Kommungemensam e-tjänstelegitimation och inloggningsmetod – behov, lösningsförslag samt rekommendationer

Sammanfattning

Denna förstudie har undersökt behoven av en gemensam e-tjänstelegitimation i Nacka kommun samt tagit fram åtgärdsförslag.

Intervjuer och annan informationsinhämtning har gjorts med verksamheten, andra kommuner och leverantörer.

Tillitsnivåer för e-legitimation enligt DIGG.

Tillitsnivå 1
Epost adress + lösenord

Tillitsnivå 2
Krav på tvåfaktorsautentisering, exv via engångslösenord från mobil. Viss tillit till identiteten

Tillitsnivå 3
Krav på tvåfaktorsautentisering, exv via skyddad app i en mobil. Hög tillit till identiteten, samma krav som vid fullgod svensk legitimationshandling.

Förutsättningar och antaganden

- Ingen ska behöva använda sin privata BankID för identifiering i tjänsten.
  -DIGG: "*Privata e-legitimationer i tjänsten bör endast användas när det inte är möjligt att använda e-tjänstelegitimationer" och kräver då överenskommelse mellan medarbetaren och arbetsgivaren*
  -Motstånd i verksamheten vid användning av privat BankID
- Behovet av SITHS kvarstår
- E-legitimationen ska vara godkänd av DIGG
- Digitala nationella prov (DNP) kräver Tillitsnivå 2 för lärare och Säker digital kommunikation (SDK) kräver Tillitsnivå 3.

- Skolans (VS) system för kränkningsanmälningar innehåller känslig information som kräver stark autentisering, även lärarnas lägre behörighet ”att bara se egna ärenden” är på gränsen till Tillitsnivå 3.
- PersonecP (personalsystem) innehåller känslig information om bl.a. hälsa som kräver stark autentisering enligt GDPR. Vi anser det motsvarar Tillitsnivå 3 i tillitskrav. Se bilaga ” Tillitsnivå för inloggning till HR-system”
- Vi bedömer behovet av tillitsnivå som oklar gällande Office365, filytor i vår IT-miljö etc men det borde vara Multifaktorautentisering.

Tillitskrav och volymer

Nacka kommun har ca 5400 anställda

- 400 har SITHS-kort - I stora drag uppfylls behoven av e-tjänstelegitimation i dessa grupper (Tillitsnivå 3). Dock har 100 av SITHS-användarna behov av mobil som bärare (bara kort idag)
- 2000 anställda och politiker skulle behöva e-tjänsteleg. enligt verksamheten (Tillitsnivå 3)
  -1200 lärare (Tillitsnivå 2, på gränsen till Tillitsnivå 3)
  -200 skolledare och specialpedagoger (Tillitsnivå 3)
  -300 Signportanvändare i stadshuset (Tillitsnivå 3)
  -210 politiker, för att komma åt digitala handlingar i Ciceron (Tillitsnivå 3)
- 3000 ”Övriga anställda”- skulle sannolikt behöva e-tjänsteleg. enligt projektgruppen. Eftersom samtliga ska ha tillgång till Personec P krävs Tillitsnivå 3.

Behov och krav

-100 SITHS-användare behöver mobil som bärare (bara kort idag)
-2000 e-legitimationer Tillitsnivå 3 enligt verksamheten
-3000 e-legitimationer Tillitsnivå 3 enligt projektgruppen (sannolikt)
-Stöd för flera olika bärare. Mobil, kort, USB/Yubikey, lärare har chromebooks och PC.
-Enkel administration och ev 24/7-support
-För e-signaturanvändare är det viktigt att inte personnummer används som identifierare/attribut i e-tjänstelegitimationen.
-Ska kunna användas för Windows-inloggning
-Bör kunna användas för stark autentisering mot Microsoft 365 (men kräver separat utredning)

-E-tjänstelegitimationen ska kunna användas som en autentiseringsmetod i Nackas IDP för att komplettera tex SITHs-kort

Kostnader och lösningar/rekommendationer

Ingen leverantör är godkänd av DIGG för Tillitsnivå 2 - därför gäller priser mm Tillitsnivå 3 enbart

2000 st och 5 år: 216-234 kr styck/år, totalt ca 2,3 milj kr
5000 st och 5 år: 190 kr styck/år, totalt ca 4,7 milj kr (Pointsharp)

Lägre kostnad om bara mobil bärare krävs ca 150 kr/år och 5 år

- Upphandling av e-legitimation med krav enligt föregående rubrik. 2000 användare Tillitsnivå 3 eller 5000 beroende på hur man ser på gruppen ”övriga användare”

- Nackas IdP behöver uppgraderas med ny version som kommer kv 3 2023 och en del inställningar behövs för att på ett DIGG-godkänt sätt hantera signering där IdP:n används vid autentisering. Det bör läggas ett uppdrag till lämplig konsult (konsulter) att föreslå lämpliga åtgärder och utföra dessa

Allmänt om behov

Som bakgrund till behovsredovisningen nedan har det tillsammans med verksamheten tagits fram en Excelmatris som visar vad olika yrkesgrupper har för behov av e-tjänstelegitimation och hur det är löst i dagsläget. Se bilaga MFA grupper.xlsx

Vi kan konstatera att vi inte inom överblickbar tid kommer att kunna byta ut våra drygt 400 st SITHS-kort helt. En del system som kräver SITHS-kort kan, som vi ser nu, byta ut SITHS-korten mot annan likvärdig lösning. Men många systemleverantörer har inga planer på stöd för ytterligare multifaktorsinloggningar. Listan med system som använder SITHS-kort idag finns i “bilaga Använder SITHS”. SITHS-korten används också för IT-miljön samt dörrar inom VSS. SITHS-korten används främst inom Hälso- och sjukvård.

Vi kommer alltså inte att helt kunna standardisera på EN lösning om inte SITHS väljs (och kanske inte då heller). Vi ser inte detta som avgörande, det viktiga är att vi har en huvudinriktning gällande e-tjänstelegitimation som de flesta använder. Dock bör lösningen medföra att man i så stor utsträckning som möjligt undviker att den enskilda användaren behöver dubbla autentiseringslösningar på olika

bärare. Kan troligen lösas med kommunens IdP (Identity Provider), där både SITHS och kommunens e-tjänstelegitimation kan användas vid inloggning etc. Detta kräver dock en del extra insatser i form av uppgraderingar och inställningar för att nå en av DIGG godkänd nivå. Bl.a kommer en nödvändig uppgradering först juli-aug -23 som behövs för DIGG-godkänd signering där IdP:n används vid autentisering.

Två nya tillämpningar i form av nationella initiativ kommer användas inom kommunen som ställer krav på en lösning för multifaktorsautentisering godkänd av DIGG (Myndigheten för digital förvaltning). Det är Digitala nationella prov (DNP) med tillitsnivå Tillitsnivå 2 och säker digital kommunikation (SDK) med tillitsnivå Tillitsnivå 3. Även Elektroniska underskrifter och andra DIGG-godkända lösningar kräver DIGG-godkänd autentisering på tillitsnivå 3 (Tillitsnivå 3). Därmed blir en e-tjänstelegitimation godkänd av DIGG på miniminivån Tillitsnivå 3 ett krav. Möjligen att lärarna skulle kunna ha Tillitsnivå 2, mer om det under avsnitt om ”huvudsakliga krav”.

Privat BankID används i ganska stor omfattning bland annat för att SITHS anses för dyrt för att all personal ska kunna ha det. Ett kort kostar ca 450 kr i engångskostnad och.ca 126 kr/år. En annan anledning till att BankID används är att man har behov av att använda vissa av ”SITHS-systemen” i mobilen. Där finns ännu ingen SITHS-lösning därför blir man tvungen att använda BankID. Dock uppfattar man ett motstånd från användarna att använda privat BankID i tjänsten och det rekommenderas inte av bland annat DIGG. Vi gör därför bedömningen att det ska undvikas och anpassar ambitionsnivån därefter.
För de system som använder SITHS och körs på mobilen kommer en mobil SITHS eID efter årsskiftet -23/-24.

I vår, och de flesta andras, lösningar för DIGG-godkända e-underskrifter visas metadatat kopplat till autentiseringen i Adobe Reader. Eftersom BankID används visas personnumret vilket är problematiskt ur GDPR-synvinkel.
Ett krav är alltså att e-tjänstelegitimationen inte innehåller personnummer.

Inom många områden är det en stor fördel, eller ett krav, att ha fysisk tjänstelegitimation med foto. I SITHS-fallet kombineras e-tjänstelegitimation med fysisk legitimation på kortet. Dock medför SITHS-kortet som bärare av e-tjänstelegitimation att datorn och mobiler måste ha utrustning för att kunna läsa kortet därför kan mobilen föredras som bärare i många fall. Andra kortlösningar finns som använder NFC vilket kräver att mobil och dator har NFC men det behövs igen extra utrustning. E-tjänstelegitimationen tappas sällan bort när den är på kort och mobil.

Korten används i vissa fall som dörr/låsöppnare och i IT-miljön. Det är en fördel om e-tjänstelegitimationens bärare kan vara både mobil och kort för att framtidssäkra och därmed undvika att användaren måste ha dubbel utrustning. För inpassering bör möjligheten att stödja modern kryptering utvärderas, exempelvis Mifare Desfire.

För utförandesidan som hanterar stora volymer användare blir kostnaden väldigt hög med befintliga affärsmodeller för e-legitimation, varför lågt pris för e-tjänstelegitimationen blir viktigt.

Välfärd samhällsservice (VSS) och skolan (Välfärd skola, VS) har inom vissa delar av verksamheten gemensam utrustning, bl.a. gemensamma mobiltelefoner t.ex. larmtelefoner på äldreboenden. E-tjänstelegitimationen ska fungera på delad utrustning.

Skolan (VS) har potentiellt många användare, kanske tusentals. Idag har alla tillgång till system för kränkningsanmälningar med huvudsakligen två behörighetsnivåer, en nivå för tex lärare som bara anmäler och ser sina egna anmälningar och en för de som hanterar alla anmälningar tex skolledare. BankID och Nacka eID används, även på privata mobiler. Skolledarna behöver Tillitsnivå 3 men frågan är om lärarna kan ha Tillitsnivå 2. Dessutom kommer det att ingå digitala moment i läroplanen för förskola, särskola och grundskola vilket kan/kommer att kräva att pedagogisk personal utöver lärare kan logga in på delade enheter så som plattor och mobiltelefoner. I framtiden kommer även Digitala Nationella Prov (DNP) enligt ovan.

Gällnde e-ElevID är kraven för otydliga ännu. Vi väljer att exkludera det i denna förstudie och följer utvecklingen.

Det en stor fördel om e-tjänstelegitimationslösningen också kan användas för inloggning till Microsoft-miljön (Windows, office365). För att skydda vår IT-miljö och våra digitala identiteter samt vår information i office365 och filytor. Vi ser dock inte att det idag med någon av de e-tjänstelegitimationer som denna utredning berör kan användas för inloggning i Office365 på ett tillämpbart vis för Nacka kommuns organisation. Detta har inte med e-legitimationerna att göra utan med begränsningar i stöd för annat än Microsofts MFA i deras Onlinetjänster. För att förstå detta ytterligare föreslås en separat utredning med fokus på O365.

Administration och förvaltning av e-tjänstelegitimationslösningen måste vara så enkel som möjligt då många berörs och det snabbt blir ett omfattande arbete annars som drabbar många.

Sammanfattning, behov som saknar befintlig lösning

Volymer

I Nacka kommun finns drygt 5400 anställda. Vi har 400 SITHS-kort i organisationen. I stora drag uppfylls behoven av multifaktorsautetisering (MFA) för SITHS-användargruppernas behov. Dock har ett 100-tal av dessa behov av mobil bärare som framtida SITHS eID sannolikt löser.

Förutom de behov av MFA som har lösts med SITHS-kort så finns ytterligare behov enligt följande:

Totalt ca 1900 anställda och politiker skulle behöva e-tjänstelegitimation för att de använder/eller inom snar framtid kommer att använda system som kräver det, se Excelmatris ”MFA grupper”. Detta är resultat av intervjuer med verksamheten.

- 1200 lärare
- 200 skolledare, adm chefer i skolan och specialpedagoger
- 295 signportanvändare (e-signatur) i Stadshuset
- 210 politiker, för att komma åt digitala handlingar i Ciceron
- 100 SITHS-kortanvändare som behöver lösning på mobil (kommande SITHS eID kanske)

Förutom de 400 SITHS-användarna och de 1900 som har relativt tydliga behov av MFA som nämns ovan finns knappt 3000 ”övriga anställda” där behoven är oklara. Man kan konstatera att alla dessa behöver kunna använda t.ex. Personec (personalsystem) och sannolikt åtminstone någon gång kommer att använda ”säkra meddelanden” (Tillitsnivå 3-krav) och office365-miljön. Det är inte helt klarlagt vilken nivå av skydd Personec P och office365-miljön behöver. Dock finns det mycket som talar för att personal-systemet innehåller känslig information enligt GDPR, t.ex. hälsodata av olika slag, och därmed ställer lagstiftningen krav på en stark autentisering. Då är det logiskt att kräva en hög tillitsnivå, Tillitsnivå 2-3. Se bilaga ” Tillitsnivå för inloggning till HR-system”

Huvudsakliga krav

- Ca 700 st med tydliga krav på Tillitsnivå 3. Men för 1200 lärare är det gränsfall att det räcker med Tillitsnivå 2, dock finns ingen DIGG-godkänd Tillitsnivå 2-lösning. För Digitala Nationella Prov (DNP) räcker det med Tillitsnivå 2 men kränkningsanmälningarna är gränsfall. Även om lärarna bara ser sina anmälningar är det känslig information. Lutar åt Tillitsnivå 3 för lärarna. I sådana fall har vi 1900 anställda med Tillitsnivå

3-krav. De knappt 3000 ”övriga anställda” som bl.a. ska komma åt Personalsystemet, för bl.a. anmälan av frånvaro för semester och sjukdom, ska ha Tillitsnivå 3 om vi ska vara på säkra sidan. Då är vi uppe i ca 5000 Tillitsnivå 3=alla anställda som använder dator eller mobil.

- Stöd för flera olika bärare viktigt. Lärare har oftast inte egen tjänstemobil men en del har det och då fungerar mobil som bärare, annars finns chromebooks och PC som tänkbara bärare och kort och kanske usb/yubikey.
- Enkel administration av e-tjänsteleg. är viktigt då många berörs.
- Det finns en större grupp som är e-signaturanvändare där det är viktigt (på grund av lagkrav) att inte personnummer används som identifierare/attribut i e-tjänstelegitimationen och mobil bärare är viktigt.
- Det skulle förenkla användningen för samtliga, även de 400 SITHS-kortanvändarna, om vår IdP, på ett DIGG-godkänt sätt, kunde hantera inloggningar och autentisering vid underskrifter så att användarna i så liten utsträckning som möjligt slipper ha flera olika e-tjänsteleg. för olika tillämpningar.
- Behov av en teknisk lösning för multifaktorsautentisering (MFA) i syfte att ge ett stärkt skydd för våra elektroniska (Nacka) identiteter.
  En MFA-lösning ger stärkt skydd för information i verksamhetssystem som använder Single-sign-on och filytor i vår lokala IT-miljö, samt information i vår Office 365-miljö, så som Teams, Sharepoint, Outlook.
  Oklar kravnivå gällande tillit.

Tänkbara lösningar samt kostnader och rekommendationer till hur vi går vidare

- Lärarnas behov är viktiga, eftersom en stor del av e-legitimationerna kommer vara till lärare. Behoven varierar, en del har chromebooks, andra har PC, ganska få har tjänstemobil. Kort är troligen bästa bäraren för e-tjänsteleg. men en flexibilitet vad gäller bärare för lärare behövs.
  Tillitsnivå 2 finns ännu inte DIGG-godkänt från någon leverantör och är inte aktuellt att använda så länge ingen är godkänd. Därför vet vi inte om det är billigare än Tillitsnivå 3, troligen ingen jätteskillnad. För Tillitsnivå 3 är kostnaden för de leverantörer som har kortbaserade bärare ca 216-234 kr/pers och år för 2000 personer (hela behovet utom för ”övriga anställda”) och 5 år. Totalt 2,16 – 2,34 milj kr för 5 år och 2000 pers. För 5000 personer blir det ca 190kr/pers och år. Om kravet är bara mobil som bärare kan kostnaden bli lägre 150 kr/pers för 2000 pers och 5 år.
- Flera av de lösningar för e-tjänstelegitimation som är aktuella fungerar också för Windowsinloggning enligt leverantörerna, vilket är att föredra.

Microsoft har en egen lösning för MFA för office365 men den föredragna lösningen har mobil som bärare vilket kan bli svårt för vissa användargrupper och den har ingen fastställd tillitnivå enligt DIGG. Även andra bärare kan vara möjliga. Detta behöver utredas, om lösningen i övrigt är önskvärd. Lösningen ser ut att ingå i de licenser vi redan har. Vi behöver också undersöka om det finns andra lösningar för windowsinloggning och office365.

- Vi rekommenderar en upphandling med kraven som framkommit i behovsanalysen. Frågan är hur man ska se på ”övriga anställda” som är många (3000 st). Närmast till hands är att det är lika bra att kräva Tillitsnivå 3 för att de förr eller senare kommer behöva det, om så inte redan är fallet, eller så får det vara en option. Förutom lärarnas behov av flexibilitet när det gäller bärare är det viktigt att det finns stöd för mobil bärare och att inte personnummer används som identifierare/attribut i e-tjänstelegitimationen.

- Nacka kommuns IdP är viktig i sammanhanget för att
    - Underlätta för användarna så att både SITHS och nya e-tjänstelegitimationen kan användas till flera av våra system, i bästa fall med single sign on, utan att en person behöver ha flera olika lösningar för MFA. Extra värdefullt vore det vid t.ex. e-signering med Signport, då de som har SITHS-kort skulle kunna använda dem vid signering och för att kunna använda både SITHS och nya e-tjänstelegitimationen (för dom som ändå har det) till inloggning i Windowsmiljön.
    - Undvika att personnummer från autentiseringen vid intern användning hamnar i e-signerade dokument genom att IdP:n skickar något annat än personnummer t.ex email adress eller genom att göra det möjligt att använda autentisering utan personnummer, t.ex. SITHS.

  IdP:n behöver uppgraderas med ny version som kommer kv 3 2023 och en del inställningar behövs för att på ett DIGG-godkänt sätt hantera signering där IdP:n används vid autentisering. Det bör läggas ett uppdrag till lämplig konsult (konsulter) att föreslå lämpliga åtgärder och utföra dessa.