IAM Strategi

Med kommunernas behov i fokus

- Endast nuläge -

Innehåll

Bilagor

Bilaga 1 – Regulatoriska krav

Revisionshistorik

Version	Datum	Författare	Kommentar
0.1	2020-03-13		Första utkast för diskussion i arbetsgruppen
0.2	2020-03-19		Andra utkast efter diskussion i arbetsgruppen
0.3	2020-03-25		Tredje utkast efter diskussion i intervjugruppen
0.4	2020-03-31		Fjärde utkast för korrektur i intervjugruppen
0.5	2020-04-09		Femte utkast efter korrektur av nuläget (v0.4) i intervjugruppen och sammanflätning med mål (v0.3) och strategi (v0.2) som vuxit fram parallellt med nuläget. Kompletterande regulatoriska krav är också inflätade. Ett avsnitt om förslag till beslut har lagts till.
0.6	2020-04-16		Sjätte utkast efter inspel från styrgrupp med flera. Beslut att lägga regulatoriska krav i bilaga.
0.7	2020-04-21		Sjunde utkast efter en andra korrektur i intervjugrupp och styrgrupp samt inspel från arbetsgruppen.
0.9	2020-04-28		Utdrag innehållande endast nuläget i väntan på beslut av strategin i sin helhet.
1.0	2020-05-05		Beslutad version för publicering

1. Inledning

1.1 Dokumentets syfte och målgrupp

Detta dokument är utdrag ur *Ineras strategi för identitet och åtkomst (IAM) med kommunernas behov i fokus* innehållande endast nuläget i väntan på beslut av strategin i sin helhet.

1.2 Kort om IAM

Identity and Access Management (IAM) syftar till att fastställa vilka användare som kan få tillgång till en organisations informationstillgångar och till vilken grad de får behandla informationen med verksamhetskraven och de regulatoriska krav som verksamheten är förenad med som grund.

Styrning av åtkomst är en betydande del i det strukturerade informationssäkerhetsarbetet och för informationstillgångar med ett högt skyddsvärde är det en rad grundläggande processer som måste finnas på plats och över tid väl fungerande rutiner som informationstillgångarnas ägare ytterst ansvarar för. Tillgångens ägare fastställer lämpliga regler för styrning av åtkomst, rättigheter och begränsningar för specifika roller. Detaljrikedomen, och hur stränga säkerhetsåtgärderna är, avspeglas i de säkerhetsrisker som är förknippande med informationen.

De regulatoriska kraven på åtkomst inom en kommun är omfattande. De för en kommun vanligaste regulatoriska kraven redovisas i bilaga 1 för att ge läsaren en orientering i kravmassan utan att för den skull ha ambitionen att sammanställningen är uttömmande.

Läsaren av detta dokument förväntas ha grundläggande förståelse om IAM-området.

2. Nuläge

Nuläget har bestämts genom intervjuer med ett 50-tal representanter från Sveriges kommuner . Intervjuerna har skett med ett enklare intervjuunderlag som grund. Intervjuerna har förts i förutsättningslösa samtal om behov och utmaningar utifrån ett kommunalt IAM perspektiv för att inte låsa diskussionen om nuläget i en riktning.

Med hänsyn till sekretess är inte enskilda kommuners behov eller utmaningar beskrivna eller exemplifierade utan skrivningarna är gjorda på en sådan nivå att information inte röjs. Undantaget det som redan är allmänt känt eller är publikt.

Beskrivningen av nuläget följer strukturen i standarden för ledningssystem för informationssäkerhet SS-ISO/IEC 27001 och SS-ISO/IEC 27002 avseende styrning av åtkomst.

Nuläget har kompletterats med ett avsnitt om de regulatoriska kraven avseende åtkomst som en kommun har att förhålla sig till i syfte att tydliggöra de krav som ytterst reglerar området.

Därutöver finns det ett par områden som inte direkt relaterar till IAM men som ändå återkommit i intervjuerna varför de kort har belysts.

2.1 Avgränsningar

Områden som i huvudsak är administrativa och organisatoriska har avgränsats:

- Regler för styrning av åtkomst
- Granskning av användares åtkomsträttigheter
- Hantering av användares konfidentiella autentiseringsinformation
- Användaransvar
- Begränsning av åtkomst till information

Vi har också valt att avgränsa områden som inte lyfts fram inom intervjuerna såsom:

- Hantering av privilegierade åtkomsträttigheter
- System för lösenordshantering
- Användning av privilegierade verktygsprogram
- Åtkomstkontroll till källkod för program

2.2 Kommunernas nuläge avseende IAM

2.2.1 Registrering och avregistrering av användare

Intervjuerna visar att allt fler kommuner har en livscykelhantering för användaridentiteter i exempelvis en kommungemensam katalog. Uppfattningen är att allt fler har HR- och elevadministrativa system som grund för användarhanteringen. Kvalitén i dessa register varierar. Det går exempelvis inte med säkerhet säga att all personal har legitimerat sig vid anställningen och källsystemen är i högst varierad grad avstämda med folkbokföringsdatabasen[1] hos Skatteverket.

I utbildningsverksamheten råder det en stor frihetsgrad varför det inte går att säga att alla skolor är en del av en kommungemensam infrastruktur utan där är variationen mycket stor. Det är mer regel än undantag att kommunen som skolhuvudman har en väg fram och en enskild skola en annan. Vikarier och timanställda lyfts också fram som en grupp som inte är en självklar del. Andra hanteringar som varierar mellan kommuner är hur externa utförare, anhöriganställningar och personliga assistenter hanteras.

Sammantaget går det att se en mognadstrappa där olika kommuner befinner sig på olika steg där spännvidden från de som står på första steget till de som står på det översta steget är stor. Det går inte entydigt att säga att mognadsgraden är kopplat till storleken på kommunen utan uppfattningen är att det är flera olika faktorer som spelar in där ledning och styrning är en viktig faktor.

Vad gäller kopplingen till folkbokföringsdatabasen är det noterbart att merparten av de intervjuade inte bara har en lösning utan ofta flera lösningar, ibland från samma leverantör, för indirekt åtkomst till Skatteverkets aviseringstjänst Navet[2]. Kännedomen i kommunerna om Ineras Personuppgiftstjänst[3] är låg.

I intervjuerna är det också tydligt att förmågan är bättre på att föda en källa med användaridentiteter än att upprätthålla dess aktualitet över tid. I de fall det finns en integration med HR- och elevadministrativa system är uppfattningen att de även avregistreras på ett kontrollerat sätt. Om modet finns, ska tilläggas, här vittnar flera om att de inte riktigt vågar avregistrera alla konton med risk för att det blir fel, utan flera uppger att inaktiverade konton är en väg fram.

---

1 https://www.skatteverket.se/omoss/varverksamhet/offentligauppgifter/vilkaregisterfinnshosskatteverket/folkbokforing.4.2cf1b5cd163796a5c8bd9b5.htm

2 https://www.skatteverket.se/foretagochorganisationer/myndigheter/informationsutbytemellanmyndigheter/navethamtauppgifteromfolkbokforing.4.18e1b10334ebe8bc80001754.html

3 https://www.inera.se/personuppgiftstjansten

Bredden på den kommunala verksamheten gör också att det finns ett ökande behov att använda olika typer av identitetsbegrepp, från lokala identitetsbegrepp, skolgemensamma (ex eppn[4]), vårdgemensamma (ex HSA-id[5]) till nationella (ex personnummer) identitetsbegrepp. Det var inte några större diskussioner kring samordningsnummer i intervjuerna men det kan antas att det blir ett växande problem även i kommunerna. Det är en förhoppning att den statliga utredningen *Åtgärder för att minska fel i folkbokföringen* (Dir 2019:54)[6] adresserar exempelvis brister i tillit till uppgifterna.

I relationer över organisationsgränser uppfattas en önskan att ingå i en federation, dvs att det egna registret över användaridentiteter ligger till grund vid åtkomst även till regionala och nationella tjänster. I första hand via identitetsintyg som utfärdas av kommunen eller av en betrodd part, i andra hand genom provisionering med kommunens källa av användaridentiteter som grund för överföring av användaruppgifter till tjänsten i förväg. Det är också en önskan om att sektorsövergripande lösningar för autentisering frikopplas från behörighetshanteringen. I sammanhanget är det också viktigt att inte glömma perspektivet single sign-on (SSO). Det blir i värsta fall en isolerad företeelse i den egna organisationen som inte sträcker sig utanför den egna organisationsgränsen.

Skolfederation är den federation som samlat flest medlemmar, 70% av elevernas kommunala skolhuvudmän är medlemmar enligt Internetstiftelsen, men detta till trots är bara varannan kommun är medlem. Någon nämner svårigheten att få Microsofts lösning för federering, ADFS[7], att fungera fullt ut i en federation som en orsak, andra nämner att det är enklare att sätta upp partsrelationer direkt med leverantörerna av lärresurserna. I det senare fallet erhålls samma fördelar ur ett IAM-perspektiv men kan antas vara administrativt betungande över tid.

De lärare som intervjuats har vittnat om en besvärlig situation med en mängd olika inloggningar i flera olika plattformar, flera e-postsystem osv. Det gäller även hos skolhuvudmän som är anslutna till Skolfederation men ändå inte har implementerat nyttorna med federationen. De nämner även att de har egna lösningar (t o m privata lösningar) för exempelvis filhantering och e-post för att de inte litar på lösningarna som tillhandahålls. Ur deras perspektiv är SSO långt från en realitet.

Digitala nationella prov (DNP)[8] från Skolverket är en ny drivkraft för att ansluta sig till Skolfederation eller andra av Skolverket godkända federationer. DNP kommer också att ställa krav på provisionering med den svenska standarden SS 12000[9] som grund. Här kommer den

---

[4] https://wiki.refeds.org/pages/viewpage.action?pageId=44957737#eduPerson2016-02-eduPersonPrincipalName

[5] https://www.inera.se/globalassets/tjanster/katalogtjanst-hsa/dokument/styrande-dokument/informationsspecifikation_for_katalogtjanst_hsa.pdf

[6] https://www.regeringen.se/rattsliga-dokument/kommittedirektiv/2019/09/dir.-201954/

[7] https://docs.microsoft.com/en-us/windows-server/identity/active-directory-federation-services

[8] https://www.skolverket.se/om-oss/var-verksamhet/skolverkets-prioriterade-omraden/digitalisering/digitala-nationella-prov/digitalisering-av-de-nationella-proven

[9] https://www.sis.se/produkter/informationsteknik-kontorsutrustning/ittillampningar/ittillampningar-inom-utbildning/ss-120002018/

centrala källan i kommunerna för elevidentiteter att ställas på prov då Skolverket förutsätter att kommunen kan provisionera en rad elevrelaterade attribut[10]. Inte minst mot bakgrund av att alla skolor i kommunen inte nödvändigtvis är en del av den kommungemensamma källan för detta.

Även inom vården ställs det krav på provisionering, exempelvis HSA[11] där personal som ska använda nationella tjänster måste finnas med. Provisioneringen till HSA sköts av de flesta vi har intervjuat helt manuellt, oftast av omsorgsverksamheten. Ett hinder för att automatisera provisioneringen av HSA är att det ställs krav på anslutning till Sjunet[12]för åtkomst till integrationsgränssnittet mot HSA.

En växande dimension inom användarhantering är när en användare inte är en fysisk person utan en tingest eller sak. Tillväxten av sakernas internet (IoT), gör att antalet identiteter kommer att öka drastiskt. Det samma gäller robotiserade processer (RPA) där identitetsbegreppet tenderar till att närma sig en fysisk person i det dagliga talet om digitala medarbetare. Intervjuerna visar att RPA för det stora flertalet är ett integrationsgränssnitt i frånvaro av integrationsgränssnitt i verksamhetssystemen. Detta till trots är det ett växande område att ta hänsyn till. Hos Inera pågår ett utredningsuppdrag[13] hur RPA påverkar de nationella tjänsterna som kan ge kommunerna viss vägledning i frågeställningarna.

2.2.2 Tilldelning av användaråtkomst

I de flesta kommuner finns det en eller flera centrala kataloger som grund för övergripande åtkomst. De används av allt fler system som har förmåga att integreras med en katalogtjänst, inte sällan Microsoft AD, eller som har förmåga att konsumera identitetsintyg[14] med en katalog som grund. Dessa integrationer möjliggör också SSO vilket vi uppfattar att de flesta intervjuade kommuner har genomfört. Flera kommuner vittnar om att de mest frekvent använda system i kommunen har SSO även om verksamheterna inte alltid delar den bilden, vilket inte minst medarbetare med mobila arbetssätt vittnar om. Tydligt är att appar inte kan inkluderas i den här bilden då app-leverantören oftast utvecklat egna lösningar för åtkomst och därmed inte drar nytta av den kommungemensamma infrastrukturen.

I katalogen skapas ofta användarroller och andra behörighetsstyrande attribut som kan ligga till grund för åtkomst i verksamhetssystemen, men de används sällan. Den granulära åtkomsttilldelningen görs i verksamhetssystemen. Flera av de större förekommande verksamhetssystemen i kommunerna uppfattas inte ha förmågan att konsumera åtkomsträttigheter från någon annan källa än det egna systemets källa för åtkomsträttigheter. Ur det kommunala perspektivet är uppfattningen den samma oavsett om det är lokala, regionala eller nationella system, även om det finns exempel på separerade källor för åtkomsträttigheter

---

[10] https://www.skolfederation.se/teknisk-information/attribut/

[11] https://www.inera.se/tjanster/katalogtjanst-hsa/

12 https://www.inera.se/kundservice/dokument-och-lankar/tjanster/hsa/

[13] https://www.inera.se/aktuellt/programkontorets-arendelista/pagaende-arenden/identitet-och-atkomst-for-rpa-robotar/

[14] https://elegnamnden.se/download/18.4498694515fe27cdbcf13a2/1513326654206/E-legitimationsn%C3%A4mndens-tekniska-ramverk.version1.5.pdf

men de är i sin tur frånskilda kommunernas centrala lösningar varför de uppfattas som sektorsspecifika lösningar, exempelvis HSA.

2.2.3 Borttag eller justering av åtkomsträttigheter

I de fall en kommungemensam källa finns för identiteter och att det finns en integration med HR-system och elevadministrativa system är uppfattningen att avregistrering eller inaktivering av användarkonton också leder till att åtkomsten till verksamhetssystemen stryps. Detta under förutsättning att verksamhetssystemet har någon form av relation med de kommungemensamma källorna, exempelvis via en kommungemensam katalog.

Uppfattningen är vidare att den granulära åtkomsttilldelningen inte med självklarhet följer förändringar som borde påverka åtkomsttilldelningen. Exempelvis när en anställd byter tjänst.

2.2.4 Säkra inloggningsrutiner

Kommunerna har i allt högre grad anammat de nationella definitionerna av tillitsnivåerna[15] som Myndigheten för Digital förvaltning (DIGG) definierat för att bestämma graden av tillit till en uppgiven identitet. Det finns också en växande förmåga att utifrån informationens skyddsvärde ställa krav på en nivå av tillit som krävs för åtkomst till en informationstillgång. I exempelvis SKR:s verktyg KLASSA[16] finns en tydlig relation mellan informationens skyddsvärde och val av tillitsnivå. Den ökade förståelsen ligger också till grund för val av tekniska lösningar för autentisering och för själva utfärdandet av handlingen.

I intervjuerna kan konstateras att det är främst utmaningar och behov kring stark autentisering och tillitsnivå 3 som diskuterats. Ingen har i någon större grad fört diskussioner om utmaningar och behov kring autentisering på lägre grader av tillit varför det avgränsas från det fortsatta resonemanget.

Vad gäller tillitsnivå 3 och stark autentisering så anser flera att det inte är tydligt uttryckt vad som gäller och vad det innebär. Datainspektionen har uttryckt stark autentisering i ett antal tillsynsärenden när åtkomst till känsliga personuppgifter ska ske över öppna nät såsom internet och Sjunet utan att närmare specificeras vad som avses. Flera kommuner uppfattar att det är olyckligt att Datainspektionen inte uttrycker att det är tillitsnivå 3 i enlighet med DIGG's tillitsramverk som avses. Samtidigt ska det ses i ljuset av att försörjningen av godkända e-legitimationer på tillitsnivå 3 inte anses tillräcklig vilket ger en något större frihetsgrad.

I samband med de digitala nationella proven kommer Skolverket att ställa krav på stark autentisering för lärarna, sannolikt inte på tillitsnivå 3 på grund av den låga försörjningen på marknaden och det stora antalet lärare.

---

15 https://www.elegnamnden.se/elegitimering/kvalitetsmarketsvenskelegitimation/omtillitsnivaerforelegitimering.4.4498694515fe27cdbcf101.html

16 https://klassa-info.skl.se/

Uppfattningen är att de flesta kommunerna inte ser SITHS[17] som en lösning som rullas ut på bred front, utan det är en sektorsspecifik lösning endast för de användare som har behov av åtkomst till de nationella tjänsterna inom vård och omsorg vilka enbart stödjer SITHS. Det finns ett missnöje från början av 2010-talet när kommunerna tvångsanslöts till SITHS-konceptet för att möjliggöra åtkomst till nationella tjänster som Pascal som också behöver beaktas. Utan någon inbördes ordning nämns bland annat frånvaro av mobilanpassning, en begränsad RFID implementation (enbart stöd för MIFARE Classic som anses osäkert), samexistens med andra kort, utgivningsprocessen och kostnaden som hinder för ett breddinförande av SITHS.

Det finns en förståelse att exempelvis utgivningsprocessen för en e-legitimation på tillitsnivå 3 måste vara rigorös. Här nämns förslaget i den statliga utredningen *Ett säkert statligt ID-kort – med e-legitimation* (SOU 2019:14)[18] som möjliggörare där id-växling tillåts från en statlig e-legitimation på nivå 4. Vad gäller id-växling nämns också det faktum att Finansiell ID-teknik inte tillåter id-växling från exempelvis ett mobilt BankID vilket annars hade kunnat förenkla ett eget utfärdande. I sammanhanget nämns också att Freja eID Plus medger ID-växling, förutsatt att det avtalats. Under intervjuerna har frågan ställts om id-växling är tillåten med SITHS, vilket Inera inte ser några hinder med. Även Skatteverkets E-legitimation (AB Svenska Pass) används för id-växling, bland annat i eduID.

Uppfattningen är vidare att allt fler kommuner löser sin egen försörjning med marknadens aktörer som stöd för att möta det egna behovet av stark autentisering, men utan någon egentlig strävan att möta de krav som följer av DIGG's tillitsramverk på nivå 3. Det finns något enstaka undantag som har för avsikt att bli godkända utfärdare. Uppfattningen är också att kommunen kommer att ha flera lösningar och över tid olika lösningar för stark autentisering. Detta ses inte som något negativt utan är en naturlig väg fram för att kunna möta dagens och morgondagens behov.

Den som har erfarenhet av att implementera en e-legitimation som godkänts av DIGG (då E-legitimationsnämnden) på nivå 3 konstaterar att det var förgäves eftersom tjänster utanför den egna organisationen ändå inte accepterade den e-legitimationen trots att den var godkänd. I sammanhanget uttrycks därför också en önskan att de nationella tjänsterna accepterar alla godkända e-legitimationer och inte avgränsas till att exempelvis bara stödja SITHS, på samma sätt som att kommunerna försöker vara öppna för att acceptera alla godkända[19] e-legitimationer i sina tjänster.

Det lyfts en frustration över att myndigheterna såsom Försäkringskassan och CSN inte heller accepterar alla godkända E-legitimationer utan kräver att tjänstemännen i kommunerna ska använda BankID i kontakt med myndigheten. Här används i dag personnummer som identifierare, men det torde vara mer intressant att säkerställa att tjänstemannen har behörighet

---

[17] https://www.inera.se/tjanster/identifieringstjanst-siths/

[18] https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2019/03/sou-201914/

[19] https://www.elegnamnden.se/elegitimering/kvalitetsmarketsvenskelegitimation/godkandaelegitimationer.4.4498694515fe27cdbcf1a3.html

att företräda exempelvis kommunen i det aktuella ärendet, något som SKRs *Rapport enkät e-legitimationer*[20] särskilt belyser.

Återkommande lyfts också diskussionen huruvida exempelvis ett mobilt BankID är en ”privat” e-legitimation eller inte. Det finns exempel på kommuner som framgångsrikt använder BankID i tjänsten, exempelvis för vikarier och timanställda, men också som en reservlösning om inte kommunens lösning för stark autentisering finns tillhanda. Det finns också exempel på kommuner som möter motstånd mot att använda godkända e-legitimationer på marknaden då de upplevs som privata e-legitimationer. Den diskussionen leder ofta vidare till att det egentliga motståndet rör installationen av exempelvis ett BankID på en enhet som innehavaren inte förfogar över, exempelvis en delad enhet. Det senare är för övrigt inte förenlighet med användarvillkoren för exempelvis BankID[21].

I diskussionen om behovet av ett brett införande av stark autentisering nämns också hinder i form av användare som inte förfogar över tjänstemobiler, utmaningen med att flera delar arbetsredskap, ex läsplattor, och det faktum att flera lösningar förutsätter åtkomst till ett nät.

I intervjuerna vittnar verksamheten om scenarios där vårdpersonal behöver logga in i flera olika appar, upp mot 5-8 st, på en mängd olika vis under ett 15 minuters besök. Det är tydligt att autentisering i en app befinner sig på ungefär samma nivå som inloggningen i en webbapplikation för ungefär fem år sedan där varje leverantör hade sin lösning till dess att standardiseringen[22] kring inloggning i webbapplikationer fick dagens fotfäste. Det finns en stark önskan att även autentisering i appar standardiseras och att de befintliga lösningarna i kommunen för autentisering används även här. Det finns också en önskan om modernare autentiseringslösningar, utan att för den skull göra avkall på tilliten, som bättre passar in i ett mobilt användningssätt. Exempelvis nämndes kontaktlösa e-legitimationer (så kallade dual interface kort).

[20] https://webbutik.skr.se/bilder/artiklar/pdf/7585-823-4.pdf

[21] https://online.swedbank.se/ConditionsEarchive/download?bankid=1111&id=WEBDOC-PRODE23084070

[22] http://rivta.se/documents/ARK_0046/Referensarkitektur-Identitetochatkomst-RevA.pdf

2.3 Regulatoriska åtkomstkrav ur ett kommunalt perspektiv

Inom ramen för beskrivningen av nuläget har ett tiotal regulatoriska krav identifierats som har bäring på IAM. Dessa har sammanställts i bilaga 1. Det är inte en uttömmande förteckning utan syftar till att ge en bild av utmaningen att hantera IAM i en kommun ur ett regulatoriskt perspektiv.

2.4 Övrigt

Utöver IAM har några diskussioner lyfts återkommande varför även de bör uppmärksammas.

2.4.1 Elektroniska underskrifter

Det finns en samlad bild i intervjuerna att området elektroniska underskrifter saknar tillräcklig vägledning. Marknaden tenderar till att lösa behov i stuprör utan någon som helst förståelse för de regulatoriska kraven för elektroniska underskrifter som följer av eIDAS-förordningen. Det innebär exempelvis att det görs elektroniska underskrifter som inte är arkiveringsbara. Även om formkraven[23]följs godtas inte de elektroniska underskrifterna av andra myndigheter som Polisen, Domstolsverket och Statens Institutionsstyrelse.

Osäkerheten i frågan utgör också ett hinder för den digitala dokumenthanteringen. Om sakfrågan kring den elektroniska underskriften inte undanröjs är det svårt att för att inte säga omöjligt att digitalisera processen.

En statlig utredning under benämningen *Ökad och standardiserad användning av betrodda tjänster i den offentliga förvaltningen* (Dir 2020:27) är tillsatt den 13 september i syfte att bringa klarhet i bland annat frågan om elektroniska underskrifter. Uppdraget ska redovisas senast den 30 december 2020.

2.4.2 Inlåsningseffekter

Under intervjuerna kan vi konstatera att det finns en rad inlåsningseffekter som gör det svårt att ersätta exempelvis en leverantör mot en annan utan att det får stora konsekvenser. Det faktum att ett stort antal leverantörer av verksamhetssystem fortsatt bygger in egna lösningar inom IAM-området förvånar. Detta trots att det finns en rad standarder på området såsom SAML2[24] och Open ID Connect (OIDC)[25] för att exempelvis lösa SSO och auktorisation, inte minst i appar där förmågan att nyttja kommungemensamma lösningar för identiteter och åtkomst nästan helt lyser med sin frånvaro. Ytterligare en dimension är att det inte går att kravställa på exempelvis molntjänster på samma sätt som på traditionella verksamhetssystem vilket också blir en inlåsningseffekt i sig. Inte sällan leder molntjänsterna till relativt slutna ekosystem avseende IAM.

---

[23] https://www.elegnamnden.se/eunderskrift/omeunderskrifter.4.4498694515fe27cdbcff0.html
[24] http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
[25] https://openid.net/connect/

3. Målbild

Givet det nuläge som beskrivs i denna strategi om kommunernas behov och utmaningar inom IAM har ett antal tänkbara målbilder formulerats. Till målbilder har kopplats sammanfattande resonemang från nulägesinventeringen.

Målbilderna presenteras när *Ineras strategi för identitet och åtkomst (IAM) med kommunernas behov i fokus* i sin helhet är beslutad.

4. Strategi

För att nå de målbilder som uttrycks här, givet nuläget, föreslås följande strategi.

Strategin presenteras när *Ineras strategi för identitet och åtkomst (IAM) med kommunernas behov i fokus* i sin helhet är beslutad.