kirei

PM

14 juni 2012

E-legitimationsnämnden
Kirei 2012:09

Kartläggning av internationella tillitsramverk

Innehåll

Sammanfattning

Denna promemoria belyser relationen mellan det tillitsramverk som tagits fram inom ramen för Kantara-initiativet och det tillitsramverk som är under framtagande inom ISO/IEC 29115 genom att tydliggöra huvuddragen i respektive tillitsramverk, vilka huvudsakliga skillnader som föreligger mellan dem och i vilken utsträckning de olika ramverken är förenliga med varandra.

I promemorian analyseras även fördelar och nackdelar utifrån ett svenskt perspektiv att eftersträva överensstämmelse med respektive tillitsramverk. Här redogörs för frågor kopplat till kostnader för inblandade parter och möjligheter till internationell interoperabilitet.

Promemorian visar också på en tänkbar implementering av dessa internationella tillitsramverk avseende samtliga tillitsnivåer i en nationell profil, anpassad för svenska förhållanden. Fokus ligger på att ge en bild av hur de olika tillitsramverkens regler kan översättas och tillämpas i ett nationellt tillitsramverk, för att tydliggöra de krav som ställs på respektive part och för respektive tillitsnivå.

Den nationella profilen strävar efter så långt som det kan anses vara rimligt överensstämma med såväl ISO/IEC 29115 som Kantara, och där avvikelser föreligger belyses detta särskilt i profilen. Fokus ligger inte på att åstadkomma ett färdigt förslag till nationell profil, utan avgränsas till att ge en översiktsbild över hur de internationella kraven kan implementeras nationellt.

1 Bakgrund och syfte

E-legitimationsnämnden har ett behov av att ta fram ett nationellt tillitsramverk, som ska ingå som en central komponent i den basstruktur som E-legitimationsnämnden äger och förvaltar. Detta nationella tillitsramverk bör i stor utsträckning vila på internationella standarder för motsvarande tillitsramverk, för att säkerställa internationell interoperabilitet och undvika onödigt utvecklingsarbete för E-legitimationsnämnden.

Syftet med denna promemoria har varit att kartlägga relevanta internationella tillitsramverk, visa på en möjlig svensk implementation samt belysa skillnader mot nuvarande lösningar.

Kartläggningen av internationella tillitsramverk kan sammanfattas i följande tre punkter:

1. Att ge ett underlag för vidareutveckling av nationellt tillitsramverk.
2. Att ge en bättre förståelse för relationen mellan tillitsramverken enligt ISO/IEC 29115 och Kantara, samt vikten ur ett nationellt och internationellt perspektiv att en svensk anpassning överensstämmer med dessa.
3. Att tydliggöra skillnaderna mellan nuvarande regler för utfärdande av e-legitimationer samt motsvarande regler i internationella tillitsramverk.

2 Säkerhet och tillit vid elektronisk identifiering

Under det senaste decenniet har det, i första hand inom e-förvaltningsområdet, vuxit fram breda lösningar för elektronisk identifiering av såväl medarbetare som allmänheten. De lösningar som upphandlats har emellertid baserats på olika tekniska lösningar som också besitter olika säkerhetsegenskaper.

En e-tjänst som önskar använda dessa lösningar har att göra teknisk integration mot var och en av leverantörerna, men också att göra en riskbedömning baserat på var och en av leverantörernas utlovade skyddsnivå. Denna princip fungerar så länge antalet leverantörer av elektroniska ID-tjänster är lågt, och att varje e-tjänsteägare besitter tillräcklig kompetens och tillräckliga resurser för att kunna avgöra i vilken mån leverantören faktiskt uppfyller kraven. I ett läge där det är önskvärt att utöka antalet leverantörer eller utvidga funktionaliteten till att även innefatta internationell samverkan, då leverantörerna av ID-tjänster kan bli mångdubbelt fler, är det inte längre realistiskt att bedöma varje enskild e-tjänst utifrån den risk denne kan utsättas för genom att lita på samtliga av dessa leverantörer. Säkerhetsegenskaperna för de utgivna e-legitimationerna måste harmoniseras och göras kända enligt någon eller några väldefinerade skyddsnivåer.

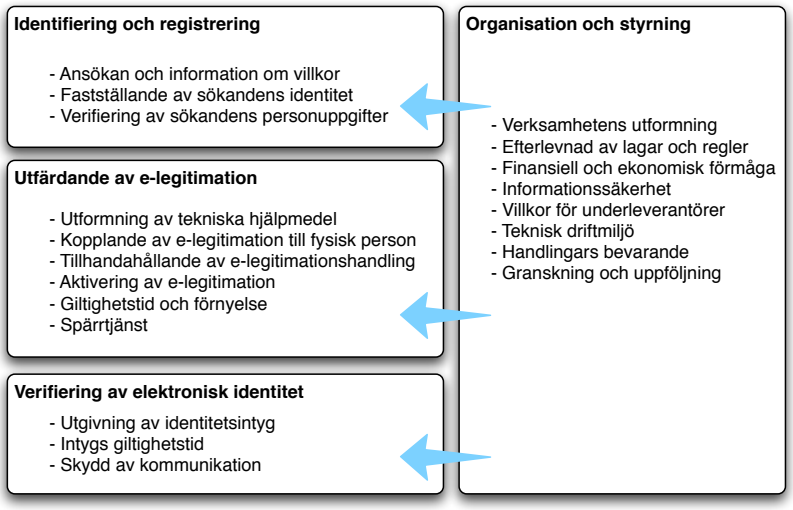
Situationen är inte unik för Sverige, och flertalet internationella insatser har företagits för att möjliggöra samverkan över organisations- och landsgränser. Exempel på sådana harmoniseringsarbeten är den amerikanska budget- och förvaltningsstyrningsbyråns (OMB) vägledning för elektronisk identifiering kallad M-04-04, och EU-projektet STORK:s motsvarighet, kallad STORK QAA.

2.1 En säkerhetsmodell för federerad elektronisk identifiering

Frågan om säkerhet och tillit vid elektronisk identifiering har åter aktualiserats i Sverige genom den föreslagna modell för federerad identifiering som lades fram i utredningen om E-legitimationsnämnden och Svensk e-legitimation (SOU 2010:104), och som låg till grund för E-legitimationsnämndens bildande. I utredningen föreslås samtliga leverantörer av ID-tjänster som uppfyller vissa givna kriterier att få leverera sina tjänster genom ett valfrihetssystem enligt Lagen om Valfrihetssystem (LOV).

För att en sådan identitetsfederationen ska fungera krävs att samtliga kritiska funktioner från samtliga leverantörer lever upp till en eller flera definierade skyddsnivåer. Dessa kriterier för säkerhet bör klargöras i ett tillitsramverk, så att förlitande e-tjänster ska kunna avgöra sin egen risk i samband med användningen av e-legitimationer.

Figur 2.1 illustrerar översiktligt vad som brukligt innefattas i ett sådant tillitsramverk.



Figur 2.1 – Tillitsramverkets olika delar

I definitionen av kriterierna utgår denna promemoria ifrån en allmänt vedertagen modell för elektronisk identifiering, där denna

delas in i tre olika faser:

- Ansökan och fastställande av sökandens identitet
- Utfärdande och tillhandahållande av e-legitimationshandling
- Verifiering av e-legitimation och utställande av identitetsintyg

I var och en av dessa faser krävs särskilda åtgärder för att upprätthålla en definierad skyddsnivå i hanteringen av e-legitimationer. Gemensamt för samtliga faser är säkerhetskrav som rör

- organisatoriska och operationella aspekter,
- fysisk, administrativ och personorienterad säkerhet, samt
- teknisk säkerhet.

Ansökan och fastställande av sökandens identitet

Förutsättningarna för elektronisk identifiering börjar i att en person ansöker om en e-legitimation. Ansökan görs skriftligen i elektronisk form eller på traditionellt sätt med underskrift och intyg om att lämnade uppgifter är fullständiga och riktiga. Ansökan behandlas sedan av en registraturfunktion (*Registration Authority, RA*) som också utför kontrollerna som krävs för att fastställa sökandens identitet.

Vid fastställande av sökandens identitet används traditionella metoder som legitimering med fullgod legitimationshandling vid personligt besök, identifiering genom korrespondens via reguljär postgång (inkluderande tjänster som t.ex. rekommenderat brev med personlig utlämning och mottagningsbevis), eller en kombination av dessa. Som alternativ kan även en tidigare upprättad elektronisk relation för ekonomiskt eller rättsligt betydelsefulla mellanhavanden användas, givet att denna relation i sin tur en gång upprättats på likvärdigt sätt som kraven för den aktuella e-legitimationen.

Utfärdande och tillhandahållande av e-legitimationshandling

I utfärdadefasen kopplar en utfärdarfunktion (*Credential Service Provider, CSP*) en e-legitimationshandling till den av registraturfunktionen fastställda identiteten. Utformningen av e-legitimationshandlingen

kan variera beroende vilka säkerhetskrav som ställs, men gemensamt för samtliga idag förekommande metoder för elektronisk identifiering är att ett stycke konfidentiell information binds till innehavaren på ett tillräckligt säkert sätt. Detta kan till exempel vara ett lösenord, en uppsättning engångskoder, en kryptografisk nyckel eller en personlig säkerhetsmodul.

Verifiering av e-legitimation och utställande av identitetsintyg

I fasen för verifiering av e-legitimation och utställande av identitetsintyg brukar innehavaren sin e-legitimation för att söka åtkomst till en förlitande e-tjänst ansluten till identitetsfederationen. I denna fas gör innehavaren ett påstående om sin elektroniska identitet och bevisar sedan genom ett verifieringsförfarande kontroll över den konfidentiella information som en gång lämnats ut till denne. Om verifieringen lyckas ställer identitetsintygsgivaren ut ett identitetsintyg avsett för den aktuella tjänsten.

Denna fas hanteras av en identitetsintygsgivningsfunktion (*Verifier*).

Avgränsningar

Övriga steg nödvändiga för att slutföra en identifieringsprocess, som att knyta samman parterna i federationen, äkthetskontroll och tolkning av identitetsintyg, kontroll av behörighet, tekniska specifikationer och ansvarsfördelning mellan parterna, ligger utanför avgränsningen av det som här kallas tillitsramverk.

Dessa aspekter, som visserligen kan vara av stor betydelse för förlitande e-tjänster, kan hanteras på olika sätt inom olika federationer, och kan också vara beroende av vilken teknisk lösning som används. Ett tillitsramverk bör gå att tillämpa i alla olika sammanhang som rör identifiering, oavsett teknik, konstellation eller andra förutsättningar, varför detta är en rimlig avgränsning att göra.

2.2 Definition av säkerhetskrav

Utgångspunkten bör vara att den elektroniska identifieringen ska vara tillräckligt bra för det ändamål och i det sammanhang den skall brukas. Det skulle vara orimligt att ställa drastiskt högre krav på det

elektroniska förfarandet vid genomförandet av en transaktion, än vad som ställs om denna genomförs på traditionellt sätt.

Man bör därför tillämpa ett riskbaserad förhållningssätt, där flera tillitsnivåer definieras utifrån den aktuella transaktionens art och den hotbild som existerar. De faktiska krav som blir tillämpliga i var och en av de tidigare nämnda faserna, bestäms genom en samlad riskbedömning där kostnader vägs mot nytta och genom jämförelser med hur motsvarande transaktion fungerar i den fysiska verkligheten.

I denna definition av tillitsnivåer bör man särskilt avhålla sig från att föreskriva vissa särskilda tekniska egenskaper. Dels riskerar säkerhetskraven att snabbt bli inaktuella, och dels kan de även utgöra begränsningar som leder till kostnadsdrivande lösningar och minskad användbarhet.

2.3 De fyra tillitsnivåerna

Inom den amerikanska e-förvaltningen växte i början på 2000-talet en flora av olika identifieringslösningar, både internt på myndigheterna och gentemot invånarna. För att skapa underlag för harmonisering och främja interoperabilitet, tog den amerikanska budget- och förvaltningsstyrningsbyrån (OMB) år 2003 fram en vägledning för elektronisk identifiering kallad M-04-04.

OMB M-04-04 definierar fyra *tillitsnivåer* utifrån de enskilda e-tjänsternas skyddsbehov. Skyddsbehovet baseras på möjliga konsekvenser som kan tänkas uppstå vid ett säkerhetsbrott, i syfte att vägleda de olika förvaltningarna att välja rätt tillitsnivå för varje e-tjänst.

Det uppdrogs åt National Institute of Standards and Technology (NIST) att från tid till annan ge ut en teknisk vägledning innehållande en kravställning som svarar mot respektive tillitsnivå. Denna skrift heter NIST Special Publication (SP) 800-63.

OMB M-04-04 tillsammans med NIST SP 800-63 kan sägas utgöra det första kompletta tillitsramverket, som därmed kunnat användas för att harmonisera nivåer av tillit mellan organisationer.

NIST lyder under amerikanska handelsdepartement (Department of Commerce), och har ett stort inflytande inom IT-säkerhetsområdet i flertalet internationella standardiseringsorgan, som bl.a. IETF, ITU-T och ISO/IEC. Det är därför inte förvånande att de grundprinciper

som läggs fast i de amerikanska dokumenten återkommer i snart sagt samtliga efterföljande ansatser till harmonisering av säkerhet och tillit inom elektronisk identifiering, inklusive det pågående arbetet med ISO/IEC 29115 som beskrivs närmare i avsnitt 3.3.

Samtliga av de studerade tillitsmodellerna tar sin utgångspunkt i den konsekvensbaserade riskbedömningsmodell som definieras i M-04-04, och som identifierar 6 olika riskområden. Vart och ett av riskområdena värderas utifrån hur allvarliga konsekvenser ett säkerhetsbrott kan leda till. Detta ger en nyanserad bild och en tydlig vägledning för en e-tjänsteägare att välja rätt säkerhetsnivå.

De riskområden som är föremål för bedömning är:

- Olägenhet, oro eller ryktesskada
- Finansiell skada eller skadeståndsansvar
- Skada på allmänintresse eller förlitande e-tjänsts verksamhet
- Röjande av känslig information till obehöriga
- Civilt- eller straffrättsligt brott
- Personsäkerhet

Samma riskbaserade tillitsmodell tillämpas även i ISO/IEC 29115, och skiljer sig endast åt ifrån M-04-04 såtillvida att i förslaget till ISO-standard definieras fyra konsekvensnivåer (begränsade, måttliga, betydande och svåra), medan M-04-04 definierar tre (begränsade, måttliga och svåra).

STORK QAA använder samma definitioner på de fyra tillitsnivåerna, men ger ingen ytterligare vägledning för en e-tjänsteägare att avväga rätt skyddsnivå, då detta ligger utanför de definierade leverablerna i delprojektet.

De tillitsnivåer som är gemensamma för samtliga av de nämnda tillitsramverken är:

Tillitsnivå 1

På tillitsnivå 1 finns ingen eller liten tilltro till angiven identitet. Användning av denna nivå är lämplig när konsekvenserna av en felaktig identifiering endast förväntas leda till mycket begränsade negativa följder.

Tillitsnivå 1 erbjuder viss tillit till att det är samma individ som återkommer, som först utförde registreringen. Felaktig identifiering i en e-tjänst får på denna nivå på sin höjd innebära (för någon av de inblandade parterna):

- viss olägenhet eller ryktesskada
- mycket begränsade finansiella förluster eller litet skadeståndsansvar

Exempel: Uppgiftslämnande via en e-tjänst kan använda sig av tillitsnivå 1 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, PIN-kod eller motsvarande. Denna nivå kräver inte heller starkt kryptografiskt skydd av identiteten.

Tillitsnivå 2

På tillitsnivå 2 finns viss tilltro till angiven identitet. Användning av denna nivå är lämplig då resultatet av en felaktig identifiering endast leder till måttliga negativa konsekvenser för någon av de inblandade parterna.

Användning av starkt lösenord över Internet är en acceptabel identifieringsmekanism på denna nivå. Tillitsnivå 2 kräver mekanismer för skydd mot avlyssning, återuppspelning och gissning av lösenord.

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

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

- måttliga monetära förluster
- att delvis känslig information kommer i orätta händer
- lindrigare form av brottslig gärning

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 tillitsnivå 2 förutsatt att inga av de övriga kraven för högre tillitsnivåer blir tillämpliga.

Tillitsnivå 3

På tillitsnivå 3 finns hög tilltro till angiven identitet. Användning av denna nivå är lämplig när det föreligger risk för betydande skador 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 sökandens identitet är starkare än på tillitsnivå 2, och kräver att relationen mellan användare och utgivare baseras på ekonomiskt eller rättsligt betydelsefulla mellanhavanden, eller 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:

- betydande finansiella förluster
- att känslig information kommer i orätta händer
- viss skada på allmänintresse

Exempel: En e-tjänst som stöder inhämtning och utlämnande av känsliga uppgifter som traditionellt kräver identifiering med godkänd fotolegitimation, kan använda sig av tillitsnivå 3.

Tillitsnivå 4

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

Denna nivå kräver att identifiering av sökanden och tillhandahållande av e-legitimationshandling görs vid

personligt besök, på motsvarande sätt som för traditionell legitimationshandling.

Den elektroniska identifieringen ska 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 dataöverföring 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:

- stor skada på allmänintresse
- stora monetära förluster (> 10 M EUR)
- att mycket känslig information kommer i orätta händer
- omfattande ryktesskada
- viss fara för kroppsskada

2.4 Val av tillitsnivå

Det är ägaren till en förlitande e-tjänst som har att välja tillitsnivå. Vid avvägning av vilken tillitsnivå som krävs bedöms var och en av de 6 riskområdena gentemot ett värsta scenario för vad ett säkerhetsbrott skulle kunna leda till för konsekvenser. Tabellen i figur 2.2 ska läsas så att för varje given tillitsnivå, så får de samlade konsekvenserna för ett säkerhetsbrott inte på något område överstiga den angivna nivån. Om så är fallet måste en högre tillitsnivå väljas för den aktuella tjänsten.

Det betyder t.ex. att tillitsnivå 1 aldrig kan komma ifråga om det föreligger någon som helst risk att känslig information röjs till obehöriga. På samma sätt kan det inte komma i fråga att använda en tillitsnivå lägre än tre om det föreligger risk för mer än måttlig olägenhet, oro eller ryktesskada för någon av de inblandade parterna.

Om det över huvud taget föreligger risk för personskada, om så ens med begränsade konsekvenser, så är den lägsta tillitsnivån 3.

Om det föreligger risk för bedrägerier (ett straffrättsligt brott) med begränsat/lågt straffvärde, men där förlitande e-tjänster även kan lida

Konsekvenser vid ett säkerhetsbrott	Tillitsnivå			
	1	2	3	4
Olägenhet, oro eller ryktesskada				
Finansiell skada eller skadeståndsansvar				
Röjande av känslig information till obehöriga				
Civilt- eller straffrättsligt brott				
Skada på verksamhet eller allmänintresse				
Personsäkerhet				

begränsade
måttliga
betydande
svåra

Figur 2.2 – Acceptabla konsekvenser för varje tillitsnivå

måttliga finansiella skador, kan alltså tillitsnivå 2 användas. En sådan tjänst skulle kunna vara e-handel med varor av begränsade värden.

Vid bedömningen av om en e-tjänst är lämplig för en viss tillitsnivå är huvudregeln att nyttan måste överstiga de negativa konsekvenser en felaktig identifiering kan få.

E-legitimationer med särställning

I vissa fall kan det förekomma att en enskild typ av e-legitimation tillskrivs en särställning i en förlitande e-tjänst. Denna särställning kan t.ex. komma av att det existerar ett anställningsförhållande, eller att e-legitimationshandlingen ges ut och används i en separat teknisk och administrativ miljö, och av den anledningen kan tillskrivas en annan tillit än en som getts ut av en annan utfärdare på samma tillitsnivå.

Som exempel kan nämnas polisens eller sjukvårdens tjänstekort. I e-tjänster som inte vänder sig till allmänheten kan det vara rimligt att kräva en viss typ av e-tjänstelegitimation för en viss behörighetsnivå.

Upphandlingen av en sådan e-tjänstelegitimation kan även omfattas av strängare krav än vad som ställs i tillitsramverket, exempelvis i form av särskilda tekniska krav på bärare för e-legitimationen.

Detta hindrar dock inte att samma e-legitimation som har en särställning i ett sammanhang, används som vilken annan e-legitimation som helst (med den angivna tillitsnivån) i ett annat.

2.5 Principer för identifiering

Följande är huvuddragen för de principer som tillämpas i de internationella ramverken för att uppnå den erforderliga skyddsnivån. Flertalet av metoderna som anges går inte att direkt översätta till svenska förhållanden, mycket beroende på den offentlighet som råder kring personuppgifter i Sverige, men även på grund av banksekretess som medför att sådana uppgifter inte kan användas på samma sätt som sker i andra länder.

Redogörelsen här är inte uttömmande, utan syftar endast till att belysa de viktigaste aspekterna för några av momenten i de olika faserna.

Fastställande av sökandens identitet

Tillitsnivå 2: (på distans) Sökanden styrker sin identitet genom att lämna två olika typer av uppgifter som endast denne förmodas ha kännedom om. Dels ett legitimationsnummer från en godkänd legitimationshandling, dels ett bankkontonummer eller ett aktivt kundnummer hos ett bolag som utför en allmännyttig tjänst med anknytning till bostadsadressen (elektricitet, telekommunikation, gas, sophämtning, VA, fjärrvärme).

Registraturfunktionen kontrollerar rimligheten i uppgifterna, och verifierar minst en av uppgifterna gentemot källan. Registraturen bekräftar att namn, adress och andra lämnade personuppgifter överensstämmer med ansökan. I fallet då ett kundnummer hos ett bolag som utför en allmännyttig tjänst ska verifieras, så ska även bekräftas att sökanden känner till omständigheter som rör debiteringen, t.ex. förbrukning.

Tillitsnivå 2: (vid personlig besök) Sökanden styrker sin identitet genom att legitimera sig med godkänd legitimationshandling.

Registraturfunktionen kontrollerar legitimationshandlingens äkthet och giltighet.

Tillitsnivå 3: (på distans) Sökanden styrker sin identitet genom att lämna två olika typer av uppgifter som endast denne förmodas ha kännedom om. Dels ett legitimationsnummer från en godkänd legitimationshandling, dels ett bankkontonummer eller ett aktivt kundnummer hos ett bolag som utför en allmännyttig tjänst med anknytning till bostadsadressen (elektricitet, telekommunikation, gas, sophämtning, VA, fjärrvärme).

Registraturen kontrollerar rimligheten i uppgifterna, och verifierar båda uppgifterna gentemot källan. Utfärdaren bekräftar att namn, adress och andra lämnade personuppgifter överensstämmer med ansökan. I fallet då ett kundnummer hos ett bolag som en allmännyttig tjänst, så ska även bekräftas att sökanden känner till omständigheter som rör debiteringen, t.ex. förbrukning.

Tillitsnivå 3: (vid personlig besök) Sökanden styrker sin identitet genom att legitimera sig med godkänd legitimationshandling.

Registraturen kontrollerar legitimationshandlingens äkthet och giltighet.

Tillitsnivå 4: (endast vid personlig besök) Sökanden styrker sin identitet genom att legitimera sig med godkänd legitimationshandling, samt någon av följande två alternativ:

- ytterligare en godkänd legitimationshandling, eller
- genom att uppge ett bank- eller värdepapperskonto, och som går att verifiera att sökanden är innehavare till.

Registraturen kontrollerar legitimationshandlingars äkthet och giltighet, samt i förekommande fall verifierar att kontouppgifterna stämmer överens med sökandens lämnade personuppgifter.

Tillhandahållande av e-legitimationshandlingen

Tillitsnivå 2: (på distans) E-legitimationshandlingen ska tillhandahållas på ett sätt som:

- bekräftar att personen kan ta emot reguljär post på den adress som framgår av ansökan, eller

- om telefonnummer eller e-postadress framgår av uppgifterna som inhämtats från officiellt register, bekräftar att sökanden kan ta emot information som sänts genom telefonsamtal, textmeddelanden eller e-post, eller
- bekräftar brevledes till adress inhämtad från officiellt register att utgivning av e-legitimationshandling skett.

Tillitsnivå 2: (vid personligt besök) E-legitimationshandlingen ska tillhandahållas på ett sätt som:

- om telefonnummer eller e-postadress framgår av uppgifter som inhämtats från officiellt register, bekräftar att sökanden kan ta emot information som sänts genom telefonsamtal, textmeddelanden eller e-post, eller
- om bostadsadress framgår av identifikationshandlingen, bekräftar brevledes att utgivning av e-legitimationshandling skett, eller
- om bostadsadress inte framgår av identifikationshandlingen, tillhandahåller e-legitimationen på ett sätt som bekräftar att personen kan ta emot reguljär post på adressen som inhämtats från officiellt register.

Tillitsnivå 3: (på distans) E-legitimationshandlingen ska tillhandahållas på ett sätt som:

- bekräftar att personen kan ta emot reguljär post på den adress som framgår av ansökan, eller
- om telefonnummer framgår av uppgifter som inhämtats från officiellt register, inhämtar bekräftelse att sökanden tagit emot e-legitimationshandlingen och först därefter aktivera den.

Tillitsnivå 3: (vid personligt besök) E-legitimationshandlingen ska tillhandahållas på ett sätt som:

- om telefonnummer framgår av uppgifter som inhämtats från officiellt register, inhämtar bekräftelse att sökanden tagit emot e-legitimationshandlingen och först därefter aktivera den, eller

- om bostadsadress framgår av identifikationshandlingen, bekräftar brevledes att utgivning av e-legitimationshandling skett, eller
- om bostadsadress inte framgår av identifikationshandlingen, tillhandahåller e-legitimationen på ett sätt som bekräftar att personen kan ta emot reguljär post på adressen som inhämtats från officiellt register.

Tillitsnivå 4: (endast vid personligt besök) E-legitimationshandlingen ska tillhandahållas på ett sätt som:

- inkluderar ett biometriskt avtryck (foto eller fingeravtryck) vid ansökningstillfället, och
- tillhandahåller e-legitimationen på ett sätt som bekräftar att personen kan ta emot reguljär post på adressen som inhämtats från officiellt register.

Utformning av tekniska hjälpmedel

Tillitsnivå 2: Ett starkt lösenord som valts genom kontrollerade former eller genom automatisk framställning är tillräckligt för att identifiera innehavaren. Andra former inkluderar kort med förtryckta och numrerade lösenord eller s.k. "skraplotter".

Tillitsnivå 3: Tvåfaktorsautentisering genom mjuka bärare med kryptografisk funktion (symmetrisk eller asymmetrisk) validerad enligt FIPS 140-2 nivå 1.

Tillitsnivå 4: Tvåfaktorsautentisering genom hårda bärare med kryptografisk hårdvarumodul (symmetrisk eller asymmetrisk) som validerats enligt FIPS 140-2 nivå 2, samt innefattande fysiska skyddsmekanismer som validerats till FIPS 140-2 nivå 3.

3 Jämförelse av internationella tillitsramverk

3.1 Kantara IAF

Kantara är en icke-vinstdrivande organisation som syftar till att bidra till utvecklingen inom elektronisk identitetshantering, och grundandes av bl.a. Liberty Alliance och Internet Society (ISOC). Medlemmarna består i ett 70-tal organisationer från 11 länder. Kantara Identity Assurance Framework (IAF) hänskjuter till NIST SP 800-63 att definiera tillitsnivåerna, och adderar en modell för certifiering av utfärdare på respektive tillitsnivå, baserat på en ackrediteringsmodell för revisorer/granskare.

Kärnan i Kantara IAF är dokumentet *Service Assessment Criteria* (SAC). I detta dokument definieras granskningskriterier för alla faser av hantering av digitala identiteter, i alla aspekter, för de fyra tillitsnivåerna.

Även om Kantara är en internationell organisation så väger den amerikanska traditionen och värdegrunden tungt i utformningen av många delar av det befintliga IAF-ramverket. Flertalet av de tongivande intressenterna inom Kantara IAF har kopplingar till amerikansk e-förvaltning. Det är därför rimligt att anta att SAC kommer rätta sig efter de krav NIST från tid till annan formulerar för amerikanska myndigheter.

En svensk anpassning av Kantara IAF skulle sannolikt skilja sig ganska markant, både i hur kravställningar formuleras, på vilken nivå den ställs, men också i metoder för fastställande av en persons identitet. Inte minst på grund av kulturella skillnader och hur personuppgifter hanteras i Sverige.

3.2 STORK QAA

STORK-projektets leverabel D2.3, *Quality Authenticator Scheme* (QAA), syftar till att etablera en taxonomi för elektroniska legitimationshandlingar, för att underlätta samordning av e-förvaltningsfrågor mellan EU:s medlemsstater.

STORK QAA tar sin utgångspunkt i en rapport från IDABC (Interoperable Delivery of European eGovernment Services to Public Administrations, Businesses and Citizens) om interoperabilitet i elektronisk identifiering med flera tillitsnivåer. IDABC-rapporten föreslår fyra tillitsnivåer som bär stora likheter med M-04-04 och kravställningen från NIST SP 800-63. Bland skillnaderna märks ett väsentligt större inslag av statlig styrning, och en betydligt mer invecklad riskmodell som i många fall leder till striktare krav på att använda högre tillitsnivåer. Den utgår från hela 14 olika riskområden, somliga vars relevans i sammanhanget kan ifrågasättas.

STORK-projektet har dock valt att bortse från dessa delar av IDABC-rapporten. STORK QAA bär därmed också stora likheter med NIST SP 800-63, och kravformuleringen ligger på ungefär samma bredd men med en mer begränsad detaljnivå. Följaktligen stämmer STORK QAA även överens med principerna som ligger till grund för Kantara IAF.

Skillnaderna står främst att finna i kravställningen på organisation och styrning, där kontraktuella förhållanden med myndigheter och ansvarsreglering i enlighet med EU-direktivet 1999/93/EC står i centrum, medan NIST SP 800-63 ställer mer precisa krav på en utfärdares mognadsgrad ur ett IT-säkerhetshänseende.

3.3 ISO/IEC 29115

I denna promemoria betraktas ISO/IEC 29115 utifrån det nuvarande utkastet (DIS) av dokumentet, och mot bakgrund av den svenska hållningen att avsnitt 10 bör utgå.

ISO/IEC 29115 bär titeln *Entity Authentication Assurance Framework* och är ett vägledningsdokument som beskriver en samverkansmodell med fyra tillitsnivåer, och vilka överväganden var och en av de inblandade intressenterna ställs inför i en sådan samverkan. Arbetet med dokumentet är en samarbete mellan ISO och ITU-T (International Telecommunication Union, Standardization Sector).

Modellen kopierar M-04-04 i definitionen av de fyra tillitsnivåerna (se kapitel 2.3).

Arbetet med ISO/IEC 29115 byggde ursprungligen på ett omfattande bidrag från Kantara (och med en federerad struktur för ögonen), men har sedan dess omarbetats i stora delar. De intressenter som är verksamma inom ITU-T har t.ex. ett behov av att identifiera inte bara människor, utan även maskiner och enheter, och ofta i slutna tekniska miljöer. Sammanföringen av dessa två världar har inte varit friktionsfri, vilket satt väsentliga avtryck i dokumentets kvalitet. Detta har också medfört en viss ändamålsglidning utifrån de ursprungliga tankarna kring ISO/IEC 29115.

Resultatet är den nuvarande och sista utkastversionen kallad DIS. Kvaliteten i detta utkast är diskutabel, och särskilt avsnittet 10 som rör säkerhetskontroller i ett par olika sammanhang innehåller motstridigheter med övriga texten och är i övrigt inte komplett med avseende på tillitsramverkets avgränsningar. Avgörande delar, bl.a. krav på organisation och styrning, har helt utelämnats vilket medför att överensstämmelse med ISO/IEC 29115 inte är tillräckligt för att bedöma säkerheten i en elektronisk identifiering. Ytterligare utvärderingar måste göras i det enskilda fallet, vilket också begränsar nyttan med dokumentet.

Av denna orsak har ett flertal länder, bl.a. Sverige, röstat nej till att ta DIS-utkastet vidare. I skrivande stund ser emellertid fler länder ut att stödja förslaget än att förkasta det, då ett svikande stöd sannolikt hade medfört att dokumentet som helhet förpassats till papperskorgen. Det i sin tur kan leda till en långvarig försening för utarbetande av ett nytt.

Under SC27:s (arbetsgruppen inom ISO som behandlar IT-säkerhetsstandarder) Stockholmsmöte i maj 2012 lanserades emellertid ett förslag till ett nytt dokument, tänkt att fokusera kring en internationell harmonisering av principer för att fastställa en sökandens identitet. Det går dock redan nu att skönja ett flertal beröringspunkter där detta förslag överlappar med ISO/IEC 29115, men i många avseenden också kompletterar.

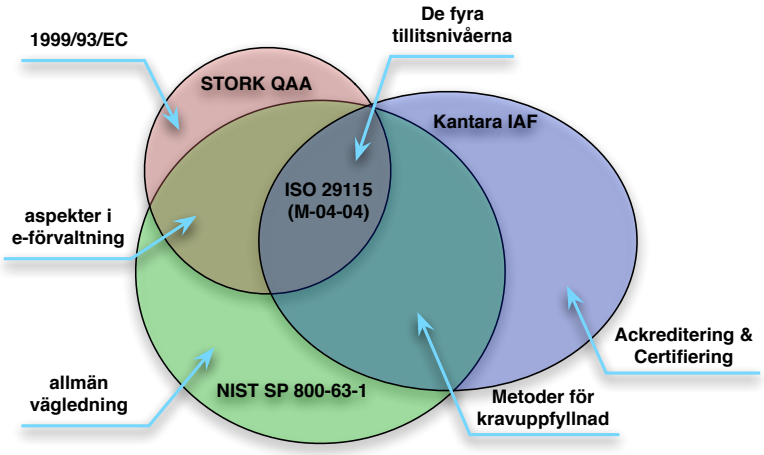
3.4 Sammanfattning av tillitsramverk

Sammanfattningsvis får konstateras att även om det pågår omfattande arbete kring realiserandet av federativa modeller för

elektronisk identifiering, så återstår en del kring mognadsgraden i de olika tillitsramverken.

NIST SP 800-63-1 är sannolikt det mest genomarbetade dokumentet, och som ger den vägledning inför en tillämpning som krävs. Kantara IAF SAC är redan nu något föråldrat, och ger mycket liten flexibilitet för utfärdare att anpassa säkerhetskontroller efter sin egna verksamhet och behov.

Det saknas idag dokument (med konsensus bakom) som beskriver hur uppfyllnad av tillitsnivåerna ska göras vid internationell samverkan, så att interoperabilitet av tillit kan göras på ett ändamålsenligt sätt.



Figur 3.1 – Skillnader och likheter mellan befintliga tillitsramverk

Däremot finns det mycket bred uppslutning kring definitionerna av de fyra tillitsnivåerna utifrån riskperspektivet (som redogjorts för i avsnitt 2.3). Det är därför högst rimligt att även Sverige bygger sin tillitsmodell på dessa, men gör en bred tolkning av hur respektive tillitsnivå kan implementeras vid svenska förhållanden.

Att åstadkomma internationell interoperabilitet av tillit är förstås önskvärt, men det måste också betraktas utifrån att behovet idag är relativt begränsat och att det för närvarande saknas praxis på området. Behovet av internationell samverkan kommer sannolikt öka, men vägen dit följs av diskussioner om hur motsvarande tillitsgrad kan uppnås mellan länder med helt olika förutsättningar, kultur och

rättsliga principer för identifiering.

Tills dess att enhetliga riktlinjer finns för hur olika tillitsgrader ska implementeras i dessa olika länder, bör nämnden i egenskap av svensk myndighet med ansvar för samordning av e-legitimationerna, göra en tolkning och svara för att dokumentera på vilket sätt respektive tillitsnivå uppfylls i Sverige. Därmed torde en de-facto tillit kunna etableras som åtminstone löser de omedelbara behov av internationell samverkan som trots allt existerar.

4 En svensk anpassning

4.1 Identitetsbegreppet i Sverige

Personnummer tilldelas alla personer folkbokförda i Sverige, och används av bl.a. myndigheter för att unikt identifiera en person. Tilldelningen av personnummer och registreringen i folkbokföringsregistret sker genom Skatteverkets försorg och regleras i folkbokföringslagen (1991:481). Folkbokföringen innebär fastställande av en persons bosättning samt registrering av uppgifter om identitet, familj och andra förhållanden, som enligt lagen (2001:182) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet, får förekomma i folkbokföringsdatabasen.

Tillgång till uppgifter i folkbokföringshandlingar regleras i offentlighets- och sekretesslagen. Sekretess för personuppgifter gäller om det av särskild anledning kan antas att den enskilde eller någon honom närstående lider men om uppgiften röjs (SFS 2009:400, 22 kap., 1 §). Ett s.k. rakt skaderekvisit uppställs, dvs. offentlighet uppställs som huvudregel, och att sekretess gäller endast om det kan antas att viss skada uppkommer om uppgiften röjs. Det måste således föreligga någon särskild anledning för att sådana uppgifter ska få hemlighållas.

För uppgifter om namn, adress, personnummer och civilstånd gäller alltså normalt inte någon sekretess.

4.2 Statens Personadressregister (SPAR)

Direktåtkomst till uppgifterna i folkbokföringsdatabasen är noga reglerad, och bestäms i förordning (2001:589) om behandling av personuppgifter i Skatteverkets folkbokföringsverksamhet. För ändamål som inte faller inom ramen för det som anges i 2001:589, tillgodoser Skatteverket samhällets informationsförsörjningsbehov av befolkningsinformation via det statliga personadressregistret (SPAR).

SPAR bildades 1978, på Datainspektionens initiativ, för att begränsa möjligheterna för myndigheter och enskilda att med hjälp av dåtidens nya teknik, s.k. automatisk databehandling (ADB), föra omfattande personregister. Ett statligt befolkningsregister med monopolliknande ställning och under betryggande kontroll ansågs bättre från integritetssynpunkt än ett flertal offentliga och privata personregister.

SPAR är ett offentligt register som omfattar alla personer som är folkbokförda i Sverige, och uppdateras varje dygn med en delmängd av uppgifterna som finns lagrade i folkbokföringsregistret.

När personuppgifter behandlas i SPAR gäller personuppgiftslagen (1998:204), om inte lagen (1998:527) om det statliga personadressregistret innehåller avvikande bestämmelser. Syftet med SPAR framgår av de ändamål som anges i 3 § lagen (1998:527) , där anges att personuppgifter får behandlas för att:

1. aktualisera, komplettera och kontrollera personuppgifter,
2. ta ut uppgifter om namn och adress genom urvalsdragning för direktreklam, opinionsbildning eller samhällsinformation, eller annan därmed jämförlig verksamhet.

Att behandla uppgifter är i detta avseende det samma som att lämna ut uppgifterna elektroniskt. Uppgifter i SPAR lämnas ut elektroniskt efter beslut av Skatteverket.

Enligt 4 § får SPAR innehålla uppgifter om personer som är folkbokförda i landet och personer som har tilldelats personnummer enligt 18 b § folkbokföringslagen (1991:481). SPAR får även innehålla uppgifter om personer som har tilldelats samordningsnummer, om det inte råder osäkerhet om personernas identitet. Följande uppgifter får anges:

1. namn,
2. person- eller samordningsnummer,
3. födelsetid,
4. adress,
5. folkbokföringsort,

6. födelsehemort,
7. svenskt medborgarskap,
8. make eller vårdnadshavare,
9. avregistrering från folkbokföringen på grund av dödsfall, med angivande av tidpunkt, eller avregistrering av annan anledning,
10. summan av fastställd förvärvsinkomst och inkomst av kapital, dock lägst noll kronor,
11. ägare av småhusenhet eller lantbruksenhet med småhus på tomtmark samt uppgift om kommun (belägenhet), och
12. taxeringsvärde för småhusenhet.

4.3 Offentlighetsprincipen

Den tekniska utvecklingen har inneburit att offentlighetsprincipen nu får andra följder än tidigare, eftersom uppgifter i allmänna handlingar blivit mer lättåtkomliga och massuttag av personuppgifter har blivit möjliga.

Kreditupplysningsregistren används till exempel inte längre enbart för kreditupplysningsverksamhet. Flera kreditupplysningsföretag har skaffat sig utgivningsbevis med stöd av YGL (yttrandefrihetsgrundlagen, 1991:1469), och distribuerar därigenom uppgifter från sina kreditupplysningsregister. Eftersom YGL gäller framför vanlig lag blir effekten att kreditupplysningsföretagen varken behöver följa kreditupplysningslagen eller personuppgiftslagen. De kan därmed sälja personuppgifter för andra ändamål än kreditupplysning och de behöver inte heller sända ut en omfrågandekopia till den registrerade personen när en kreditupplysning tagits.

Denna spridning av personuppgifter har medfört att det är nära på trivialt slå upp en invånares namn, adress, person-/samordningsnummer, inkomst och civilstånd.

4.4 Skillnader gentemot andra länder

Sverige har på detta sätt ett av världens mest öppna förhållningssätt till spridning och insyn i invånarnas personuppgifter. I Finland råder

jämförbara förhållanden, medan både Danmark och särskilt Norge tillämpar ett betydligt striktare regler och kontroll över spridningen av personuppgifter.

I stark kontrast till de svenska personnummer- och folkbokföringstraditionen står Tyskland. Här saknas myndighets-centrala system, och ett sådant system, om det inrättades, skulle bryta mot vissa av landets lagar. Olika myndigheter har därför också olika sätt att inordna befolkningen, och en invånare förväntas heller inte memorera dessa olika identitetsnummer.

I USA och Storbritannien, och även övriga delar av världen som brukar räknas till anglosfären (bl.a. innefattande Kanada, Irland, Australien och Nya Zeeland), och som har liknande kultur och rättsliga traditioner, tillämpas även där en helt annorlunda syn på hanteringen av personuppgifter och identiteten i stort.

I flertalet av dessa länder finns visserligen någon variant av nationellt identitetsnummer, ofta baserat på skattenummer eller socialförsäkringsnummer, men där dessa är sekretessbelagda och förväntas vara en uppgift som endast myndigheten och innehavaren känner till.

Det är heller inte ovanligt att det saknas enhetliga regler för utformning och utgivning av fotolegitimation, och att delar av befolkningen inte innehar vare sig körkort eller pass.

Försök att införa en enhetlig fotolegitimation i USA, Storbritannien och Australien har hittills fallit på grund av kraftiga protester.

Detta har medfört att kännedom om identitetsnumret ofta används som metod för att bestyrka en identitet, ofta i kombination med att personen i fråga kan visa upp en handling med anknytning till bostadsadressen, som t.ex. el- eller gasräkning.

I anglosfären krävs inte ens fotolegitimation för att öppna ett konto. Omvänt finns en större öppenhet i bankväsendet, där uppgifter om en invånares förehavanden med banken kan exploateras i olika syften. Bankuppgifter används därför också frekvent för att verifiera en persons identitet, t.ex. genom att kontrollera att ett angivet bankkontonummer tillhör en viss person, eller genom att kontrollera saldo eller förekomst av en viss transaktion.

Dessa traditioner har lett till omfattande problem med identitetsstölder. Personuppgifter kan röjas genom att identitetstjuvar letar igenom sopor eller genom att försöka lura av offret

personuppgifter via s.k. nätfiske. Uppgifterna kan sedan användas för att t.ex. ta lån, ansöka om kreditkort eller teckna mobiltelefonabonnemang.

4.5 Tillitsnivåerna i Sverige

Tillitsnivå 4 definieras som den högsta praktiska säkerhetsnivån att tillämpa i sammanhang som rör invånare. I andra sammanhang, där det kan finnas ett anställningsförhållande, eller andra omständigheter som gör att en viss identitet är känd i en varaktig relation, är det tänkbart att kopplingen till en fysisk identitet går att göra ännu starkare. Detta är dock inte tillämpligt på en befolkning i stort.

Som så kallad *fullgod identitetshandling* enligt SBC 151 räknas svenskt körkort, nationellt ID-kort, svenskt pass i vinröd bok, SIS-märkt ID-kort eller ID-kort utfärdat av statlig myndighet (t.ex. Skatteverket). Detta är i Sverige den typen av legitimation varmed invånare styrker sin identitet i alla upptänkliga sammanhang. Det är rimligt att samma krav ställs för utgivningsprocessen för e-legitimationer av tillitsnivå 4, som för denna typ av fotolegitimation.

Tillitsnivå 1 På denna nivå förekommer inga åtgärder för fastställande av innehavarens identitet eller verifiering av angivna personuppgifter. Tillitsnivå 1 erbjuder viss tillit till att det är samma individ som återkommer, som först utförde registreringen. Individen kan identifieras genom lösenord, PIN-kod eller motsvarande.

Tillitsnivå 2 På nivå 2 har innehavarens identitet verifierats genom att denne kunnat uppvisa kontroll över något som normalt endast personen i fråga förfogar över. Detta kan vara ett telefonnummer, ett kreditkort eller en fysisk traditionell postadress. Personen kan identifieras genom ett starkt lösenord.

Tillitsnivå 3 Innehavarens identitet får verifieras på distans, om detta kan ske på ett tillförlitligt sätt och utfärdaren nått grundläggande kundkännedom på motsvarande sätt som penningtvättregelverket ställer. Det innebär att utgivaren och innehavaren ska ha en relation för ekonomiskt eller rättsligt betydelsefulla mellanhavanden. E-legitimationshandlingen ska tillhandahållas på ett sätt som bekräftar att personen kan ta

emot reguljär post på folkbokföringsadressen. Personen ska identifieras genom tvåfaktorsautentisering.

Tillitsnivå 4 Innehavarens identitet har verifierats vid personligt besök på motsvarande sätt som vid utgivning av traditionell SIS-märkt identitetshandling. E-legitimationshandlingen ska tillhandahållas på ett sätt som bekräftar att personen kan ta emot reguljär post på folkbokföringsadressen. Personen ska identifieras genom tvåfaktorsautentisering med hård bärare.

4.6 Tillitsnivå 3 på distans

Den identifiering som ska ske av den som tilldelas en Svensk e-legitimation blir en betydelsefull del i den kedja av kontroller och skydd av annat slag som måste införas för att tilliten till infrastrukturen ska kunna upprätthållas. Vid införandet av dagens e-legitimationssystem angavs i denna del, att utfärdaren ska identifiera sökanden vid personligt besök, på likvärdigt sätt som vid en ansökan om en SIS-märkt identitetshandling. Samtidigt infördes emellertid en regel om att en sökande som, på angivet sätt, redan har identifierats vid ett personligt besök för att få använda bank på Internet eller någon liknande tjänst för ekonomiskt eller rättsligt betydelsefulla mellanhavanden, istället får identifieras genom denna tjänst. En sådan förenklad rutin skulle emellertid inte få användas om den spärrats eller om det annars kan antas att den inte identifierar sökanden på ett tillräckligt säkert sätt.

Den kravställning som gjordes vid Ramavtalsupphandlingen eID 2008 har en liknande lydelse för att genom ett förenklat förfarande ge ut e-legitimation på distans:

> *[...] Detta förutsätter att den sökande, för att få möjlighet att använda denna e-tjänst, tidigare identifierats vid ett personligt besök, på likvärdigt sätt som vid ansökan om en SIS-godkänd identitetshandling, och att e-tjänsten avser ekonomiskt eller rättsligt betydelsefulla mellanhavanden (t.ex. Internetbank). Den elektroniska ansökningsrutinen får inte användas om den har spärrats eller om det kan antas att den inte identifierar den sökande på ett tillräckligt säkert sätt.*

Kravet på ursprungsidentifiering på likvärdigt sätt som vid utfärdande av en SIS-märkt identitetshandling, innebär att bl.a. att utfärdaren ska följa kraven i SBC 151 med tillkommande regler för utfärdande till allmänheten.

Vid den genomgång som gjorts inför utarbetandet av denna promemoria har det emellertid visat sig att vissa aktörer inte torde uppfylla dessa krav. I det sammanhanget noterades att rutinen för identifiering brukar bygga på att en personlig kod, som sänds med rekommenderat brev, används vid aktivering av en e-tjänst på Internet, varefter kunden kan erhålla en e-legitimation. I vissa fall efter det att ett mottagningsbevis nått banken och registrerats.

I detta sammanhang bör också noteras att Id-kortsutredningen i sitt betänkande (SOU 2007:100) *Id-kort för folkbokförda i Sverige* förklarat att *"Det är vanligt att andra företag tillhandahåller Posten utlämningsställen för privatpersoner, som t.ex. mataffärer. Dessa är emellertid knappast lämpliga som utfärdandeplatser för id-kort."*.

En lägsta nivå idag förefaller vara att en personlig kod, som används gång på gång vid inloggning i e-tjänsten, sänds till användaren med rekommenderat brev. Denna kod används för att komma åt vissa av funktionerna i e-tjänsten, bl.a. beställning av e-legitimation, förutsatt att kunden har minst en finansiell tjänst kopplad till detta konto. Detta innebär i så fall att:

- det inte är fråga om en engångskod, utan något som används upprepade gånger,
- utlämning av koder sker genom rekommenderat brev, vilket inte är ett sådant förfarande som godtas för SIS-märkt identitetshandling, och
- det har inte vidare undersökts i vilken utsträckning kunden behöver etablera en i verklig mening ekonomiskt eller rättsligt betydelsefull relation med utfärdaren.

De utfärdare som har undersökts är ICA Banken, Skandiabanken, Ikano Bank och Länsföräkringar. Samtliga erbjuder banktjänster via Internet, där den ursprungliga identifieringen baseras på rekommenderat brev, som ska förenas med användningen av en finansiell tjänst. Härvid har emellertid heller inte närmare undersökts hur säkerhetslösningen utformats, eller vilka kontroller utfärdaren utför vid sidan om ursprungsidentifieringen.

Ett närliggande område är också det regelverk som gäller till följd av lagen (2009:62) om åtgärder mot penningtvätt och finansiering av terrorism. Av 2 kap. 1 § följer att vissa verksamhetsutövare ska vidta åtgärder för att uppnå kundkännedom och att omfattningen av dessa åtgärder ska anpassas efter risken för penningtvätt eller finansiering av terrorism. Enligt 2 kap. 3 § avses med sådana åtgärder bl.a. kontroll av kundens identitet genom identitetshandling, registerutdrag eller på annat tillförlitligt sätt. Finansinspektionen har utfärdat föreskrifter och allmänna råd om åtgärder mot penningtvätt och finansiering av terrorism (FFFS 2009:1) där det i 4 kap. 2 § - beträffande ett företags identifiering av en fysisk person på distans – föreskrivs att

> 3 § Ett företag ska utföra identitetskontroll på distans genom att
>
> 1. använda elektronisk legitimation för att skapa en avancerad elektronisk signatur enligt definition i 2 § lagen (2000:832) om kvalificerade elektroniska signaturer eller använda någon annan motsvarande teknik för elektronisk identifiering, eller
> 2. säkerställa kundens identitet genom att på lämpligt sätt
>   (a) inhämta uppgift om kundens namn, personnummer eller motsvarande och adress,
>   (b) kontrollera uppgifterna mot externa register, intyg, annan dokumentation, eller motsvarande, samt
>   (c) kontakta kunden genom att skicka en bekräftelse till kundens folkbokföringsadress, se till att kunden skickar in en kopia av id-handling, eller motsvarande.

Preliminär bedömning

Vid en utformning av flera tillitsnivåer för Svensk e-legitimation, och som samtidigt innebär en harmonisering mot att överensstämma med motsvarande internationella tillitsramverk, kan den redovisade utvecklingen mot förenklade förfaranden visa sig vara en rimlig väg att gå för att möjliggöra även för aktörer utan fysisk representation (telefon- och Internetbanker, försäkringsbolag, fondkommissionärer

och liknande) att baserat på den relation de upprättat, och som är att betrakta som att avse *ekonomiskt eller rättsligt betydelsefulla mellanhavanden*, använda denna för utgivning av Svensk e-legitimation på nivå 3.

I förutsättningarna för detta ingår då att relationen ska, i tillägg till kraven för upprättande, också avse *ekonomiskt eller rättsligt betydelsefulla mellanhavanden*. Det är i denna mening inte tillräckligt att en affärsförbindelse etableras, eller en enstaka transaktion utförs på distans, för att en e-legitimation ska få utfärdas. Det krävs i praktiken att utfärdaren står en ekonomisk eller rättslig risk i anknytning till den upprättade distansrelationen. Närmare vägledning för kraven på denna relation får följa av den praktiska utvecklingen och de faktiska risker som föreligger för missbruk av sådana tjänster.

4.7 Svensk e-legitimation och Tillitsnivå 1

De allra flesta idag förekommande tjänsterna på Internet bygger på en identifiering likvärdig med tillitsnivå 1. Användare har en gång registrerat sig och uppgett några för tjänsten nödvändiga personuppgifter. Detta är i verklig mening inte en legitimation. En legitimation är en urkund som styrker en persons identitet. På tillitsnivå 1 existerar inte denna koppling till personens identitet. Därmed uppträder en person som identifierar sig på tillitsnivå 1 snarare med en pseudonym eller helt anonymt. Enligt det resonemanget torde tillitsnivå 1 falla utanför vad infrastrukturen för Svensk e-legitimation bör tillhandahålla.

Behovet av identifiering på tillitsnivå 1 är emellertid omfattande. Det finns ett stort värde i att t.ex. kunna veta att det finns fysisk person bakom en pseudonym, att det går att vidta sanktioner (t.ex. uteslutning från en nätdiskussion) och ytterst också att det går att spåra pseudonymen ifall brottsliga gärningar företas.

Det är alltså tänkbart att e-legitimationer som utfärdats för högre tillitsnivåer används i sammanhang för tillitsnivå 1, men att förlitande e-tjänst i dessa fall aldrig får del av några personuppgifter i identitetsintyget (endast en unik identifieringssträng förekommer).

Om det vore möjligt att tillämpa en sådan användning av Svensk e-legitimation så skulle det sannolikt bidra till en högre användarnytta och därigenom också skapa en större spridning bland både användare och e-tjänster som brukar Svensk e-legitimation.

4.8 Relationen mellan tillitsnivåer och kvalificerade certifikat

Kvalificerade certifikat enligt lagen (2000:832) om kvalificerade elektroniska signaturer anger visserligen en del grundläggande säkerhetskrav för utgivaren, men är annars att betrakta som en juridisk status snarare än en viss säkerhets- och tillitsnivå.

I tillitsramverket definieras ingående krav för var och en av faserna vid hanteringen av e-legitimationer, tillkommande generella krav på organisation och styrning. I 9 § signaturlagen finns visst överlapp med dessa generella krav, men där de säkerhetskrav som ställs för utfärdare av kvalificerade certifikat i signaturlagen dock är allmänt hållna:

> *9 § En certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten skall 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.*

Utöver ovanstående finns krav på spärrtjänst och handlingars bevarande. Vad beträffar övriga krav i tillitramverket saknas

motsvarigheter i signaturlagen, och inga av de krav som i tillitsramverket särskiljer de olika tillitsnivåerna berörs i signaturlagen, varför ett kvalificerat certifikat kan utfärdas på samtliga tillitsnivåer 2–4.

Konkreta och relevanta exempel med avgörande betydelse för säkerheten och tilliten innefattar fastställande av sökandens identitet och hur e-legitimationshandlingen tillhandahålls innehavaren.

Därmed kan man inte förutsätta att en e-legitimation som baseras på ett kvalificerat certifikat besitter några särskilda säkerhetsegenskaper endast på grundval av att det är kvalificerat. Kvalificerade certifikat utgör också en begränsning i valet av teknisk lösning, men som i sig inte heller borgar för en högre säkerhetsnivå.

Kvalificerade certifikat kan dock användas i de sammanhang med federativ struktur som nämns här, men måste klassificeras enligt en given tillitsnivå, bl.a. beroende på

- hur ansökningsförfarandet går till,
- hur sökandens identitet fastställs,
- hur e-legitimationshandlingen utfärdas och tillhandahålls användaren,
- hur de tekniska hjälpmedlen utformas, och
- mognadsgraden i utgivarens ledningssystem för informationssäkerhet.

Kvalificerade certifikat är därmed snarare en juridisk status på en e-legitimationahandling, och har ingen direkt bäring på säkerhet och tillit som vi här definierar.

4.9 Särskilt kostnadsdrivande krav

Av de krav som förekommer i de internationella tillitsramverken, och som kan vara av särskilt kostnadsdrivande art utan att för den sakens skull påverka risknivån på något avsevärt sätt, kan följande från Kantara IAF SAC särskilt lyftas fram:

- Krav på certifiering av säkerhetsmoduler enligt tillämpliga amerikanska FIPS-standarder, vilka har till syfte att säkerställa

att framställning, användning och skydd av kryptografiskt nyckelmaterial sker på ett betryggande sätt. Certifiering enligt dessa standarder genomförs av NIST (National Institute of Standards and Technology), som lyder under amerikanska Department of Commerce. Certifieringskravet begränsar utbudet av säkerhetsmoduler och påför även ytterligare krav som dagens e-legitimationer i vissa fall inte når upp till. I det tillitsramverk som föreslås i kapitel 8 har kravet därför ändrats till att lyda:

[...] säkerhetsmekanismerna för skydd av nyckelmaterial är genomlysta och baserade på erkända och väletablerade standarder.

- Krav på ytterligare kontroller i tillhandahållandet av e-legitimationshandlingen, för att säkerställa att de uppgifter som används (t.ex. folkbokföringsadressen) är aktuella, genom att t.ex. fördröja kvittens eller aktiveringskod. Detta krav skulle påföra fördröjningar som särskilt i utfärdande av e-legitimation på distans kan medföra alltför stora olägenheter, samtidigt som nyttan av att fördröja tillhandahållandet kan ifrågasättas. Andra kompletterande kontroller föreslås istället formuleras i riktlinjerna.

- Krav innebärande att en e-legitimation som inte använts de senaste 18 månaderna automatiskt ska spärras (även om dess giltighetstid i övrigt sträcker sig längre) kan leda till ett resursslöseri i vissa fall. Idag utfärdas fotolegitimation på kort som även innehåller e-legitimation, där giltighetstiden är 5 år. En person som erhåller en e-legitimation på sådant sätt kanske inte omedelbart använder denna, eftersom det primära syftet var att skaffa en fotolegitimation. Det är dock svårt att se någon rimlig anledning till att e-legitimationen skall bli ogiltig efter 18 månader, om legitimationshandlingen i övrigt är giltig ytterligare flera år. Detta kan förväntas bli särskilt kostnadsdrivande, varför kravet föreslås lämnas helt utan avseende.

I det tillitsramverk som föreslås i kapitel 8 har dessa krav utelämnats just av den orsaken att de förväntas bli orimligt kostnadsdrivande, och samtidigt ha begränsad påverkan på risknivån.

4.10 Profilering

Profilering innebär att anpassa kraven i ett befintligt tillitsramverk till de lokala förhållanden som råder inom den aktuella intressesfären, t.ex. en nation, en bransch eller någon annan typ av sammanslutning för elektronisk identifiering.

Att för Svensk E-legitimation strikt följa ett tillitsramverk utformat för utländska förhållanden skulle sannolikt te sig tämligen orimligt, särskilt i utformningen av de krav som ställs för fastställande av sökandens identitet. Att formulera svenska krav på samma nivå som t.ex. Kantara IAF SAC skulle också vara synnerligen kostnadsdrivande i utfärdarledet genom dess rigida struktur. Att formulera kraven på en högre nivå i enlighet med vad som är brukligt i upphandlingsunderlag kan förväntas leda till ett långsiktigare och stabilare regelverk med högre acceptans i utfärdarledet, och också vara mer tilltalade för nya presumtiva utgivare då dessa får en större flexibilitet i utformningen av tjänsten, utan att för den sakens skull tumma på de väsentliga skyddsaspekterna.

Vid en profilering av de internationella tillitsramverken bör man sträva efter att göra en tolkning av den bakomliggande intentionen i respektive krav, och att aldrig sänka den givna ambitionen för den ifrågavarande tillitsnivån. Den principen underlättar för att nå acceptans vid internationell samverkan och att skapa en de-facto tillit till Svensk e-legitimation. Det tillitsramverk som föreslås i kapitel 8 kan ses som en profilering av ISO/IEC 29115 i detta avseende.

5 Dagens e-legitimation

Dagens e-legitimation som används i Sverige motsvarar relativt väl tillitsnivå 3 i den internationella definitionen. Grundkriterier som denna bedömning vilar på, innefattar bl.a.:

- identitet styrks genom fullgod och giltig fotolegitimation, antingen vid personligt besök, eller via bevittnad kopia
- kan ges ut på distans, genom t.ex. Internetbank
- användarens aktivering av e-legitimationen sker genom tvåfaktorsprincip med mjuka eller hårda bärare

De största skillnaderna blir att de befintliga utfärdarna av e-legitimation ska uppfylla ett uniformt regelverk, och där enstaka kontroller kan tänkas avvika från de som för närvarande tillämpas. Exempel på sådana kan vara:

- utfärdande på distans ska innefatta verifiering av att innehavaren kan ta emot reguljär post på folkbokföringsadressen,
- utfärdare ska tillhandahålla en utfärdardeklaration, *tillgänglig för allmänheten*, där principer för kravuppfyllnad av respektive punkt i tillitsramverket ska redogöras för,
- utfärdare ska tillhandahålla funktion för utgivning av identitetsintyg.

Redan i Ramavtalsupphandlingen eID 2008 finns skall-krav för utfärdardeklaration, men att denna bara behöver tillhandahållas avropande parter. Skillnaden mot internationella regelverk är att de ska finnas offentligt tillgängliga.

Ramavtalsupphandlingen eID 2008 innefattar också bör-krav för Ledningssystem för Informationssäkerhet motsvarande ISO/IEC 27001. Kravet motsvarar det som ställs i de internationella tillitsramverken på nivå 2 och 3. Detsamma gäller krav på revision, där det förväntas att leverantören är föremål för extern oberoende granskning var 12:e månad.

Övriga krav i ramavtalsupphandlingen eID 2008 motsvarar de krav som ställs i de internationella tillitsramverket, t.ex. med avseende på bevarande av handlingar och arkivering/gallring, information till innehavare, fastställande av sökandens identitet och tillhandahållande av e-legitimationen och spärrtjänst.

En skärpning av kraven gentemot ramavtalsupphandlingen eID 2008 är att utfärdare som ger ut e-legitimationer på nivå 4, ska inneha certifiering enligt ISO/IEC 27001, och där avgränsningen för certifieringen ska inkludera samtliga krav och säkerhetsaspekter som lyfts fram i tillitsramverket.

6 Kontroll av efterlevnad

Allt eftersom användningen och spridningen av e-legitimationer ökar, kan också samhällets beroenden till denna infrastruktur komma att bli allt mer kritisk. Det är rimligt att anta att infrastrukturen för Svensk e-legitimation på sikt kommer att kunna betraktas som en samhällsviktig funktion. Den federerade modellens distribuerade struktur medför en robusthet mot enskilda svåra händelser, men också utmaningar i form av att kontrollera att alla aktörer fullgör sina åtaganden.

Särskilt utfärdarnas intygsgivningsfunktion är i detta avseende föremål för påtaglig risk ur tillitssynpunkt. Ett säkerhetsbrott i en intygsgivningsfunktion kan, beroende på säkerhetsbrottets art, drabba hela infrastrukturen för Svensk e-legitimation och snabbt undergräva förtroendet bland såväl invånare som förlitande e-tjänster. Nämnden i rollen som ansvarig för infrastrukturen har därmed ett ansvar att säkerställa att samtliga funktioner, och intygsgivningsfunktionen i synnerhet, från tid till annan åtnjuter rätt skydd för att sådana kriser inte skall uppkomma.

Det är därför viktigt att myndigheten får de verktyg som krävs för att kunna utveckla och anpassa skyddsnivån efter omvärldens krav och nyuppkomna hot, samt förmåga att vidta kraftfulla och omedelbara åtgärder vid händelse av allvarliga säkerhetsbrott.

Detta är viktigt för att samhällets aktörer, vare sig de verkar inom den offentliga eller privata sektorn, kan fästa och upprätthålla en tillit till infrastrukturen.

6.1 Kontroll genom anslutningsavtal

Risktagande är en naturlig del av all affärsverksamhet. Anslutna utfärdare kan antas vidta de åtgärder och ta de risker som de anser vara lönsamma ur ett affärsriskperspektiv. Det innebär

att den samlade infrastrukturens behov av säkerhetsskydd inte nödvändigtvis måste sammanfalla med en utfärdares intressen. Det är därför viktigt att medel står till buds för att kunna genomföra ingående kontroller, och att upptäckta allvarliga missförhållanden innan de orsakat incidenter som riskerar att rubba tilliten till infrastrukturen. Förelägganden om rättelse bör kunna förenas med vite och omedelbar avstängning tills dess att missförhållandena avhjälpts.

Det är också viktigt att former för incidentrapportering fastställs i anslutningsavtalet, eftersom detta utgör en viktig del av den grund för vilken nämnden har att utveckla tillitsramverket.

I det föreslagna anslutningsavtalet (*utkast 2012-04-19*) ges nämnden möjlighet att utföra kontroll av utfärdare genom oberoende tredje parts utlåtande om de rådande förhållandena hos en ansluten utgivare. Tillitsramverket antas ligga till grund kontrollen.

Avgörande för att denna kontroll ska vara effektiv är att den utförs proaktivt och innefattar samtliga faser i hanteringen av e-legitimationen, så som beskrivs i avsnitt 2.1.

Slutligen måste kontrollen innefatta en bedömning av om de av utfärdaren vidtagna skyddsåtgärderna är tillräckliga med avseende på verksamhetens omfattning och den tillitsnivå utfärdaren verkar på, och det är då väsentligt att anslutningsavtalet är utformat på ett sätt som medger att sådana tolkningar kan göras.

6.2 Certifiering

Krav på certifiering i enlighet med principerna för ISO/IEC 27001 (och med tillitsramverket som avgränsning) inträder på tillitsnivå 4 i tillitsramverket. Certifieringskravet innebär att ledningssystemet för informationssäkerhet granskas av ackrediterad revisor, och att de kontroller som faller inom avgränsningen är på plats och fungerar. Det innebär att efterlevnaden granskas på en förhållandevis hög nivå. Kritiska säkerhetsaspekter, som t.ex. att den faktiska driftmiljön håller en hög IT-säkerhetsmässig standard, att det fysiska skyddet är lämpligt utformat och att personalen besitter rätt kompetens, är förhållanden som är svåra att avgöra vid en revision, och kräver mer ofta ingående undersökningar. Därför bör inte certifiering enligt ISO/IEC 27001 vara den enda kontrollmekanismen som tillämpas för att säkerställa kvalitet och säkerhet för svensk e-legitimation.

6.3 Tillsyn med stöd av lag

Vikten av att säkerställa funktionalitet, säkerhet och innehavarnas integritet i samband med användning av e-legitimationer kan utgöra skäl att ställa utfärdarnas verksamhet under offentlig tillsyn med stöd av lag.

Tillsynsmyndigheten kan då meddela de förelägganden som behövs för efterlevnaden av denna lag eller de föreskrifter som har meddelats med stöd av lagen, och att beslut om föreläggande kan förenas med vite i den mån det anses nödvändigt för att nå rättelse.

Inom ramarna för Svensk e-legitimation har någon lagstadgad tillsynsroll emellertid inte bedömts nödvändig, med hänsyn till de starka civilrättsliga avtalsrelationer som skapas mellan samtliga deltagande parter. Ändrade förutsättningar på området, exempelvis genom allvarliga incidenter eller tvingande Europeisk lagstiftning, kan dock leda till ett behov av att framöver se över möjligheterna att även ställa utfärdarnas verksamhet under offentlig tillsyn med stöd av lag.

6.4 Säkerhetsskyddad upphandling

För verksamheter som stöder utfärdande av e-legitimationer enligt högsta tillitsnivå, och till vilket säkerhetsberoendet kan komma att bli särskilt kritiskt, kan en möjlighet vara att teckna säkerhetsskyddsavtal (SUA-avtal) med leverantörerna av ID-tjänster, i enlighet med 8 § säkerhetsskyddslagen.

Verksamhet som omfattas av säkerhetsskyddslagen ska ha det säkerhetsskydd som behövs med hänsyn till verksamhetens art, omfattning och övriga omständigheter. Ansvaret för säkerhetsskyddet ligger hos den som är verksamhetsansvarig. För att tillgodose kravet på säkerhetsskydd när sådan verksamhet utförs på uppdrag av en myndighet, ska den uppdragsgivande myndigheten träffa ett skriftligt avtal – säkerhetsskyddsavtal – med leverantören om det säkerhetsskydd som behövs i det enskilda fallet. Denna process benämns säkerhetsskyddad upphandling.

Säkerhetsskyddet ska förebygga:

1. Att hemliga uppgifter obehörigen röjs, ändras eller förstörs (informationssäkerhet),

2. Att obehöriga får tillträde till platser där de kan få tillgång till uppgifter som avses i punkt 1 eller där verksamhet som har betydelse för rikets säkerhet bedrivs (tillträdesbegränsning),

3. Att personer som inte är pålitliga från säkerhetssynpunkt deltar i verksamhet som har betydelse för rikets säkerhet (säkerhetsprövning).

Myndigheten kan meddela egna föreskrifter inom det aktuella verksamhetsområdet om verkställigheten av säkerhetsskyddslagen, och formerna för tillsyn regleras sedan i säkerhetsskyddsavtalet. Säkerhetsskyddet hos företag som har träffat säkerhetsskyddsavtal ska kontrolleras av den myndighet som har ingått avtalet. Försvarsmakten och Säkerhetspolisen kan också i samråd med myndigheten utföra kontroll av säkerhetsskyddet. Att ett säkerhetsskyddsavtal har slutits innebär inte att säkerhetsskyddslagen blir tillämplig på hela företagets verksamhet, utan kan preciseras till vad som behövs i det aktuella uppdraget.

7 Förslag till dokumentstruktur

Det nationella tillitsramverket blir en central komponent i den basstruktur som E-legitimationsnämnden äger och förvaltar. Detta nationella tillitsramverk bör vila på vedertagna principer och formulera säkerhetsmålsättningar (regler) på en tillräckligt hög nivå för att bli ett långsiktigt, stabilt och vederhäftigt dokument.

De olika aktörerna bör därvid ges utrymme att lösa säkerhetsmålsättningarna på ett effektivt sätt som passar den egna verksamheten, för att på så sätt undvika att tillitsramverkets regler leder till onödigt kostnadsdrivade lösningar och minskad användbarhet. Det bör vara möjligt för den enskilda aktören att utforma sina egna kontroller som säkerställer att den angivna skyddsnivån uppnås och upprätthålls. Det bör också vara möjligt att utelämna målsättningar som formuleras i tillitsramverket, men som inte är tillämpliga i den egna verksamheten. Detta förutsätter att aktören kan redogöra för på vilket sätt målsättningen inte är tillämplig, och hur denne uppnår en motsvarande säkerhetsgrad genom t.ex. kompenserande kontroller.

Det föreslås därför att det i tillitsramverket formuleras de övergripande och långsiktiga reglerna och säkerhetsmålsättningarna, och att tillitsramverket kompletteras med ett vägledningsdokument, som från tid till annan närmare anger hur efterlevnad kan uppnås. Vägledningen bör utarbetas mot bakgrund av utvecklingen i omvärlden och i samråd med utfärdare och förlitande e-tjänster. Här kan ges utrymme för att på en mer detaljerad nivå beskriva syfte och innebörd av respektive regel, samt ge exempel på hur den avsedda skyddsnivån kan uppfyllas. Vägledningen bör också belysa sådana tekniska säkerhetsaspekter som är av sådan karaktär att de kan tänkas ändras förhållandevis ofta eller med kort varsel.

Vägledningsdokumentet bör betraktas utifrån att aktörer inte ska göra en väsensskild annan tolkning av tillitsramverkets säkerhetsmålsättningar. Det står dock aktörerna själva fritt att välja och kombinera kontroller lämpliga i sammanhanget för att uppnå målsättningen. Vägledningen blir därmed också det dokument som tillsammans med tillitsramverket ligger till grund för extern granskning och uppföljning av aktörernas säkerhetsarbete.

Vid sidan om tillitsramverket och vägledningen bör nämnden upprätta och underhålla ett överensstämmelsedokument, som på ett tydligt sätt redogör för hur det svenska tillitsramverket förhåller sig till motsvarande internationella standarder eller de-facto standarder, och visa på eventuella avsteg eller alternativa vägar nämnden valt för Svensk e-legitimation.

8 Utkast till ett svenskt tillitsramverk

Kraven i detta utkast till tillitsramverk gäller tillitsnivå 2 till 4. I enlighet med resonemanget i avsnitt 4.7, definieras inte krav för utfärdande på tillitsnivå 1. Kravuppfyllnad ska tolkas så att om tillitsnivå inte finns angivet, så ska kravet uppfyllas på samtliga nivåer. Krav som anges för en lägre nivå ska bortses från om annat krav finns formulerat för den aktuella nivån. Annars ska kravet på närmast lägre nivå uppfyllas. Som alternativ till ett krav på en given nivå får kravuppfyllnad göras på en högre nivå. Krav på olika nivåer är aldrig kumulativa.

8.1 Organisation och styrning

Övergripande krav på verksamheten

K1.1. Utfärdare av Svensk e-legitimation ska drivas som ett registrerat bolag samt teckna och vidmakthålla för verksamheten erforderliga försäkringar.

K1.2. 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.

K1.3. Utfärdare ska förfoga över tillräckliga ekonomiska medel för att kunna bedriva verksamheten i minst 1 år och bära risken för skadeståndsskyldighet.

Informationssäkerhet

K1.4. 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, resurstilldelning samt tekniska respektive administrativa säkerhetsåtgärder, och utgöra en kvalitetsprocess som kontinuerligt utvärderar och anpassar verksamheten till aktuella 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.

K1.5. Ledningssystemets mognadsgrad

Nivå 3: Ledningssystemet för informationssäkerhet ska följa ISO/IEC 27001, och inom avgränsningen för detta inkludera samtliga krav som ställs på utfärdare av Svensk e-legitimation på Nivå 3.

Nivå 4: Ledningssystemet för informationssäkerhet ska vara certifierat enligt ISO/IEC 27001 av ackrediterad revisor. Avgränsningen för certifieringen ska inkludera samtliga

krav som ställs som utfärdare av Svensk e-legitimation på Nivå 4.

Villkor för underleverantörer

K1.6. 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.

Handlingars bevarande

K1.7. 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 och kontrollerna fungerar.

K1.8. 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.

Granskning och uppföljning

K1.9. 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.

8.2 Fysisk, administrativ och personorienterad säkerhet

K2.1. 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 tillträde till dessa utrymmen kontinuerligt övervakas.

K2.2. Innan en person antar någon av de roller som identifierats i enlighet med K1.4a, 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 tillfredsställande, korrekt och säkert sätt.

8.3 Teknisk säkerhet

K3.1. Utfärdare ska kunna visa att de tekniska kontroller som finns införda är tillräckliga för att uppnå den skyddsnivå som behövs med hänsyn till verksamhetens art, omfattning och övriga omständigheter, och att dessa kontroller fungerar och är effektiva.

K3.2. Kommunikation mellan komponenter över allmänna telekommunikationsnät eller andra kommunikationslänkar som inte är fysiskt skyddade i enlighet med K2.1, ska begränsas och ömsesidigt identifieras med en styrka som minst motsvarar kraven för Svensk e-legitimation (för den aktuella nivån), samt skyddas mot insyn, manipulation och återuppspelning.

K3.3. 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) nyckelmaterialet skyddas när det inte är under användning, direkt eller indirekt, via kryptografisk hårdvarumodul med aktiva säkerhetsmekanismer som skyddar mot både fysiska och logiska försök att röja nyckelmaterialet.

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

(e) **Nivå 3:** Aktiveringsdata för skydd av nyckelmaterial hanteras genom flerpersonkontroll.

K3.4. Utfärdaren ska ha en dokumenterad och fungerande process för styrning och ändring av IT-system i enlighet med vedertagna principer, och som innefattar kontinuerlig omvärldsbevakning av de produkter och tekniker som används i tjänsten, samt ändamålsenlig beredskap för förändrade risknivåer.

8.4 Ansökan, identifiering och registrering

Information om villkor

K4.1. Utfärdaren ska tillhandahålla uppgifter om avtal, villkor samt anknytande uppgifter och eventuella begränsningar i användandet av tjänsten till anslutna användare, e-tjänsteleverantörer och andra som kan komma att förlita sig på utfärdarens tjänst.

K4.2. 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.

K4.3. Utfärdaren ska tillhandahålla en utfärdardeklaration som bl.a. innefattar:

(a) bolagets identitet och kontaktuppgifter,

(b) beskrivning av de regler och rutiner som utfärdaren tillämpar för att uppfylla kraven i tillitsramverket,

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

(d) tillvägagångssätt för 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.

Nivå 3: På begäran, av e-legitimationsnämnden eller andra som har ett berättigat intresse, redogöra för ägarstruktur och grunder för bolagsstyrning.

K4.4. Utfärdare av Svensk e-legitimation ska inhämta användarens samtycke vid nyteckning eller ändring av tjänsten, samt regelbundet var 5:e år.

K4.5. En utfärdare av Svensk e-legitimation som upphör med sin verksamhet ska informera sina användare och E-legitimationsnämnden. Utfärdaren ska hålla arkiverat material tillgängligt i enlighet med K1.7.

Ansökan

K4.6. Ansökningsförfarandet

Nivå 2: Svensk e-legitimation får utfärdas endast efter skriftlig ansökan i elektronisk eller traditionell form. Sökanden ska intyga att lämnade uppgifter är riktiga och fullständiga.

Nivå 3: 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.

K4.7. Förenklat ansökningsförfarande

Nivå 3: Om en sökande redan har identifierats (i enlighet med K4.10 Nivå 3) för ekonomiskt eller rättsligt betydelsefulla mellanhavanden, och sökanden kan identifieras på annat tillförlitligt sätt som är likvärdigt med kraven för Svensk e-legitimation Nivå 3, får utfärdaren identifiera och ta emot ansökan genom denna tjänst i stället för enligt K4.6.

Nivå 4: Ej tillämpligt.

K4.8. 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.

Fastställande av sökandens identitet

K4.9. Kontroll av uppgifter

Nivå 2: Utfärdare av Svensk e-legitimation ska kontrollera att de uppgifter som sökanden lämnat är fullständiga och stämmer överens med uppgifter som finns registrerade i ett officiellt register.

Nivå 3: Utfärdare av Svensk e-legitimation ska kontrollera att ansökan om e-legitimation är behörigen undertecknad på papper eller lämnad elektroniskt enligt K4.7, och att de uppgifter som sökanden lämnat är fullständiga och stämmer överens med uppgifter som finns registrerade i ett officiellt register.

K4.10. Identifiering av sökanden

Nivå 2: Utfärdare av Svensk e-legitimation på Nivå 2 som identifierar sökanden **på distans**, ska tillhandahålla e-legitimationen i enlighet med K5.5 Nivå 2.

Nivå 3: Utfärdare av Svensk e-legitimation på Nivå 3 som identifierar sökanden **på distans**, ska göra detta i en relation som avser ekonomiskt eller rättsligt betydelsefulla mellanhavanden på det sätt som anges i K4.7.

Nivå 3: Utfärdare av Svensk e-legitimation på Nivå 3 som identifierar sökanden **vid personligt besök**, ska fastställa dennes identitet genom kontroll av fullgod identitetshandling.

Nivå 4: Utfärdare av Svensk e-legitimation på Nivå 4, ska kontrollera sökandens identitet vid ett **personligt besök**, på likvärdigt sätt som vid en ansökan om en traditionell identitetshandling.

Registrering

K4.11. Utfärdare ska, beaktat reglerna för persondataskydd, föra register över anslutna användare och de tilldelade elektroniska identitetshandlingarna, och hålla detta register aktuellt.

8.5 Utfärdande och spärr av e-legitimation

Utformning av tekniska hjälpmedel

K5.1. Tekniska hjälpmedel

Nivå 2: Tekniska hjälpmedel för elektronisk identifiering genom Svensk e-legitimation på Nivå 2, ska utformas så att användaren tilldelas en eller flera personliga koder som användaren brukar för att identifiera sig.

Nivå 3: Tekniska hjälpmedel för elektronisk identifiering genom Svensk e-legitimation på Nivå 3, ska utformas enligt sådan tvåfaktorsprincip att en del består i elektroniskt lagrad information som användaren ska inneha, och en del i det som användaren ska bruka för att aktivera e-legitimationen (personlig kod).

Nivå 4: Tekniska hjälpmedel för elektronisk identifiering genom Svensk e-legitimation på Nivå 4 ska utformas enligt sådan tvåfaktorsprincip att en del består i en personlig säkerhetsmodul som användaren ska inneha, och en del i det som användaren ska bruka för att aktivera säkerhetsmodulen (personlig kod).

K5.2. Aktiveringsmekanismen och personlig kod ska utformas så att det är osannolikt att en utomstående kan forcera skyddet, ens på maskinell väg.

K5.3. Användare av Svensk e-legitimation ska på eget initiativ kunna byta personlig kod, och genom automatisk framställning eller genom vägledning få hjälp att upprätthålla kraven i K5.2.

K5.4. Utfärdare av Svensk e-legitimation ska säkerställa att alla sökande tilldelas en unik elektronisk identitet som är entydigt kopplad till den tillhandahållna e-legitimationshandlingen.

Tillhandahållande av e-legitimationshandling

K5.5. Tillhandahållande

Nivå 2: En utfärdare av Svensk e-legitimation **på distans** ska tillhandahålla personlig kod som användaren ska bruka för att aktivera e-legitimationen, på ett sätt som bekräftar att denne kan ta emot reguljär post på folkbokföringsadressen.

Nivå 3: En utfärdare av Svensk e-legitimation som **vid personligt besök** eller via elektroniskt förfarande som är förenligt med K4.7, 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.

Nivå 4: En utfärdare av Svensk e-legitimation på Nivå 4 ska **vid personligt besök** tillhandahålla den elektroniska legitimationshandlingen, och ska också tillhandahålla personlig kod som användaren ska bruka för att aktivera e-legitimationen på ett sätt som bekräftar att denne kan ta emot reguljär post på folkbokföringsadressen.

Spärrtjänst

K5.6. 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).

K5.7. 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.

8.6 Verifiering av elektronisk identitet

Utställande av identitetsintyg

K6.1. Utfärdare av Svensk e-legitimation som tillhandahåller tjänst för utgivning av identitetsintyg till förlitande e-tjänster, ska tillse att denna tjänst har god tillgänglighet och att utlämnande av identitetsintyg föregås av en tillförlitlig kontroll av den angivna elektroniska identiteten och den elektroniska identitetshandlingens giltighet.

Nivå 4: Intygen ska vara starkt kryptografisk kopplade till användarens e-legitimationshandling.

K6.2. 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 endast är läsbar för den avsedda mottagaren, och att den som tar emot intyget kan kontrollera att mottagna intyg är äkta.

K6.3. Utfärdaren ska kunna påvisa att tekniska säkerhetskontroller införts vid kontroll av elektroniska ID-handlingar och vid utfärdande av identitetsintyg, så att det är osannolikt att utomstående genom gissning, avlyssning, återuppspelning eller manipulation av kommunikation kan forcera skyddsmekanismerna.

A Överensstämmelse med Kantara IAF

Tabellen i figur A.1 visar hur det föreslagna tillitsramverket förhåller sig till motsvarande Kantaras *Service Assessment Criteria* version 2.0.

Som tidigare nämnts är kravformuleringen i Kantaradokumenten på en lägre nivå än vad som föreslås för Svensk E-legitimation, och att flertalet krav inte är fullt tillämpliga under svenska förhållanden. Det innebär att det finns ett visst tolkningsutrymme i översättningen, och matrisen bör läsas från den synvinkeln.

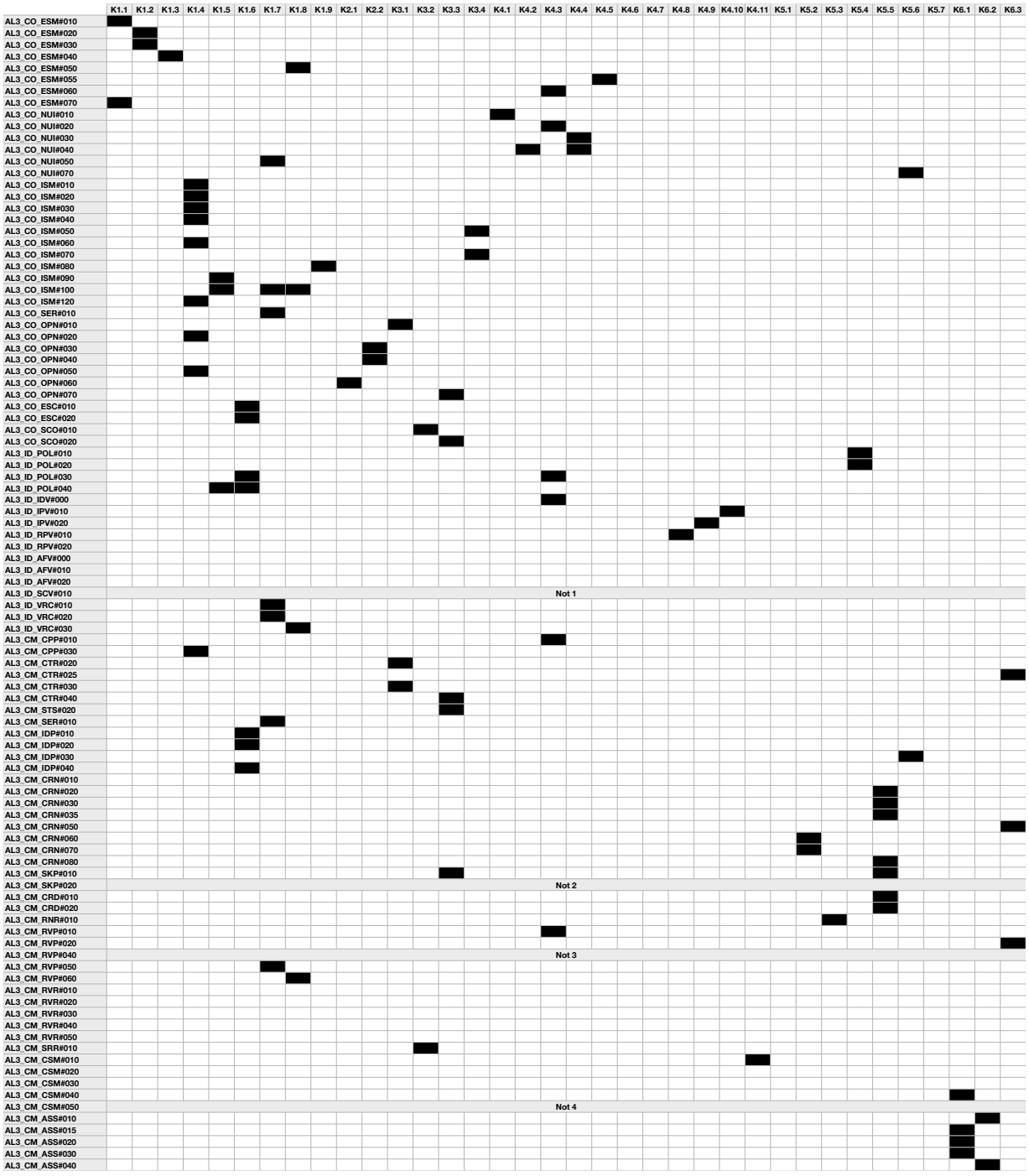
Följande kriterier i Kantara-dokumentet har inte sina motsvarigheter i det föreslagna tillitsramverket:

Not 1 Kriteriet **AL3_ID_SCV#010** rör ytterligare kontroller vid tillhandahållandet av e-legitimationshandlingen, för att säkerställa att de uppgifter som ligger till grund för utgivningen (företrädesvis folkbokföringsadressen) är aktuella. Detta genom att t.ex. fördröja tillhandahållandet av kvittens eller aktiveringskod. Detta krav skulle påföra fördröjningar som särskilt i utfärdande av e-legitimation på distans kan medföra alltför stora olägenheter och bli kostnadsdrivande, samtidigt som nyttan av att fördröja tillhandahållandet kan ifrågasättas. Andra kompletterande kontroller föreslås istället formuleras i riktlinjerna.

Not 2 Kriteriet **AL3_CM_SKP#020** rör situationer då innehavaren framställer sitt egna nyckelmaterial att använda i tvåfaktorsautentiseringen. Det föreslagna tillitsramverket gör emellertid ingen skillnad på vem eller var nyckelmaterialet framställs, det ska framställas på ett säkert sätt. Kravet utgår därför.

Not 3 Kriteriet **AL3_CM_RVP#040** saknar relevans i en Svensk anpassning.

Not 4 Kriteriet **AL3_CM_CSM#050** innebär att en e-legitimation som inte använts de senaste 18 månaderna automatiskt ska spärras (även om dess giltighetstid i övrigt sträcker sig längre) kan leda till ett resursslöseri i vissa fall. Idag utfärdas fotolegitimation på kort som även innehåller e-legitimation, där giltighetstiden är 5 år. En person som erhåller en e-legitimation på sådant kort kanske inte omedelbart använder denna, eftersom det primära syftet var att skaffa en fotolegitimation. Det är dock svårt att se någon rimlig anledning till att e-legitimationen skall bli ogiltig efter 18 månader, om legitimationshandlingen i övrigt är giltig ytterligare flera år. Detta kan förväntas bli särskilt kostnadsdrivande, varför kravet föreslås lämnas helt utan avseende.



Figur A.1 – Översättningsmatris mellan Kantara IAF SAC 2.0 och det föreslagna svenska tillitsramverket