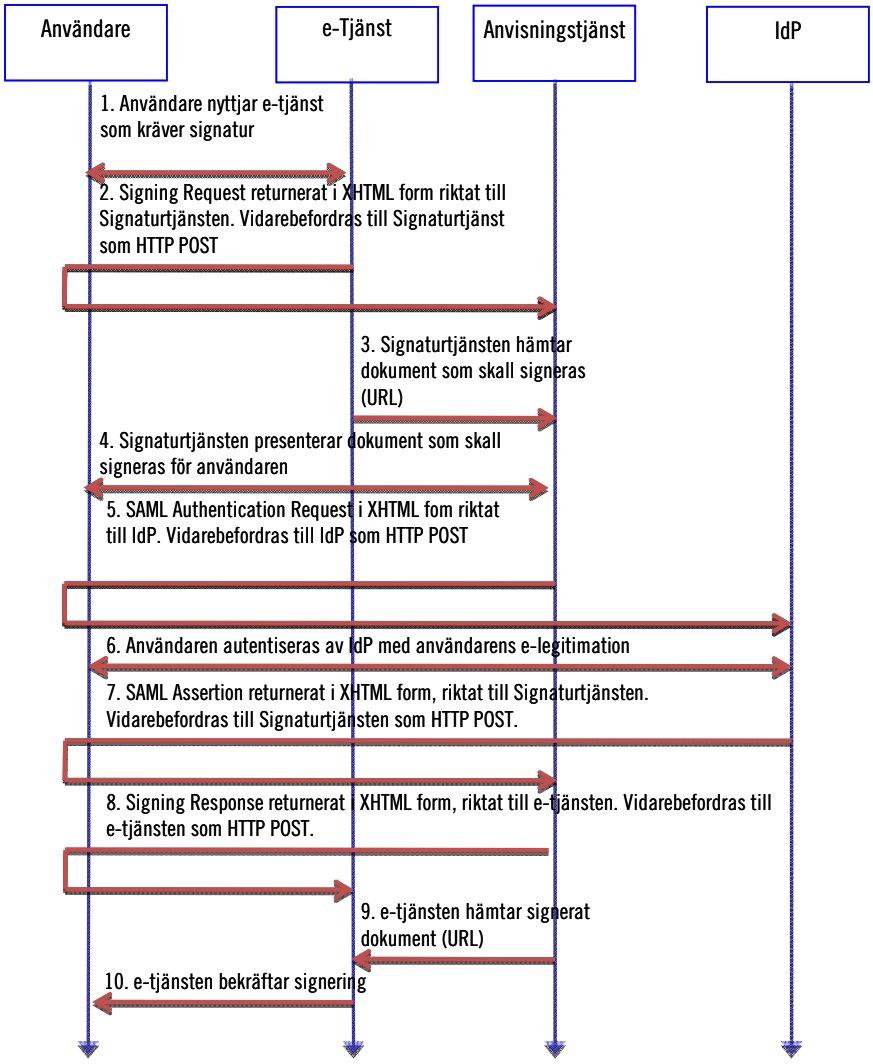
Vid SAML HTTP Post binding kommuniceras ett svar till användaren när denne gör ett aktivt val i sin webbläsare (ex. väljer att skriva under). Användarens val resulterar i en HTTP request från användaren till webbtjänsten. Detta resulterar i en HTTP response som innehåller en XHTML form som innehåller informationen som ska vidarebefordras till nästa webbtjänst (ex en signing request till signeringstjänsten eller en authentication request till identitetsutfärdaren. När XHTML formen öppnas i användarens webbläsare så innehåller denna en instruktion att skicka information till mottagande webbtjänst som HTTP Post.

[SAML-Bindings] specificerar genom SAML HTTP Post binding hur request och response meddelanden kan förmedlas via användaren på detta sätt.

det enda som krävs för en komplett specifikation av den informationsutväxling mellan e-tjänsten och signeringstjänsten som går via användaren är att specificera ett signing request och ett signing response meddelande som kan förmedlas i XHTML form via HTTP Post.

10.2 Informationsflöden - utförande enligt alternativ 1

Informationsutväxling mellan parterna i utförande enligt alternativ ett kan ske på följande sätt:

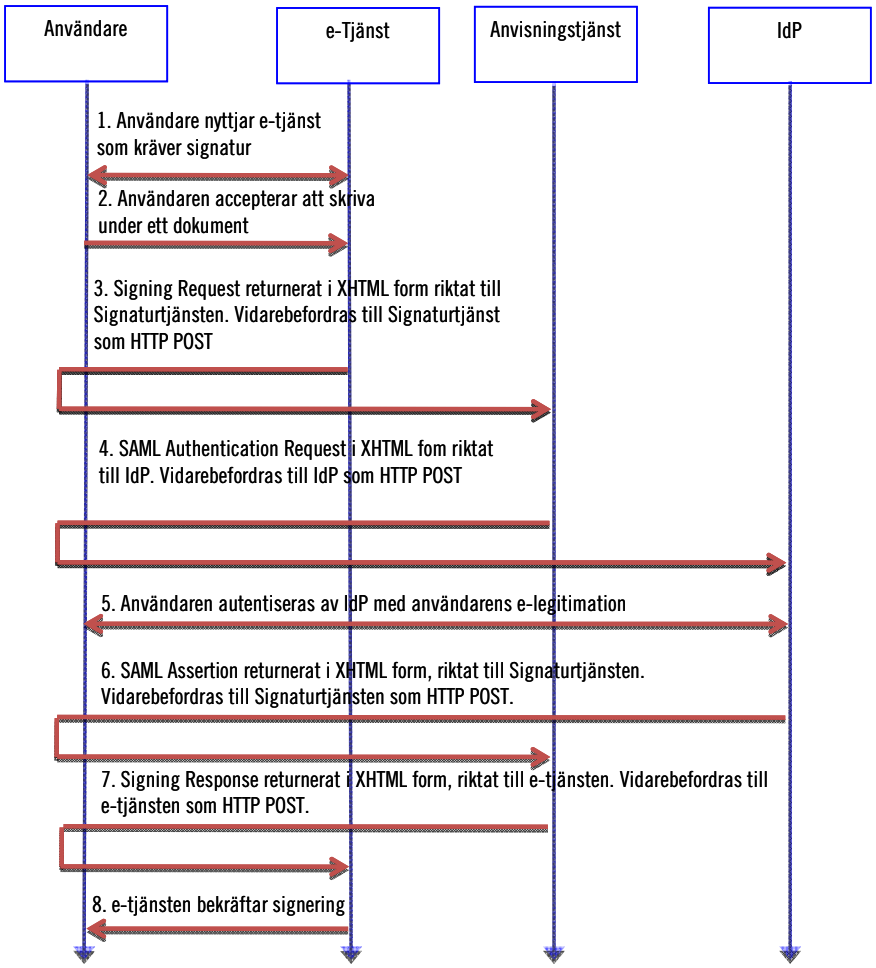


I detta utförande sker signering i signeringstjänsten efter det att användaren autentiserats och ett giltigt identitetsintyg (authentication response) mottagits av signeringstjänsten i steg 7.

Det dokument som signeras skickas inte via användaren för att undvika fördröjningar om dokumentet är stort och användaren har begränsad kommunikationshastighet. Dokument som ska signeras och signerat dokument hämtas av parterna via en URL i setgen 3 och 9. URL till dokumenten medföljer signing request respektive signing reponse i stegen 2 och 8.

10.3 Informationsutväxling – utförande enligt alternativ 2

Informationsutväxling mellan parterna i utförande enligt alternativ två kan ske på följande sätt:



I detta utförande sker signering i signeringstjänsten efter det att användaren autentiserats och ett giltigt identitetsintyg (authentication response) mottagits av signeringstjänsten i steg 6.

Det dokument som ska signeras överförs inte till signeringstjänsten. Istället överför e-tjänsten en hash av dokument som ska signeras i steg 3 till signeringstjänsten. Med hjälp av denna hash kan signeringstjänsten signera dokumentet utan att få tillgång till dokumentet i klartext (i läsbart skick).

På motsvarande vis skickas inte heller ett signerat dokument till e-tjänsten. Istället skickas signaturen på dokumentet till e-tjänsten

tillsammans med användarens certifikat i steg 7. Utifrån denna information kan e-tjänsten själv skapa det signerade dokumentet enligt ett för ändamålet lämpligt signaturformat.

10.3.1 Authentication request och response

Begäran och erhållande av identitetsintyg för användaren (stegen 5 och 7 i alternativ 1 och stegen 4 och 6 i alternativ 2) genomförs som är en ren SAML identifiering in enlighet med HTTP POST Binging, definierat i [SAML-Bindings].

Detta förfarande ska följa tekniska specifikationer för identitetsfederationen för svensk e-legitimering.

i relation till Identitetsutfärdaren så agerar signeringstjänsten som en förlitande e-tjänst (service provider) gentemot identitets-utfärdaren.

10.4 Signing request och response

Signing Request och Signing Response (steg 2 och 8 i alternativ 1 och steg 3 och 7 i alternativ 2) ska innehålla all information som signeringstjänsten och e-tjänsten behöver utbyta för att genom föra signering och hantera felsituationer med undantag för utväxling av dokument i alternativ 1.

Utgångspunkten är att följande information bör ingå:

Signing Request:

- Version (protokollversion)
- Request type (identifierar typ av request. Olika request type identifierare måste definieras för utförande enligt alternativ 1 och alternativ 2)
- Nonce (en unik identifierare för denna request)
- Identitetsattribut för användaren (Attribute assertion) (ej psudonym). Detta utgör de identitetsattribut som signerings-tjänsten måste kunna kontrolleras genom det identitetsintyg som signeringstjänsten erhåller från identitetsutfärdaren. Dessa attribut måste vara en delmängd av de attribut som signeringstjänsten registrerat som antingen required eller requested attributes i federationens metadata (federations-registret)

- Entity ID för den IdP som ska autentisera användaren vid signering
- En referens till det dokument som ska signeras i URL format (Endast alternativ 1)
- Referens till presentationsformat (stylesheeet) (URL format) (endast vid alternativ 1 och endast vid behov)
- Krypteringsnyckel/nycklar för att dekryptera information som hämtas direkt från e-tjänsten
- En hash av det dokument som ska signeras
- Identifierare av önskat signaturformat ([CMS]?, [XML Dsig], [PDF], [CAdES], [XAdES], [PAdES] etc) (Endast alternativ 1)
- Signaturoptioner
  - Tidsstämpling
  - krav på algorithmer
  - mm (Listan ska vara öppen för framtida utvidgning)

Signing Response

- Version (protokollversion)
- Response type (typ av response)
- Nonce (samma som request nonce)
- Statuskod (ex Signatur skapad, Signatur ej skapad med felkod)
- Referens till signerat dokument (URL) (endast alternativ 1)
- Krypteringsnyckel/nycklar för att dekryptera signerat dokument som hämtas direkt från signeringstjänsten (endast alternativ 1)
- Signatur på dokument som signerats (endast alternativ 2

10.4.1 Övrig kommunikation i flödesmodellerna

Informationsutväxling direkt mellan användare och e-tjänst samt mellan användare och identitetsutfärdare specificeras inte. Denna informationsutväxling utformas i sin helhet av e-tjänsten respektive identitetsutfärdaren.

Hämtning av dokument i stegen 3 och 9 sker med en HTTP GET metod enligt [HTTP] protokollet.

10.5 Tidsstämpling i alternativ 2

I alternativ 1 ombesörjer signeringstjänsten eventuell tidsstämpling av signerat dokument och bifogar tidsstämpeln i den signerade handlingen.

I alternativ 2 är detta inte möjligt eftersom signeringstjänsten inte har tillgång till det signerade dokumentet.

Om en e-tjänst behöver tidsstämpla den signerade handlingen och inkludera detta i den signerade handlingen måste e-tjänsten göra en separat begäran om tidsstämpling efter mottagande av signing response.

Detta kan ske utan att röja dokumentet för signeringstjänsten dels genom att följa tillämpliga standarder för signaturformat [CAdES], [XAdES] eller [PAdES] med avseende på vilken data som ska tidsstämplas och hur tidsstämpeln ska inkluderas i den signerade handlingen, samt dels genom att följa tidsstämplings-standarden RFC 3161 [RFC3161] för att skicka en begäran om tidsstämpling och ta emot tidsstämpel.

10.6 Kommunikations- och meddelandesäkerhet

Följande krav kommunikations och meddelandesäkerhet bör gälla:

- Kommunikation mellan signeringsserver och användare krypteras med SSL/TLS [TLS] med stöd av servercertifikat (ingen klientautentisering).
- Kommunikation mellan användare och e-tjänst skyddas företrädelsevis med SSL/TLS med stöd av servercertifikat (ingen klientautenticering).
- Kommunikation med IdP samt Authentication request och response meddelanden skyddas i enlighet med identitets-federation för svensk e-legitimation.
- Signature request och response ska krypteras till respektive mottagare och signeras av respektive avsändare.
- Dokument som ska signeras och signerat dokument krypteras med nyckel som medföljer signing request repsektive signing response. Publika nycklar för verifiering av signaturer hämtas från federationsregistret (metadata där

signaturtjänsten såväl som e-tjänsten är registrerade som e-tjänsteleverantörer).

10.7 Loggar

Signeringstjänsten behöver bland annat logga följande information för varje signering

- Signing request och signing response meddelanden
- hash av dokument som signerats
- Signatur
- Användarens signaturcertifikat
- Användarens identitetsintyg från acceptans av signering

Dokumentet som signerats och det signerade dokumentet bör inte loggas.

Loggar ska förses med tidsinformation som är tillförlitlig och spårbar till svensk tid (UTC(SP)).

11 Signering

Signeringstjänsten ska signera elektroniska dokument och i utförande enligt alternativ 1 även skapa ett signerat dokument.

Signeringstjänsten ska kunna skapa en kvalificerad elektronisk signatur enlig svensk lag om kvalificerade signaturer [Sig].

Signeringsprocessen följer ett antal väl definierade steg.

1. En hash av det dokument som ska signeras skapas med en godkänd hash algoritm
2. Dokumentets hash signeras med användarens privata signeringsnyckel
3. Ett signerat dokument skapas genom att foga samman dokumentet med signaturen och användarens signeringscertifikat.

Då signering sker enligt utförande alternativ 2 utför signeringstjänsten endast steg 2, medan steg 1 och 3 utförs av e-tjänsten som begär signering.

Innan steg 2 kan utföras måste användarens signeringsnyckel vara genererad och användarens tillhörande signeringscertifikat måste vara utfärdat.

Certifikaten som påförs den signerade handlingen i steg 3 innefattar förutom användarens certifikat även certifikat för de certifikatutfärdare som krävs för att verifiera användarens certifikat.

Om det signerade dokumentet ska tidsstämplas utförs dessutom följande steg

4. En hash av den information som ska tidsstämplas skapas med en godkänd hash algorithm (normalt en hash av själva signaturen som skapades i steg 3)
5. Hash värdet tidsstämplas
6. Tidsstämpeln infogas i det signerade dokumentet

11.1 Signaturformat

I de fall signeringstjänsten skapar ett signerat dokument (steg 3) samt i de fall signeringstjänsten skapar och för in en tidsstämpel i det signerade dokumentet (steg 4 och 6), så ska detta ske i enlighet med ett definierat signaturformat.

Signaturformatet definierar följande aspekter som är relaterat till stegen i föregående avsnitt:

- Hur signatur och dokument fogas samman till ett signerat dokument
- Hur certifikat fogas till det signerade dokumentet
- Vilken information i det signerade dokumentet som är signerad
- Vilken information som ska tidsstämplas
- Hur en tidsstämpel skal fogas till det signerade dokumentet

I de fall det signerade dokumentet inte ska förses med en tidsstämpel så ska följande signaturformat stödjas av signeringstjänsten:

- XML Signature Syntax [XML Dsig]
- Portable Document Format [PDF]

Följade signaturformat kan dessutom stödjas för icke tidsstämplade dokument:

- Cryptographic Message Syntax[CMS]
- CMS Advanced electronic Signatures enligt profil CAdES-BES [CAdES]
- XML Advanced Electronic Signatures enligt profil XAdES-BES [XAdES]
- PDF Advanced Electronic Signatures part 3 enligt profil PAdES-BES [PAdES]

I de fall en tidsstämpel ska tillfogas den signerade handlingen ska följande signaturformat stödjas av signeringstjänsten:

- XML Advanced Electronic Signatures enligt profil XAdES-T [XAdES]
- PDF Advanced Electronic Signatures enligt profil PAdES-T [PAdES]

Följade signaturformat kan dessutom stödjas för tidsstämplade dokument:

- CMS Advanced electronic Signatures enligt profil CAdES-T [CAdES]

11.2 Multipla signaturer

Samtliga standardiserade signaturformat enligt avsnitt 11.1 stödjer att ett dokument förses med flera signaturer. Detta kan vara aktuellt om samma handling måste signeras av mer än en person.

Signaturformaten [CMS} och [XMLDsig] utgör grunden för samtliga nämnda signaturformat [CMS] utgör grunden för [PDF], [PAdES] och [CAdES] signaturer medan [XMLDsig] utgör grunden för [XAdES] signaturer.

I [CMS] lagras signaturer för var och en som undertecknat dokumentet i ett ”SignerInfo” fält. [CMS} tillhandahåller även ett attribut för kontrasignaturer där varje kontrasignatur signerar en signatur i ett av dokumentets SignerInfo fält.

[XMLDsig] tillåter att flera signaturer kopplas till ett dokument genom att lägga till fler ”Signature” element.

Multipla signaturer hanteras enkelt i alternativ 1 såväl som alternativ 2. I alternativ 1 lägger signaturtjänsten till en ny signatur till en befintlig signatur då e-tjänsten tillhandahåller ett dokument för underskrift som redan är signerat. I alternativ 2 lägger e-

tjänsten själv till den nya signaturen efter det att dokumentet signerats av ytterligare personer.

12 Certifikatutfärdande

Certifikatutfärdarfunktionen skapar användarens nyckelpar för signering och utfärdar certifikat till användare som identifierats av signeringstjänsten.

Användarens privata nyckel ska raderas från systemet efter fullgjord signering och ett nytt nyckelpar ska skapas för varje användare och signeringstillfälle.

Certifikat ska utfärdas som kvalificerade certifikat.

12.1 Utfärdarrutiner

Utfärdarrutiner ska följa ETSI policy för certifikatutfärdare som utfärdar kvalificerads certifikat, TS 101 456 [TS101456].

12.2 Certifikatformat

Certifikat till användare ska utformas i enlighet med följande standards:

Standard	Funktion	Referens
RFC 5280	Huvudspecifikation för utformning av certifikat	[RFC5280]
RFC 3739	Internationell huvudstandard för utformning av kvalificerade certifikat.	[RFC3739]
TS 101 862	EU profil av RFC 3739 som specificerar utformning av kvalificerade certifikat enligt EU direktivet för elektroniska signaturer [EUSig].	[TS101862]

Certifikat bör vidare i tillämpliga delar följa TS 102 280 [TS102280] som är en ETSI profil för utfärdande av certifikat till fysiska personer. Denna standard är dock delvis inaktuell eftersom den refererar till föregångaren till RFC 5280 (nämligen RFC 3280). TS 102 280 kommer inom snart att revideras av ETSI. Till detta är gjort bör man hantera TS 102 280 endast som en rekommendation.

Utöver dessa standarder ska följande krav tillgodoses i certifikat utfärdade till användare:

Kravområde	Krav
Information om att certifikatet utfärdats som ett kvalificerat certifikat	Statement ”id-etsi-qcs-QcCompliance” ska infogas i samtliga certifikat i enlighet med TS 101 862.
Information om att privat nyckel hanteras i en ”säker anordning för signaturframställning” i enlighet med signaturlagen [Sig].	Statement ”id-etsi-qcs-QcSSCD” ska infogas i samtliga certifikat i enlighet med TS 101 862.
Information om förlitandebegränsning	Satement ”id-etsi-qcs-QcLimitValue” enligt TS 101 862 kan infogas för att kommunicera en övre monetär gräns för förlitande på utfärdat certifikat. Enligt gällande praxis kan denna gräns sättas till 0. För alla andra värden ska såväl valuta som beloppsgräns specificeras.
Identitetsattribut	Val av identitetsattribut ska följa RFC 3739. det kan vara nödvändigt att på lämpligt sätt konvertera information om användares identitet från attribut i identitetsintyg till andra attribut i certifikaten. Certifikatutfärdaren ska då tillämpa samma mappning om ett stödsystem för certifikatverifiering via SAML tillämpas
Publik nyckel	Algoritm och nyckellängd ska följa generella krav på signeringsalgoritmer i avsnitt 14.

12.3 Stödsystem för certifikatverifiering

Certifikatutfärdarfunktionen ska tillhandahålla spärrinformation. Minimikravet är att tillhandahålla en spärrlista (CRL) i enlighet med RFC 5280 [RFC5280].

12.3.1 Spärrinformation

Spärrinformation ska tillhandahållas i form av en spärrlista (CRL). En sådan spärrlista ska vara en CRL version 2 spärrlista i enlighet med RFC 5280 [RFC5280].

Som komplement kan även spärrinformation tillhandahållas som en on-line tjänst enligt OCSP protokollet [RFC2560].

Den spärrinformation som tillhandahålls måste oavsett teknik vara allmänt tillgänglig. Det får inte krävas ett särskilt avtal med certifikatutfärdaren (Signeringstjänsten) för att få tillgång till spärrinformation.

12.3.2 Certifikatverifiering via SAML

Certifikatutfärdarfunktionen kan även tillhandahålla en certifikatverifieringsfunktion via SAML där certifikatutfärdarfunktionen agerar attributstjänst.

Genom denna attributstjänst kan en e-tjänst som verifierar en användares certifikat skicka en attributsförfrågan till certifikatutfärdaren där användarens certifikat bifogas. Om certifikatet är giltigt returnerar certifikatutfärdarfunktionen ett attributsintyg med användarens identitetsattribut (angivet i enlighet med identitetsfederationens attributsprofil).

Denna attributstjänst ska implementera ”SAML V2.0 Attribute Sharing Profile for X.509 Authentication-Based Systems” [SAMLX509] samt tillämpningsprofilen ”SAML V2.0 Deployment Profiles for X.509 Subjects” [SAMLX509Dep]

13 Tidsstämpling

En tidsstämplingstjänst kan upprättas för att dels skapa tidsstämplade signerade dokument som en del av signeringsfunktionen enligt alternativ 1.

En tidsstämplingsfunktion kan även upprättas som en separat tjänst som kan anropas av en e-tjänst för att tidsstämpla ett dokument. Detta kan vara ett signerat dokument i enlighet med någon av de angivna standarderna för tidsstämplade signerade dokument, men kan även vara vilken annan handling som helst.

Tidsstämplingstjänsten tar emot ett hash av ett dokument som ska tidsstämplas och signerar detta hash tillsammans med tidsinformation (ett time-stamp token). Själva handlingen som ska tidsstämplas skickas inte till tidsstämplingsfunktionen.

13.1 Format

Format för tidsstämplar (time-stamp token) samt format för begäran om tidsstämpling ska följa RFC 3161 [RFC3161].

13.2 Transportprotokoll

Då tidsstämplingsfunktionen tillhandahålls som separat tjänst mot e-tjänster så ska transportprotokoll för begäran om tidsstämpling samt returnering av tidsstämpel vara HTTP [HTTP] och följa regler för HTTP transport i RFC 3161 [RFC3161].

13.3 Tillförlitlig tid

Det är avgörande för tidstämplingstjänstens trovärdighet att denna har tillgång till tillförlitlig tid. Tidskällan ska vara direkt spårbar till UTC(SP) (Swedish National time scale).

14 Algoritmer

Val av algoritmer och nyckellängder för tjänster som omfattas av signeringstjänsten bör följa NIST SP 800-131 [SP800-131]. ETSI TS 102 176-1 [ETSI-Algo] är en europeisk specifikation från ETSI som täcker samma område som SP 800-131, men denna är från 2007 och inte lika aktuell som SP 800-131.

Följande algoritmer rekommenderas som minsta acceptabla säkerhetsnivå för samtliga tjänster:

Användningsområde	Algoritm
Symetrisk kryptering	AES-128
Hash algoritm	SHA-256
Publik nyckel algoritm för signering och autentisering	RSA med 2048 bitars modulus. **Not:** Certifikatutfärdare som utfärdar certifikat med en giltighetstid på över 4 år (inkluderat självsignerade rotcertifikat) bör använda RSA med minst 4096 bitars modulus.
Publik nyckel algoritm för skapande av symmetrisk sessionsnyckel (Key agreement)	Diffie Hellman, p=2048 bitar

Dessa rekommendationer är kompatibla med NIST SP 800-131.

15 Referenser

[SAML-Bindings] ”Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0”, OASIS Standard, 15 March 2005.

[CMS] RFC 5652, ”Cryptographic Message Syntax (CMS)”, IETF Standard, September 2009.

[XML Dsig] ”XML Signature Syntax and Processing (Second Edition)”, W3C Recommendation, 10 June 2008.

[PDF] ISO 32000-1:2008, ”Document management — Portable document format — Part 1: PDF 1.7”, ISO Standard, 1 July 2008.

[CAdES] ETSI TS 101 733 V1.8.1, ”Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)”, ETSI Technical Specification, November 2009.

[XAdES] ETSI TS 101 903 V1.4.1, ”XML Advanced Electronic Signatures (XAdES)”, ETSI Technical Specification, June 2009

[PAdES] ETSI TS 102 778 part 1-5, ”Electronic Signatures and Infrastructures (ESI);PDF Advanced Electronic Signature Profiles”, ETSI Technical specifications, various dates.

[HTTP] RFC 2616, ”Hypertext Transfer Protocol -- HTTP/1.1”, IETF Draft Standard, June 1999.

[TLS] RFC 5246, ”The Transport Layer Security (TLS) Protocol Version 1.2”, IETF Proposed standard, August 2008.

[Sig] Lag (2000:832) om kvalificerade elektroniska signaturer.

[SP800-131] NIST SP 800-131, ”Recommendation for the Transitioning of Cryptographic Algorithms and Key Lengths”, NIST special publication draft, June 2010

[TS101456] TS 101 456, ”Electronic signatures and infrastructures (ESI); Policy requirements for certification authorities issuing qualified

certificates", ETSI Technical Specification, May 2007.

[ETSI-Algo] TS 102 176-1, "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms", ETSI Technical Specification, November 2007.

[RFC3161] RFC 3161, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)" IETF Proposed Standard, August 2001.

[RFC5280] RFC 5280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", IETF Proposed standard, May 2008

[RFC3739] RFC 3739, "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile". IETF Proposed Standard, March 2004.

[TS101862] ETSI 101 862, "Qualified certificate profile", ETSI Technical Specification, January 2006.

[TS102280] TS 102 280 "X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons", ETSI Technical Specification, March 2003.

[OCSP] RFC 2560, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", IETF Proposed Standard, June 1999.

[SAMLX509] "SAML V2.0 Attribute Sharing Profile for X.509 Authentication-Based Systems", OASIS Committee Specification 01, March 2008.

[SAMLX509Dep] "SAML V2.0 Deployment Profiles for X.509 Subjects", OASIS Committee Specification 01, March 2008.

[EUSig] "DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures", January 2000.

Statens offentliga utredningar 2010

Kronologisk förteckning

1. Lätt att göra rätt – om förmedling av brottsskadestånd. Ju.
2. Ett samlat insolvensförfarande – förslag till ny lag. Ju.
3. Metria – förutsättningar för att ombilda division Metria vid Lantmäteriet till ett statligt ägt aktiebolag. M.
4. Allmänna handlingar i elektronisk form – offentlighet och integritet. Ju.
5. Skolgång för alla barn. U.
6. Kunskapslägesrapport på kärnavfallsområdet 2010 – utmaningar för slutförvarsprogrammet. M.
7. Aktiva åtgärder för att främja lika rättigheter och möjligheter – ett systematiskt målinriktat arbete på tre samhällsområden. IJ.
8. En myndighet för havs- och vattenmiljö. M.
9. Den framtida organisationen för vissa fiskefrågor. Jo.
10. Kvinnor, män och jämställdhet i läromedel i historia. En granskning på uppdrag av Delegationen för jämställdhet i skolan. U.
11. Spela samman – en ny modell för statens stöd till regional kulturverksamhet. Ku.
12. I samspel med musiklivet – en ny nationell plattform för musiken. Ku.
13 Upphandling på försvars- och säkerhetsområdet. Fi.
14. Partsinsyn enligt rättegångsbalken. Ju.
15. Kriminella grupperingar – motverka rekrytering och underlätta avhopp. Ju.
16. Sverige för nyanlända. Värden, välfärdsstat, vardagsliv. IJ.
17. Prissatt vatten? M.
18. En reformerad budgetlag. Fi.
19. Lärling – en bro mellan skola och arbetsliv. U.
20. Så enkelt som möjligt för så många som möjligt – från strategi till handling för e-förvaltning. Fi.
21. Bättre marknad för tjänstehundar. Jo.
22. Krigets Lagar – centrala dokument om folkrätten under väpnad konflikt, neutralitet, ockupation och fredsinsatser. Fö.
23. Tredje sjösäkerhetspaketet. Klassdirektivet, Klassförordningen, Olycksutredningsdirektivet, IMO:s olycksutredningskod. N.
24. Avtalad upphovsrätt. Ju.
25. Viss översyn av verksamhet och organisation på informationssäkerhetsområdet. Fö.
26. Flyttningsbidrag och unionsrätten. A.
27. Gemensamt ansvar och gränsöverstigande samarbete inom transportforskningen. N.
28. Vändpunkt Sverige – ett ökat intresse för matematik, naturvetenskap, teknik och IKT. U.
29. En ny förvaltningslag. Ju.
30. Tredje inre marknadspaketet för el och naturgas. Fortsatt europeisk harmonisering. N.
31. Första hjälpen i psykisk hälsa. S.
32. Utrikesförvaltning i världsklass. En mer flexibel utrikesrepresentation. UD.
33. Kvinnor, män och jämställdhet i läromedel i samhällskunskap. En granskning på uppdrag av Delegationen för jämställdhet i skolan. U.
34. På väg mot en ny roll – överväganden och förslag om Riksutställningar. Ku.
35. Kunskap som befrielse? En metanalys av svensk forskning om jämställdhet och skola 1969–2009. U.
36. Svensk forskning om jämställdhet och skola. En bibliografi. U.
37. Sverige för nyanlända utanför flyktingmottagandet. IJ.
38. Mutbrott. Ju.
39. Ny ordning för nationella vaccinationsprogram. S.

40. Cirkulär migration och utveckling – kartläggning av cirkulära rörelsemönster och diskussion om hur migrationens utvecklingspotential kan främjas. Ju.
41. Kompensationstillägg – om ersättning vid försenade utbetalningar. S.
42. Med fiskevård i fokus – en ny fiskevårdslag. Jo.
43. Förundersökningsbegränsning. Ju.
44. Mål och medel – särskilda åtgärder för vissa måltyper i domstol. Ju.
45. Händelseanalyser vid självmord inom hälso- och sjukvården och socialtjänsten. Förslag till ny lag. S.
46. Utländsk näringsverksamhet i Sverige. En översyn av lagstiftningen om utländska filialer i ett EU-perspektiv. N.
47. Alkoholkonsumtion, alkoholproblem och sjukfrånvaro – vilka är sambanden? En systematisk litteraturöversikt. S.
48. Multipla hälsoproblem bland personer över 60 år. En systematisk litteraturöversikt om förekomst, konsekvenser och vård. S.
49. Förbud mot köp av sexuell tjänst. En utvärdering 1999–2008. Ju.
50. Försvarsmaktens helikopterresurser. Fö.
51. Könsskillnader i skolprestationer – idéer om orsaker. U.
52. Biologiska faktorer och könsskillnader i skolresultat. Ett diskussionsunderlag för Delegationen för jämställdhet i skolans arbete för analys av bakgrunden till pojkars sämre skolprestationer jämfört med flickors. U.
53. Pojkar och skolan: Ett bakgrundsdokument om "pojkkrisen". Översättning på svenska av engelsk rapport: Boys and School: A Background Paper on the "Boy Crisis". + Engelsk rapport. U.
54. Förbättrad återbetalning av studieskulder. U.
55. Romers rätt – en strategi för romer i Sverige. IJ.
56. Innovationsupphandling. N.
57. Effektivare planering av vägar och järnvägar. N.
58. Rehabiliteringsrådets delbetänkande. S.
59. Underhållsskyldighet i internationella situationer – Underhållsförordningen, 2007 års Haagkonvention och 2007 års Haagprotokoll + Bilagedel. Ju.
60. Ett utvidgat skydd mot åldersdiskriminering. IJ.
61. Driftskompatibilitet och enheter som ansvarar för underhåll inom EU:s järnvägssystem. N.
62. Så enkelt som möjligt för så många som möjligt. Under konstruktion – framtidens e- förvaltning. Fi.
63. EU:s direktiv om sanktioner mot arbetsgivare. Ju.
64. "Se de tidiga tecknen" – forskare reflekterar över sju berättelser från förskola och skola. U.
65. Kompetens och ansvar. S.
66. Barns perspektiv på jämställdhet i skola. En kunskapsöversikt. U.
67. I rättan tid? Om ålder och skolstart. U.
68. Ny yttrandefrihetsgrundlag? Yttrandefrihetskommittén presenterar tre modeller. Ju.
69. Förbättrad vinterberedskap inom järnvägen. N.
70. Ny struktur för skydd av mänskliga rättigheter. + Bilagor + Lättläst + Daisy. IJ.
71. Sexualbrottslagstiftningen – utvärdering och reformförslag. Ju.
72. Folkrätt i väpnad konflikt – svensk tolkning och tillämpning. + Bilaga 7, Svensk manual i humanitär rätt m.m. Fö.
73. Svensk sjöfarts konkurrensförutsättningar. N.
74. Mer innovation ur transportforskning. N.
75. Gymnasial lärlingsutbildning – utbildning för jobb. Erfarenheter efter två års försök med lärlingsutbildning. U.
76. Transportstyrelsens databaser på vägtrafikområdet – integritet och effektivitet. N.
77. Sammanläggningar av landsting – övergångsstyre och utjämning. Fi.
78. Fondverksamhet över gränserna. Genomförande av UCITS IV-direktivet. Fi.
79. Pojkars och flickors psykiska hälsa i skolan: en kunskapsöversikt. U
80. Skolan och ungdomars psykosociala hälsa. U.
81. En ny biobankslag. S.
82. Trafikverket ICT. N.

83. Att bli medveten och förändra sitt förhållningssätt. Jämställdhetsarbete i skolan. U.
84. Hedersrelaterad problematik i skolan – en kunskaps- och forskningsöversikt. U.
85. Vem arbetar efter 65 års ålder? En statistisk analys. S.
86. Personalförsörjningen i ett reformerat försvar. Fö.
87. Skadestånd och Europakonventionen. Ju.
88. Vägen till arbete. Arbetsmarknadspolitik, utbildning och arbetsmarknadsintegration. Fi.
89. Finns det samband mellan samsjuklighet och sjukfrånvaro? En systematisk litteraturöversikt. S.
90. En ny lag om ekonomiska föreningar. Del 1+2. Ju.
91. Planering på djupet – fysisk planering av havet. M.
92. En effektivare förvaltning av statens fastigheter. Fi.
93. Att skapa arbeten. Löner, anställningsskydd och konkurrens. Fi.
94. Gotland – användningen av beteckningarna regionfullmäktige och regionstyrelse. Fi.
95. Se, tolka och agera – allas rätt till en likvärdig utbildning. U.
96. Riktiga betyg är bättre än höga betyg. Förslag till omprövning av betyg. U.
97. Resultatuppföljning, läskvalitet och skolutveckling – tre bidrag till diskussionen om jämställdhet i skolan. U.
98. Gårdsförsäljning. S.
99. Flickor, pojkar, individer – om betydelsen av jämställdhet för kunskap och utveckling i skolan. U.
100. Ansvar för järnvägssäkerheten. Kan en annan fördelning gynna en marknadsdriven utveckling? N.
101. Handlingsplan för att utveckla strategier i miljömålssystemet. M.
102. Massuppsägningar, arbetslöshet och sjuklighet. En rapport om konsekvenser av 1900-talets friställningar för slutenvårdsutnyttjande och risk för förtida död. S.
103. Särskilda spaningsmetoder. Ju.
104. E-legitimationsnämnden och Svensk e-legitimation. Fi.

Statens offentliga utredningar 2010

Systematisk förteckning

Justitiedepartementet

Lätt att göra rätt – om förmedling av brottsskadestånd. [1]

Ett samlat insolvensförfarande – förslag till ny lag. [2]

Allmänna handlingar i elektronisk form – offentlighet och integritet. [4]

Partsinsyn enligt rättegångsbalken. [14]

Kriminella grupperingar – motverka rekrytering och underlätta avhopp. [15]

Avtalad upphovsrätt. [24]

En ny förvaltningslag. [29]

Mutbrott. (38)

Cirkulär migration och utveckling – kartläggning av cirkulära rörelsemönster och diskussion om hur migrationens utvecklingspotential kan främjas. [40]

Förundersökningsbegränsning. [43]

Mål och medel – särskilda åtgärder för vissa måltyper i domstol. [44]

Förbud mot köp av sexuell tjänst. En utvärdering 1999–2008. [49]

Underhållsskyldighet i internationella situationer – Underhållsförordningen, 2007 års Haagkonvention och 2007 års Haagprotokoll + Bilagedel. [59]

EU:s direktiv om sanktioner mot arbetsgivare. [63]

Ny yttrandefrihetsgrundlag? Yttrandefrihetskommittén presenterar tre modeller. [68]

Sexualbrottslagstiftningen – utvärdering och reformförslag. [71]

Skadestånd och Europakonventionen. [87]

En ny lag om ekonomiska föreningar. Del 1+2. [90]

Särskilda spaningsmetoder. [103]

Utrikespartementet

Utrikesförvaltning i världsklass. En mer flexibel utrikesrepresentation. [32]

Försvarsdepartementet

Krigets Lagar – centrala dokument om folkrätten under väpnad konflikt, neutralitet, ockupation och fredsinsatser. [22]

Viss översyn av verksamhet och organisation på informationssäkerhetsområdet. [25]

Försvarsmaktens helikopterresurser. [50]

Folkrätt i väpnad konflikt – svensk tolkning och tillämpning. + Bilaga 7, Svensk manual i humanitär rätt m.m. [72]

Personalförsörjningen i ett reformerat försvar. [86]

Socialdepartementet

Första hjälpen i psykisk hälsa. [31]

Ny ordning för nationella vaccinationsprogram. [39]

Kompensationstillägg – om ersättning vid försenade utbetalningar. [41]

Händelseanalyser vid självmord inom hälso- och sjukvården och socialtjänsten. Förslag till ny lag. [45]

Alkoholkonsumtion, alkoholproblem och sjukfrånvaro – vilka är sambanden? En systematisk litteraturöversikt. [47]

Multipla hälsoproblem bland personer över 60 år. En systematisk litteraturöversikt om förekomst, konsekvenser och vård. [48]

Rehabiliteringsrådets delbetänkande. [58]

Kompetens och ansvar. [65]

En ny biobankslag. [81]

Vem arbetar efter 65 års ålder? En statistisk analys. [85]

Finns det samband mellan samsjuklighet och sjukfrånvaro? En systematisk litteraturöversikt. [89]

Gårdsförsäljning. [98]

Massuppsägningar, arbetslöshet och sjuklighet. En rapport om konsekvenser av 1900-talets friställningar för slutenvårdsutnyttjande och risk för förtida död. [102]

Finansdepartementet

Upphandling på försvars- och säkerhetsområdet. [13]

En reformerad budgetlag. [18]

Så enkelt som möjligt för så många som möjligt – från strategi till handling för e-förvaltning. [20]

Så enkelt som möjligt för så många som möjligt. Under konstruktion – framtidens e- förvaltning. [62]

Sammanläggningar av landsting – övergångsstyre och utjämning. [77]

Fondverksamhet över gränserna. Genomförande av UCITS IV-direktivet. [78]

Vägen till arbete. Arbetsmarknadspolitik, utbildning och arbetsmarknadsintegration. [88]

En effektivare förvaltning av statens fastigheter. [92]

Att skapa arbeten. Löner, anställningsskydd och konkurrens. [93]

Gotland – användningen av beteckningarna regionfullmäktige och regionstyrelse. [94]

E-legitimationsnämnden och Svensk e-legitimation. [104]

Utbildningsdepartementet

Skolgång för alla barn. [5]

Kvinnor, män och jämställdhet i läromedel i historia. En granskning på uppdrag av Delegationen för jämställdhet i skolan. [10]

Lärling – en bro mellan skola och arbetsliv. [19]

Vändpunkt Sverige – ett ökat intresse för matematik, naturvetenskap, teknik och IKT. [28]

Kvinnor, män och jämställdhet i läromedel i samhällskunskap. En granskning på uppdrag av Delegationen för jämställdhet i skolan. [33]

Kunskap som befrielse? En metaanalys av svensk forskning om jämställdhet och skola 1969–2009. [35]

Svensk forskning om jämställdhet och skola. En bibliografi. [36]

Könsskillnader i skolprestationer – idéer om orsaker. [51]

Biologiska faktorer och könsskillnader i skolresultat. Ett diskussionsunderlag för Delegationen för jämställdhet i skolans arbete för analys av bakgrunden till pojkars sämre skolprestationer jämfört med flickors. [52]

Pojkar och skolan: Ett bakgrundsdokument om pojkkrisen. Översättning på svenska av engelsk rapport: Boys and School: A Backgroundpaper on the "Boy Crisis". + Engelsk rapport.[53]

Förbättrad återbetalning av studieskulder. [54]

"Se de tidiga tecknen" – forskare reflekterar över sju berättelser från förskola och skola. [64]

Barns perspektiv på jämställdhet i skola. En kunskapsöversikt. [66]

I rättan tid? Om ålder och skolstart. [67]

Gymnasial lärlingsutbildning – utbildning för jobb. Erfarenheter efter två års försök med lärlingsutbildning. [75]

Pojkars och flickors psykiska hälsa i skolan: en kunskapsöversikt. [79]

Skolan och ungdomars psykosociala hälsa. [80]

Att bli medveten och förändra sitt förhållningssätt. Jämställdhetsarbete i skolan. [83]

Hedersrelaterad problematik i skolan – en kunskaps- och forskningsöversikt. [84]

Se, tolka och agera – allas rätt till en likvärdig utbildning. [95]

Riktiga betyg är bättre än höga betyg. Förslag till omprövning av betyg. [96]

Resultatuppföljning, läskvalitet och skolutveckling – tre bidrag till diskussionen om jämställdhet i skolan. [97]

Flickor, pojkar, individer – om betydelsen av jämställdhet för kunskap och utveckling i skolan.[99]

Jordbruksdepartementet

Den framtida organisationen för vissa fiskefrågor. [9]

Bättre marknad för tjänstehundar. [21]

Med fiskevård i fokus – en ny fiskevårdslag. [42]

Miljödepartementet

Metria – förutsättningar för att ombilda division Metria vid Lantmäteriet till ett statligt ägt aktiebolag. [3]

Kunskapslägesrapport på kärnavfallsområdet 2010 – utmaningar för slutförvarsprogrammet. [6]

En myndighet för havs- och vattenmiljö. [8]
Prissatt vatten? [17]
Planering på djupet – fysisk planering av havet. [91]
Handlingsplan för att utveckla strategier i miljömålssystemet. [101]

Näringsdepartementet

Tredje sjösäkerhetspaketet. Klassdirektivet, Klassförordningen, Olycksutredningsdirektivet, IMO:s olycksutredningskod. [23]
Gemensamt ansvar och gränsöverstigande samarbete inom transportforskningen. [27]
Tredje inre marknadspaketet för el och naturgas. Fortsatt europeisk harmonisering. [30]
Utländsk näringsverksamhet i Sverige. En översyn av lagstiftningen om utländska filialer i ett EU-perspektiv. [46]
Innovationsupphandling. [56]
Effektivare planering av vägar och järnvägar. [57]
Driftskompatibilitet och enheter som ansvarar för underhåll inom EU:s järnvägssystem. [61]
Förbättrad vinterberedskap inom järnvägen. [69]
Svensk sjöfarts konkurrensförutsättningar [73]
Mer innovation ur transportforskning. [74]
Transportstyrelsens databaser på vägtrafikområdet – integritet och effektivitet. [76]
Trafikverket ICT. [82]
Ansvar för järnvägssäkerheten. Kan en annan fördelning gynna en marknadsdriven utveckling? [100]

Integrations- och jämställdhetsdepartementet

Aktiva åtgärder för att främja lika rättigheter och möjligheter – ett systematiskt målinriktat arbete på tre samhällsområden. [7]
Sverige för nyanlända. Värden, välfärdsstat, vardagsliv. [16]
Sverige för nyanlända utanför flyktingmottandet. [37]
Romers rätt – en strategi för romer i Sverige. [55]
Ett utvidgat skydd mot åldersdiskriminering. [60]
Ny struktur för skydd av mänskliga rättigheter. + Bilagor + Lättläst + Daisy. [70]

Kulturdepartementet

Spela samman – en ny modell för statens stöd till regional kulturverksamhet. [11]
I samspel med musiklivet – en ny nationell plattform för musiken. [12]
På väg mot en ny roll – överväganden och förslag om Riksutställningar. [34]

Arbetsmarknadsdepartementet

Flyttningsbidrag och unionsrätten. [26]