Internetguide #44

Digitala identiteter

Så fungerar federationer

internetguider.se

Anders Thoresson

I den här guiden lär du dig...

- ☑ Olika former av id-kontroll på nätet
- ☑ Hur tillitsnivåer fungerar
- ☑ Hur federationer kan användas för att underlätta id-kontroller
- ☑ Exempel på federationer som finns i Sverige idag
- ☑ Skillnaden mellan autentisering och attribut
- ☑ Hur lösenord kan bli säkrare
- ☑ Om pågående EU-projekt

Innehåll

Förord

Jag heter Anders Thoresson och är född den 9 mars 1975. Tack vare mitt körkort är det uppgifter som jag lätt kan bekräfta när någon vill veta vem jag är eller hur gammal jag är.

Men körkortet fungerar bara i fysiska möten. Samtidigt lever vi allt större delar av våra liv på nätet. Och i takt med att allt mer av det vi vill och behöver göra utförs på nätet, uppstår också ett behov av ett nät-id som är lika enkelt att använda som körkortet. Vanliga användarnamn och enkla lösenord räcker inte långt.

Vi har därför vant oss vid att använda e-legitimationer som BankID så fort känsligare uppgifter ska hanteras online. Med mobilvarianten av BankID har den tekniken blivit än mer användbar.

Men även om BankID är en lösning som fungerar bra är det inte en lösning som passar för allt. Ett BankID kan användas för att identifiera någon, men inte nödvändigtvis för att avgöra vad personen i fråga kan göra när hen loggat in. Dessutom är BankID baserat på personnummer, vilket kan innebära ett integritetsproblem.

En lösning på detta är något som kallas för identitetsfederationer. Federationer är samarbeten mellan många olika parter, både sådana som tillhandahåller tjänster på nätet och sådana som är specialiserade på att sköta databaser med användare och deras inloggningsuppgifter. När identitetsfederationer används för rätt tillämpningar är resultatet en nätvardag som är enklare för företag, organisationer och inte minst de enskilda användarna.

Två exempel på federationer som vi återkommer till i texten är Skolfederation, för det svenska skolväsendet, och Sambi, för svensk sjukvård.

Anders Thoresson
Vänersborg, september 2016

Inledning

Du står i kön på Posten för att hämta ut ett rekommenderat brev. I handen har du avin. Men det räcker inte. Personalen måste veta att du verkligen är den person som står som mottagare. När det blir din tur lämnar du därför fram ditt körkort tillsammans med avin.

Samma körkort använder du sedan också på banken och Systembolaget. Vem som än vill veta vem du är eller din ålder kan titta på ditt körkort och få ett pålitligt svar på sin fråga. Ska du resa utomlands tar du med ditt pass, det gäller vilket land du än ska besöka. Ofta innehåller en identitetskontroll två olika delar. Den första handlar om att säkerställa vem någon är. Den andra om att avgöra vilka rättigheter personen i fråga har. En person över 20 år får handla på Systembolaget, till exempel.

Men det som kallas för identifiering – eller autentisering – och behörighetskontroll – auktorisation – är egentligen två olika delar. Ibland är identiteten det viktiga, ibland behörigheten. Och ibland en kombination, eftersom behörighet många gånger är knuten till identitet. Men långt ifrån alltid. På Systembolaget bryr de sig till exempel inte om vem du är, bara din ålder.

I den fysiska världen ställer frågor om identitet sällan till några större problem. Det finns ett antal godkända sätt att bevisa vem man är, sin ålder eller sin nationalitet. Och de fungerar lika bra i Sverige som utomlands. De kan användas för att identifiera någon, men också för att i vissa sammanhang, då ålder eller nationalitet är avgörande faktorer, fatta beslut om behörighet. Ett exempel är id-kort utfärdade av företag, som dels identifierar de anställda men också innehåller information om vilka delar av lokalerna som personen får besöka.

På nätet är det annorlunda. I den digitala världen saknas en universell legitimation.

Antalet inloggningsuppgifter som var och en av oss har att hantera växer ständigt, även om vissa konton har fått en mer central roll än andra. Genom att vara Facebook-, Twitter- , Microsoft- eller Googleanvändare går det idag ofta att börja utnyttja en ny tjänst utan att först skapa ett nytt konto. I stället återanvänder vi de konton vi har hos de fyra tjänsterna.

Men oavsett var kontot finns skyddas det nästan alltid av ett lösenord som du skapat själv. Ibland har du fått användaruppgifter skickade till dig från företaget som driver tjänsten och fått hämta ut dem på Posten först efter att du legitimerat dig. Och på några ställen kan du använda en e-legitimation som är kopplad till dig som individ på samma sätt som ditt körkort.

Förklaringen till att det inte finns något universellt internet-id hittar man i nätets barndom. När de första webbplatserna byggdes var innehållet statisk information. Först inte mer än text som besökarna läste, senare också bilder att titta på. Jämfört med en bok eller en tidning var den enda skillnaden att papperet var utbytt mot en skärm. Förutsättningarna för den interaktion som vi idag tar för given på nätet, där användarna är med och skapar innehåll eller kommunicerar med varandra, saknades och därmed fanns inte heller något behov av att veta vilka personer som besökte en webbsida.

I en skämtteckning från 1993 slår Peter Steiner kort och gott fast att ”på internet är det ingen som vet att du är en hund”.[1] Samma teckning skulle kunna publiceras idag.

Trots att nätet, med Facebook och andra sociala nätverk, har blivit en plats där vi dagligen kommunicerar med släkt och vänner, kan vem som helst ta sig rollen som vem som helst.

Möjligheten att vara anonym på nätet – eller att ta sig rollen som vem som helst – är och har alltid varit stor.

Ur integritetssynpunkt är det viktigt att det är så nätet fungerar. Det är viktigt att de som besöker en webbplats tillåts vara anonyma och att mycket av det de gör online inte går att koppla till dem som individer.[2] Men det finns också många tillfällen när kopplingen till individen är viktig och måste gå att göra på ett pålitligt sätt. Behovet av identifiering växer dessutom i takt med att vi vill utföra allt fler ärenden och aktiviteter på nätet där den kopplingen verkligen behövs, antingen till oss som individer eller till de roller vi har i yrkeslivet eller privat.

Det kan vara privatpersoner som vill vara säkra på att de kommunicerar med rätt person. Det kan vara en medborgare som lämnar uppgifter till en myndighet. Det kan vara ett företag som bara vill släppa in betalande kunder till sin nättjänst. Det kan vara en bank som vill vara säker på att det är rätt person som vill sälja eller köpa aktier, samtidigt som kunden vill vara säker på att det är bankens webbplats som visas i webbläsaren och inte en phishing-sajt. Ett förlag som ger ut läromedel som vill vara säkra på att användaren verkligen är elev på en skola som är kund. Eller så handlar det om ett administrativt verktyg i sjukvården där behörigheten som läkare måste säkerställas. Allt oftare finns det skäl att verifiera parterna som deltar i kommunikationen på nätet. Skolfederation och Sambi är två lösningar, två så kallade federationer som tar sig an inloggningar inom svenskt skolväsende respektive sjukvård.

För att den här behörighetskontrollen ska fungera krävs två saker. För det första måste man vara säker på att användaruppgifterna har delats ut till rätt person. Redan här brister de flesta webbtjänster på nätet, där användarna själva skapar sina konton. För det andra måste man använda teknik som gör det sannolikt att det är rätt

person som försöker logga in. Också här brister kombinationen användarnamn och lösenord, eftersom det är uppgifter som lätt kan hamna på avvägar.

Den viktiga tredje parten

I den fysiska världen är frågan Vem är du? ofta trivial och väldigt enkel att svara på. Men vad svaret blir är helt beroende på sammanhang.

På ett bröllop räcker ”brudens kusin” och möjligen en bekräftande nick från en gemensam bekant. Den som frågat har ingen anledning att misstro påståendet. På en konferens är svaret ”säljare på Göteborgskontoret” med ett överlämnat visitkort bra nog.

På banken, däremot, duger inget mindre än ett körkort eller en annan giltig identitetshandling med motsvarande status. Utan det kan du inte ta ut några pengar.

Det här är tre exempel som går att sammanfatta på ett generellt sätt: Den tillfrågade svarar med ett påstående om vem han eller hon är och lämnar samtidigt någon form av bekräftelse på att det stämmer. Ju viktigare sammanhang, desto större krav ställs på att bekräftelsen går att verifiera som korrekt och riktig. Och nästan varje gång sker det genom att en betrodd tredje part står som garant för att påståendet stämmer, som i exemplen med visitkort och körkort.

På nätet har de webbplatser som behöver identifiera sina användare tvingats bygga upp sina egna databaser med namn och lösenord, eftersom en teknisk lösning som låter en pålitlig tredje part vara en del i kommunikationen har saknats. Det är förklaringen till att nätets användare idag brottas med långa listor med lösenord. Lösenord som dessutom är en kompromiss mellan att vara användarvänliga (möjliga att komma ihåg, alltså) och tillräckligt säkra (svåra att gissa eller knäcka).

Försöken att hitta lösningar på det här problemet har pågått länge. Redan på tidigt 2000-tal talades det om teknik som skulle ge användarna ett enda lösenord till allt de sysslar med på nätet. Men då handlade det bara om den enkla biten, att underlätta för användarna. Kopplingen till den fysiska världen saknades i de visionerna. Och trots det – utvecklingen går inte alltid med det rasande tempo som ofta påstås vara typisk för nätet.

Under det senaste decenniet har listan med inloggningsuppgifter som en vanlig nätanvändare måste hålla koll på knappast krympt och något enda lösenord som fungerar på alla webbplatser finns inte i sikte.

En delad identitet

Det är inte heller säkert att en sådan lösning längre är önskvärd.

För precis som i den fysiska världen finns det behov av att kunna identifiera sig på olika sätt i olika situationer.
Stora delar av ditt liv finns idag på nätet. Du kommunicerar med dina vänner, du handlar, du deklarerar. Att separera de aktiviteterna i ett par olika elektroniska identiteter känns bättre än att samla dem i en enda, inte minst ur ett integritetsperspektiv. Åt det hållet tar nu utvecklingen stora kliv.

På konsumentsidan, för de tjänster där behovet av att kunna knyta användare till en fysisk person inte finns, är Facebook Connect som lanserades redan 2008 ett exempel. Tekniken har utvecklats sedan dess, men grundfunktionen är densamma: En användares identitet på Facebook fungerar på många andra tjänster över hela nätet. Ibland handlar det bara om att underlätta inloggningen, i andra fall om att även ”flytta med” användarnas sociala nätverk till nya tjänster.

Men Facebook, Google, Microsoft, Twitter och andra som har inloggningslösningar som andra tjänsteutvecklare kan dra nytta av löser bara det första problemet, att göra livet enklare för användarna. Det är lösningar som är perfekta för spel, fotosajter och diskussionsforum. Webbplatser där det inte spelar särskilt stor roll om du verkligen är den du utger dig för att vara.

Att det saknas en reell koppling mellan användarkontot på nätet och en person i den fysiska världen är ett problem i andra sammanhang. Det handlar bland annat om kontakter med myndigheter och affärsuppgörelser av olika slag. Trots att fyra miljoner svenskar har ett konto på Facebook ska vi inte förvänta oss att Skatteverket kommer att börja använda Facebook som inloggningsalternativ för dem som vill lämna in sin deklaration elektroniskt. Däremot har flera av de stora sociala nätverken infört en markering för det som kallas ”verifierade användare”. En vit bock på blå bakgrund visar att Facebook eller Twitter kontrollerat vem som står bakom ett visst konto.

I Sverige har lösningen på det andra problemet, när en digital identitet ska knytas till en fysisk person, varit de e-legitimationer som bland annat utfärdas av bankerna. Men de dras med flera brister, bland annat att de inte fungerar med alla tekniska plattformar (delvis adresserat av mobilt BankID) och att de vilar tungt på våra personnummer, vilket är ett potentiellt integritetsproblem. Ska du köpa skor i en nätbutik finns det inget skäl att skicka ditt personnummer till butiken.

Därför har ett initiativ tagits till införandet av en ny nationell e-legitimation och som en del i det arbetet inrättades myndigheten E-legitimationsnämnden 2011. Ambitionen är att på sikt införa ett helt nytt system för e-legitimationer i Sverige, där dagens brister ska åtgärdas. Tanken är att bygga på öppna standarder, och att göra det på ett sätt så att både offentliga verksamheter och privat näringsliv

kan dra nytta av möjligheterna som en pålitlig identifiering möjliggör. Men arbetet har gått långsammare än förväntat. Våren 2016 fattades därför beslut om en omstart, samtidigt som en övergångslösning där de befintliga e-legitimationerna används sjösattes.

Olika behov, olika lösningar

Den absolut största delen av den här Internetguiden handlar om identitetsfederationer. Det är lösningar som hanterar både autentisering och behörighetskontroll. Men federationer är inte lösningen på alla identitetskontroller som behöver göras på nätet. Och det är inte heller en ersättare till lösningar som exempelvis BankID. Den stora flora av tjänster som finns på internet har som konsekvens att det också finns ett utrymme för många olika mekanismer för identitetshantering.

I den ena änden av skalan har vi enkla tjänster där individuella användarkonton exempelvis behövs för att hålla koll på hur långt användarna har kommit i ett nätbaserat spel. I en sådan tillämpning spelar det inte någon roll vilken individ som egentligen står bakom ett användarkonto. Därför räcker det gott med ett vanligt användarnamn och lösenord som sparas i en databas som spelföretaget själv hanterar.

I den andra änden av skalan finns tjänster där det dels är viktigt att säkerställa en faktisk identitet på användarna, men också att hantera vilka delar av tjänsten som olika personer ska få utnyttja. Hit hör exempelvis ett betygssystem för skolan, där en lärare ska kunna sätta betyg medan enskilda elever bara kan se sina egna. Här räcker det alltså inte att kontrollera vem någon är, utan också i vilken roll personen i fråga agerar. Är man lärare ska man kunna sätta betyg för sina egna klasser, inga andra.

I en sådan tillämpning är en federation ett utmärkt alternativ. Skolor runt om i landet har databaser med användaruppgifter, som dessutom innehåller information om deras olika roller. Denna information kan tjänsteleverantörer som vänder sig till skolsektorn utnyttja.

Men också i en tillämpning av det senare slaget behövs mer än bara användarnamn och lösenord, eftersom vi givetvis vill försäkra oss om att en elev inte lyckas gissa sin lärares lösenord och sätter högsta betyg på sig själv.

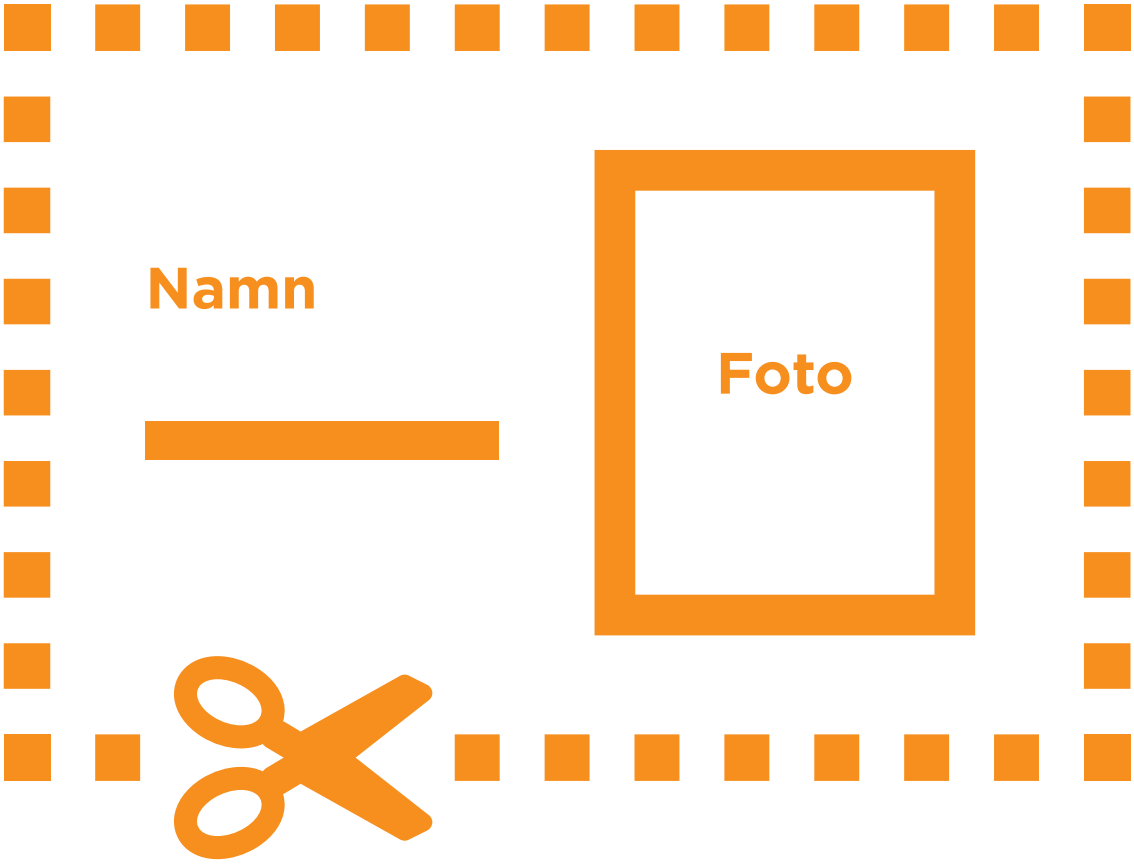
Ett begrepp som vi återkommer till är ”tillitsnivå”. Det är ett sätt att beskriva hur säkra vi är på att en person som utger sig för att vara någon verkligen också är denna individ. Ett användarnamn och lösenord man skapar själv har låg tillitsnivå, ett BankID man får efter en legitimationskontroll på sitt bankkontor har hög tillitsnivå.

Detta innebär att federationer även behöver tekniska lösningar som tillåter identifiering med en tillitsnivå som passar tjänstens behov.

När du läser resten av guiden, kom alltså ihåg att det inte finns ett motsatsförhållande mellan dagens lösningar och de federationer som diskuteras här. Ibland är en federation byggd på hög tillitsnivå det som behövs, ibland räcker det med ett enkelt lösenord som skyddar ett konto som användaren själv skapat, utan någon id-kontroll över huvud taget.

Olika behov, olika lösningar.

1. Hemmagjorda id-kort och trovärdighet



Vill du ha en legitimation kan du sätta dig vid köksbordet med en bit kartong, ett foto på dig själv, lite pennor och en limtub. En stund senare har du slöjdat ihop ett id-kort. Problemet är självklart att ingen kommer ta id-kortet på allvar. Att du själv påstår att du är den du är i många fall inte värt ett skvatt, och absolut inte de gånger någon ber dig bekräfta din identitet med en legitimation.

Man brukar tala om tillitsnivåer[3] som ett sätt att avgöra hur pålitligt ett påstående om identitet är. Ett hemmagjort id-kort har en låg tillitsnivå, ett körkort en hög. Skillnaden är att Transportstyrelsen som utfärdar körkorten i Sverige är en betrodd part, att det sker någon form av identitetskontroll när körkortet lämnas ut och att det är förhållandevis svårt att förfalska körkortet. Den som vill bekräfta en persons identitet kan därmed med hög sannolikhet avgöra vem denne är genom att titta på körkortet.

Samma grundprinciper med olika tillitsnivåer gäller på nätet. Ett konto på Facebook har låg tillitsnivå. Vem som helst kan skapa ett konto i vilket namn som helst. Med tiden kan möjligen vännerna avgöra att det faktiskt är Kajsa Karlsson som utger sig för att vara Kajsa Karlsson, tack vare att personen bakom kontot lägger upp bilder från fester Kajsa varit med på och skriver statusuppdateringar om sådant de vet att Kajsa gör. Men en faktisk koppling mellan konto och individ saknas.[4]

Jämför detta med hur en e-legitimation fungerar. Ett sätt att skaffa en e-legitimation idag är att vända sig till en bank som utfärdar så kallade BankID. Ett BankID är en fil, ett digitalt certifikat, som laddas ner till användarens dator eller en app till användarens mobiltelefon. Med ett BankID är det sedan möjligt att intyga sin identitet när man loggar in på tjänster som använder tekniken.

Men för att kunna ladda ner ett BankID räcker det inte att logga in på sin nätbank med den vanliga pinkoden. Tillitsnivån i en fyra siffror lång kombination är för låg. En kod kan lätt komma på avvägar, och därför kan banken inte vara säker på att det verkligen är Kajsa Karlsson som vill ladda ner ett nytt BankID. Det kan lika gärna vara Sven Svensson som på något sätt kommit över Kajsas kod.

För att kunna skaffa ett nytt BankID krävs i stället för pinkod att Kajsa använder en annan teknisk lösning för att logga in i nätbanken. Det kan till exempel vara en elektronisk dosa som skapar nya koder varje gång, en dosa som banken tidigare lämnat ut till Kajsa under kontrollerade former, där hon fått legitimera sig och intyga att hon verkligen är hon. På så vis vet banken, med tillräcklig sannolikhet, att det är rätt person som försöker skaffa ett BankID i Kajsas namn.

På det här sättet byggs förtroendekedjor upp i flera led på nätet. Tjänsten där Kajsa vill logga in litar på hennes påstående om vem hon är, eftersom hon använder ett BankID. Sitt BankID har Kajsa fått från banken, eftersom hon kunde legitimera sig med säkerhetsdosan.

Och säkerhetsdosan fick hon ut genom att visa upp sitt körkort, vilket Transportstyrelsen går i god för.

Men även om dagens svenska e-legitimationer innebär att en pålitlig tredje part finns med i identitetsprocessen dras de med andra svagheter.

En är sättet som de distribueras på. Eftersom ett BankID är något som laddas ner till en dator eller telefon är det en lösning som bara passar dem med en egen dator i hemmet eller en smartphone. Att lägga ett BankID på en dator på biblioteket eller jobbet är mindre lämpligt, eftersom man då lämnar sin legitimation tillgänglig för andra. Fortfarande krävs ett lösenord för att kunna utnyttja den, men lösenord är inte säkra.

En annan svaghet är att dagens e-legitimation är helt baserad på våra personnummer. Varje gång ett BankID används får tjänsten som utnyttjar tekniken reda på användarens personnummer, vilket är ett potentiellt integritetsproblem.

Vet, har eller är

Varför duger ett visitkort på konferensen, medan det behövs ett körkort hos banken? Förklaringen är inte bara vem det är som står som garant för användarens identitet eller hur svår id-handlingen är att förfalska. Det finns företag och organisationer som ger ut id-kort med samma trovärdighet som ett körkort har. En annan väldigt viktig skillnad är körkortsinnehavarens fotografi och namnteckning.

När du vill styrka påståendet om vem du är kan du göra det på tre olika sätt:

Med något du vet eller kan

En pinkod eller ett lösenord är två typexempel. Det kan också vara din namnteckning. Problemet är att detta är saker som kan stjälas eller förfalskas utan användarens vetskap. Det är också förklaringen till att lösenord har en låg tillitsnivå. Det går inte att veta att det är rätt person som loggar in, bara att det är någon som kan lösenordet. Under senare år har ett par fall av lösenordsstölder uppmärksammats i svenska medier, när svenska webbtjänster har hackats och stora mängder användaruppgifter kommit på avvägar. Detta blir extra problematiskt eftersom många gör det enkelt för sig och använder samma lösenord på flera ställen. Ett förlorat lösenord från en tjänst innebär då att vägen också ligger öppen in till andra tjänster.

Med något du har

BankID är ett exempel, som dessutom kombineras med föregående punkt eftersom du knappar in ditt lösenord varje gång du använder ditt BankID. Andra exempel på saker du har kan vara en dosa för

engångslösenord eller ett smart kort som stoppas in i en kortläsare som är kopplad till datorn.

Med något du är
I den fysiska världen handlar det om den snabba jämförelsen mellan personen som står framför kassan och fotografiet på körkortet. I den digitala världen är kontroll av fingeravtryck ett exempel.

Ett sätt att höja tillitsnivån är kombinationslösningar, där just BankID är ett exempel. Det är en fil du måste ha på din dator, men det krävs också att du kan lösenordet för att ha glädje av det digitala certifikatet.

Det här kallas för tvåfaktorsautentisering. Används bara ett lösenord är det fråga om enfaktorsautentisering, medan mer komplexa kombinationer kallas för flerfaktorsautentisering.

Ett körkort – eller annan accepterad legitimation – är ett exempel på flerfaktorsautentisering. Du har kortet, du är personen på bilden och du kan skriva samma namnteckning.

På nätet är enfaktorsautentisering fortfarande den i särklass vanligaste metoden, i form av ett lösenord som användaren kan. Det är också anledningen till att ett enkelt lösenord inte är tillräckligt för att skydda annat än de enklaste konsumenttjänster. Med kort där engångskoder skrapas fram eller dosor som skapar nya lösenord vid varje användning införs ytterligare delar i autentiseringen, och därmed ökar sannolikheten för att användaren verkligen är den han eller hon utger sig för att vara.

Vad får du göra?

Men att veta att en person verkligen är den han eller hon utger sig för att vara räcker inte alltid. På banken har du inte fri tillgång till alla kunders bankkonton så snart du legitimerat dig vid disken och lastbil får du inte nödvändigtvis köra bara för att du har ett körkort.

Autentiseringen, den process när en användares identitet fastställs, följs därför alltid av en auktorisation som avgör vad användaren får göra. I den fysiska världen innebär det att Systembolagets personal konstaterar att du dessutom är över 20 år gammal och får handla alkoholhaltiga drycker, eller att polisen som gör körkortskontrollen ser att du faktiskt har behörighet att köra en tung lastbil.

På nätet görs motsvarande kontroller för att avgöra vilka delar och funktioner just du ska få tillgång till när du loggar in i en tjänst.

Ett dubbelriktat behov

Vad som ibland glöms bort är att behovet av identitetskontroll inte är enkelriktat. Tjänsten där du vill logga in behöver veta vem du är,

men lika viktigt är att du kan vara säker på att du faktiskt är på den webbplats där du tror att du är.
Det kan låta som ett märkligt krav, men alla phishingattacker på senare år visar varför det är så viktigt. I en phishingattack luras besökaren in på en falsk webbsida, inte sällan med hjälp av länkar i e-post. Den falska webbsidan är byggd för att se ut som exempelvis inloggningssidan hos en nätbank. Och när användaren matar in sina inloggningsuppgifter hamnar de i händerna på helt fel personer.
I Sverige har bland annat bankkunder drabbats av omfattande phishingattacker.

En dellösning på det här problemet står företagen som utvecklar webbläsare för. I senare versioner har alla de stora webbläsarna ett skydd mot phishingattacker. Genom att jämföra adressen i adressfältet med en lång lista med farliga webbplatser kan webbläsaren varna användaren för att hon eller han är på väg till en sida som inte är vad den utger sig för att vara.

På en lägre nivå på internet finns en teknik som heter DNSSEC.[5] Varje webbplats på nätet har en IP-adress, en sifferkombination som talar om för webbläsaren från vilken webbserver sidan kan hämtas. Men eftersom sifferkombinationer är svåra att komma ihåg började man använda DNS, domain name system (domännamnssystemet på svenska). Det är en teknisk lösning som gör det möjligt att skriva in www.iis.se i webbläsaren, som automatiskt och bakom kulisserna får reda på att Internetstiftelsen i Sverige har (när detta skrivs) sin webbplats på en server med IP-adressen 91.226.37.214.
Men DNS-systemet går att angripa för att byta ut IP-adresserna för utvalda domännamn. DNSSEC är en teknik som gör det möjligt för webbläsare att verifiera att IP-adressen som kommer som svar på frågan verkligen stämmer.

Ytterligare nivåer av skydd får man med teknik som SSL (Secure Sockets Layer) och efterföljaren TLS (Transport Layer Security).
I båda fallen handlar det om lösningar som krypterar trafiken på nätet med funktioner för att verifiera vilka parter det är som kommunicerar med varandra.

2. Kraven på en digital legitimation

En pålitlig tredje part som intygar en persons identitet på nätet är bara en av de pusselbitar som måste finnas på plats i ett väl fungerande system för elektroniska identiteter. Att kunna avgöra att en person är den han eller hon utger sig för att vara är givetvis ett viktigt fundament för ett identitetssystem, men det finns fler delar som är viktiga att ta hänsyn till.

Kim Cameron, Chief Architect of Identity på Microsoft, skrev 2005 *The Laws of Identity*,[6] en text med de krav som han tycker att ett identitetssystem bör uppfylla. Fortfarande idag är den sju punkter långa listan väl använd i diskussioner om hur lösningar för elektroniska identiteter bör utformas.

1. Kontroll och samtycke (*User control and consent*)
För att användarna ska våga lita på ett system som hanterar deras identiteter på nätet måste användarna också känna att de har kontroll över hur informationen används. Det handlar exempelvis om att själv kunna ha sista ordet när det gäller vilka tjänster som får fråga efter personuppgifter och vad de tjänsterna då får reda på.

2. Minimera informationen och begränsa användningen (*Minimal disclosure for a constrained use*)
Personinformation är känslig och kan missbrukas. Därför bör ett system för digitala identiteter byggas upp så att bara absolut nödvändig information skickas till en tjänst. Tjänsten ska i sin tur omgående kasta all information den sannolikt inte kommer att ha nytta av i framtiden och då inte enkelt kan få reda på igen. I den fysiska världen har ett körkort den fördelen att utfärdaren inte har en aning om var körkortet används. Inte heller sparar Systembolaget personnumren på alla personer som får legitimera sig innan de handlar. Det är förhållanden som det finns stor anledning att försöka återskapa i den digitala världen, som ett skydd för den personliga integriteten.

3. Befogade deltagare (*Justifiable parties*)
Det måste kännas motiverat att det är en viss instans som intygar en persons identitet. Kim Cameron tror till exempel att få personer vill använda en statlig e-legitimation för att komma åt sin e-post. Särskilt inte i länder där det finns en misstro mot myndigheter. Därför kommer det sannolikt inte något globalt id-system som alla tjänster på nätet utnyttjar. Den troliga utvecklingen är snarare att många id-system kommer att utvecklas, alla med sitt tänkta användningsområde.

4. Riktad identitet (*Directed identity*)
Medan tjänster på nätet behöver kommunicera sin identitet till alla som besöker webbplatsen är det viktigt att användarnas identitet skickas riktat, med tjänsten som enda mottagare.

5. Ett rikt utbud av leverantörer och tekniker (*Pluralism of operators and technologies*)
Av punkt tre följer att det behövs flera olika sätt att legitimera sig, beroende på vilken typ av tjänst det är man ska använda. Man vill kanske inte använda sin företagsidentitet när man gör sina privata ärenden på nätet, inte använda sin statliga på jobbet och så vidare. Därför behövs olika system så att nätanvändarna kan sprida sin identitet i flera korgar, vilket är en fråga om integritet. Av detta följer också att det behövs ett grundläggande ramverk så att dessa olika delar kan fungera ihop, när så är motiverat. En annan viktig teknisk aspekt är att e-legitimationer ska fungera på olika apparater, så att det är möjligt att styrka sin identitet oavsett vilken typ av mobiltelefon, dator eller annan internetuppkopplad apparat man använder.

6. Den mänskliga aspekten (*Human integration*)
Kim Cameron konstaterar krasst: Vi har gjort ett bra jobb med att säkra kopplingen mellan webbserver och webbläsare med hjälp av kryptoteknik, om så avståndet är tusentals mil. Men vi har misslyckats med att säkra de sista decimetrarna mellan skärm och användare på ett bra sätt. Det är ofta den sista biten som är under attack från cyberkriminella. I klartext betyder det här att tekniken för identiteter på nätet måste bli enklare att förstå sig på, mer användarvänlig. Är det tydligt hur en teknisk lösning fungerar blir den enkel att använda och dessutom blir det svårare att lura användarna att göra fel och avslöja sina identitetsuppgifter för obehöriga, som när användare luras att klicka på falska länkar och lämna i från sig sina användaruppgifter i phishingattacker.

7. Enhetliga användargränssnitt (*Consistent experience across context*)
För att förenkla för användarna krävs att användarupplevelsen skiljer sig så lite som möjligt åt mellan olika platser på nätet. Eftersom användarna antagligen kommer att ha flera olika identiteter, som skissats i punkt fem ovan, och dessutom logga in med dem på många olika ställen krävs bland annat att det ska vara lätt att förstå vilken typ av inloggning som passar bäst att använda i en given situation.

Kraven och dagens teknik

Dagens e-legitimationer har på flera sätt varit framgångsrika. Det menade bland andra E-delegationen, som i oktober 2009 överlämnade den statliga utredningen *Strategi för myndigheternas arbete med e-förvaltning* (SOU 2009:86) till regeringen. I den ägnas ett kapitel åt e-legitimationer och E-delegationen inleder med att konstatera att ”nära nog varje vuxen svensk smidigt via nät kunnat

anskaffa det som behövs för legitimering och underskrift i digital miljö. Myndigheterna har också, i samverkan med dem som utfärdar e-legitimationer, infört dialoger och användargränssnitt för e-legitimationer som är enkla att använda och delvis självförklarande."

Inte desto mindre har de lösningar som finns i Sverige idag misslyckats med att leva upp till de sju krav Kim Cameron ställer på elektroniska identiteter. Som användare har du ingen kontroll över vilken information som skickas, tjänsten som legitimerar dig får alltid reda på ditt personnummer. Ett annat problem är att de är tekniskt komplicerade, och att de företag som utfärdar e-legitimationer valt delvis olika lösningar som inte följer en enhetlig standard. För medborgare som saknar en egen dator ställer e-legitimationer i form av filer som laddas ner från nätet till problem, eftersom en sådan lösning inte är lämplig att använda på datorer i bibliotek eller på arbetsplatser. Sammantaget gör dessa problem att dagens e-legitimationer är långt i från optimala.

En nackdel är att användarnas personnummer spelar en central roll i e-legitimationen, vilket är information som inte alltid behövs och som genom att ständigt exponeras riskerar att äventyra den personliga integriteten.

För att få en svensk e-legitimation idag krävs dessutom ett svenskt personnummer och bara i undantagsfall ges exempelvis en e-legitimation ut till minderåriga. Dagens lösning är därmed exkluderande i den mening att alla personer som behöver komma i kontakt med myndigheter och näringsliv i Sverige inte kan använda nätet. Inte heller kan svenska företag få en e-legitimation för sina myndighetskontakter. Men den är också exkluderande i den mening att det krävs viss teknisk utrustning för att kunna använda dem, som en dator med visst operativsystem.

E-delegationens förslag är därför att "målet för en svensk infrastruktur bör vara att befintlig och ny teknik ska användas för att, på det sätt som är mest effektivt, förse myndigheter och användare med de funktioner som behövs och göra dessa rutiner enkla att förstå och förenliga med gällande rätt. Detta mål bör omfatta lösningar för både fysiska och juridiska personer, såväl med svensk som utländsk hemvist."

I juni 2010 fattade regeringen beslut om att tillsätta en särskild utredare som ska förbereda och genomföra bildandet av en ny myndighet som ska få i uppdrag att samordna det offentliga Sveriges behov av e-legitimationer. Arbetet har gått långsammare än tänkt, men pågår fortsatt.

En väg framåt som löser många av de här problemen och uppfyller en hel del av önskemålen är identitetsfederationer, en modell som presenteras i nästa kapitel.

Men att det ska komma en universell och global lösning som uppfyller alla krav och fungerar vad vi än ska göra på nätet, det är inte troligt. Tilltron till systemet är ett skäl, det kommer alltid att finnas användare som av olika anledningar inte vill lägga hela sin digitala identitet på ett och samma ställe. Ett annat problem är synen på vad en identitet egentligen är. Den skiljer sig åt mellan olika länder och sammanhang. Det finns likheter men också stora skillnader mellan en student på ett svenskt universitet, en polis i Kina och en pensionär i New York. Som en konsekvens är det inte tekniken som är det största hindret för stora, nationsöverskridande lösningar för digitala identiteter. I stället är det på juridiksidan som det behövs mycket arbete för att det ska bli möjligt.

3. Federationer – en utspridd nätidentitet

Ska du boka tid för ett läkarbesök åt ditt minderåriga barn behöver vårdcentralens datorer vara säkra på att du är förälder till barnet.

Ska du lämna in deklarationen för bostadsrättsföreningen där du är ordförande behöver Skatteverkets webbtjänst kunna verifiera att du är behörig att göra det.

Är du elev på en skola behöver läromedelsförlaget inte veta vem du är när du vill läsa i den digitala läroboken på nätet, bara att du är går på en skola som är betalande kund.

Ett identitetssystem som bara delar med sig av den information som är nödvändig i en viss situation går att konstruera. Det kallas för en identitetsfederation, ett samarbete mellan flera olika parter som resulterar i en väldigt flexibel lösning som erbjuder gott om möjligheter till smarta finesser och nya funktioner, samtidigt som den personliga integriteten är skyddad.

Först ett exempel som varit i drift i flera år, för att konkretisera tankarna bakom och möjligheterna med en federation: Det är inte ovanligt att anställda och studenter vid svenska högskolor och universitet besöker andra lärosäten än det egna. Ofta behöver de då komma åt ett trådlöst nätverk från sina bärbara datorer. En lösning är att varje universitet och högskola delar ut tillfälliga konton till sina besökare. Det fungerar, men är omständligt och dyrt eftersom någon måste kontrollera besökarens identitet, förklara vilka regler som gäller och skapa kontot. Men någon som studerar på Kungliga Tekniska Högskolan eller forskar på Lunds Universitet borde väl vara betrodd att använda det trådlösa nätverket på Chalmers under ett besök i Göteborg, utan att först besöka receptionen och legitimera sig där?

Lösningen heter Swamid och är ett samarbete mellan högskolor och universitet i Sverige och andra länder som gör just den resursdelningen möjlig. Skolorna har helt enkelt bestämt sig för att lita på varandras studenter och personal.

I praktiken har skolorna som deltar i Swamid kommit överens om två saker: Vad som ligger i begreppet identitet och vilken teknik som ska användas.

Överenskommelserna som bygger en federation

Att ha en entydig definition på vad som är en användare och under vilka förutsättningar ett användarkonto delas ut och stängs av är viktiga grundstenar i en federation. Samma regler måste gälla hos alla de organisationer som deltar i federationen. Inte minst är detta viktigt för att användarna ska veta vilka regler som gäller, vad man får och inte får göra och under vilka förutsättningar ett konto kan stängas av. En annan viktig aspekt är hur användarnas identitet

kontrolleras när kontouppgifterna delas ut. Så länge alla parter först gör en id-kontroll och sen delar ut kontouppgifter fungerar federationen, men det räcker med att en part slarvar med kontrollen för att den genast ska få en svag punkt.

Vad den överenskommelse som lägger grunden för en federation omfattar varierar från federation till federation. Men vissa grundläggande saker återfinns alltid:

Tillit
Ingående parter måste känna att de kan lita på varandra. Därför behövs bland annat bestämmelser för hur nya användare läggs till i federationen.

Attribut
Uppgifter om användarna i en federation behövs ofta för att den ska kunna uppfylla sitt syfte. Med hjälp av så kallade attribut går det exempelvis att ange om en användare är lärare eller elev och utifrån det kan tjänsteleverantörer bestämma vilka delar av tjänsten som användaren ska få tillgång till.

Standarder för teknik
De överenskommelser som görs i ett konferensrum ska konkretiseras i form av tekniska implementationer, och då krävs standarder som definierar hur det ska gå till.

En gemensam infrastruktur
Den faktiska tekniken som knyter ihop federationsoperatören, identitetsleverantörerna och tjänsteleverantörerna med varandra.

Delarna i en federation

En identitetsfederation består av flera delar. Det behövs minst en identitetsleverantör, som sköter databaser med användaruppgifter och låter användarna identifiera sig. Det behövs minst en tjänsteleverantör, som erbjuder tjänster till användarna. Ofta finns det också en federationsoperatör som har ett övergripande ansvar för federationen. Om det finns flera olika identitetsleverantörer finns det också en anvisningstjänst. Anvisningstjänsten håller koll på vilka identitetsleverantörer som är med i federationen och hjälper på olika sätt användarna att hitta ”sin” leverantör.

I en federation är det alltså identitetsleverantören som har ansvaret för att kontrollera en användares identitet. Från identitetsleverantören får tjänsteleverantörerna reda på om användaren har identifierat sig på ett godkänt sätt. Men det kan också följa med information om behörighetsnivåer och annat, så kallade attribut.

Utifrån dessa attribut kan tjänsteleverantören bestämma vilka funktioner som användaren ska få tillgång till. I ett system för skolbetyg kan det till exempel innebära att en elev bara får se sina egna betyg. En lärare kan däremot ändra betyg, men bara för de klasser som de undervisar i.

För tjänsteleverantörerna är det här en stor fördel. I nätets barndom var varje tjänsteleverantör tvungen att också vara sin egen identitetsleverantör och bygga upp en databas över sina egna användare. Det var inte bara databasen med användare som behövde skapas, utan också olika tekniska lösningar för att sköta inloggningen. Det billiga och enkla sättet var givetvis ett vanligt lösenord, medan säkrare alternativ som engångskoder och liknande är både dyrare och mer komplicerade. Att ha ansvaret för användardatabasen kostar också i form av support, när användare hör av sig med bortglömda lösenord eller av andra anledningar inte lyckas logga in. I en federation hamnar den typen av frågor i stället hos identitetsleverantören.

I relationen mellan identitetsleverantör och tjänsteleverantör finns en överenskommelse om hur lyckade inloggningar ska kommuniceras mellan parterna. Däremot finns inget som specificerar vilka tekniska lösningar som användarna ska kunna välja att använda för att legitimera sig. Det innebär att identitetsleverantörerna kan följa den tekniska utvecklingen och lägga till nya inloggningsmetoder i takt med att de dyker upp och får spridning på marknaden. Men uppgiften om hur användaren loggat in finns med i den information som identitetsleverantören skickar till tjänsteleverantören. Det innebär att tjänsten kan anpassas efter säkerhetsnivån i inloggningen. Om användaren bara knappat in ett vanligt lösenord får hen bara tillgång till en begränsad del av tjänsten, medan en tvåfaktorsinloggning krävs för att få tillgång till alla funktioner i tjänsten.

Ytterligare en part kan ingå i en federation, en så kallad registerhållare. Medan identitetsleverantörernas enda uppgift är att verifiera att personer är de som de utger sig för att vara kan registerhållarna ha annan information om personerna lagrad, till exempel om en person är student eller inte.

Nu ska två av fördelarna med en federation förhoppningsvis vara tydliga:

1. Förlaget behöver inte hålla en egen databas med användarinformation uppdaterad. Den delen står i stället de skolor som är anslutna till federationen för. Det besparar förlaget investeringar i teknik och kostnader för drift och underhåll av kunddatabasen, och gör att bolaget inte heller behöver lagra personuppgifter.
2. Förlaget behöver heller aldrig få reda på Kajsas personnummer eller annan information som kan användas för att identifiera

henne. Förlaget får i stället bara reda på att hon är elev på en skola som är betalande kund och en pseudonym som gör det möjligt att personanpassa sajten. Vid missbruk eller problem kan förlaget vända sig till skolan för att få reda på vem personen med en viss pseudonym är.

Allt det här sker automatiskt i bakgrunden, utan att Kajsa märker vad som händer. För henne ser processen ut som vilken vanlig inloggning som helst.

Pengar att spara och integritet att skydda

Pengar är ofta en stark drivkraft för att bygga en identitetsfederation. Att göra id-kontroller är kostsamt. Det uppenbara är investeringar i teknik som i slutänden måste finansieras av användarna. Men det finns också mindre uppenbara kostnader, till exempel för att driva och underhålla databasen med användaruppgifter. En stor fördel med en identitetsfederation är att informationen om den enskilda användaren bara behöver finnas på ett ställe. Det gör att de sammanlagda underhållskostnaderna minskar. Med standardiserad teknik för id-kontroller och ett system där olika aktörer litar på varandra kan kostnaderna pressas.

Men det är inte bara direkta kostnadsbesparingar som ligger bakom önskemålen. Enklare utveckling är ett annat argument. Om tjänsteleverantörerna tar hjälp från en identitetsleverantör för att göra id-kontrollerna behöver inte tjänsteleverantören på egen hand hänga med i teknikutvecklingen. Om identitetsleverantör och tjänsteleverantör bara kommit överens om hur identitetsinformationen ska utbytas dem emellan kan identitetsleverantören använda vilken teknik som helst för att låta användarna identifiera sig.

En annan fördel är att det system som vill veta om användaren är behörig inte nödvändigtvis behöver få reda på vilken individ det är som vill ha tillgång till tjänsten. I skolexemplet tidigare i det här kapitlet fick förlaget aldrig reda på Kajsas faktiska identitet. I stället användes en persistent pseudonym.

Det finns gott om tillfällen när den enskildes identitet egentligen är helt ointressant. Ett tänkbart exempel är ett företag som vill låta sina anställda komma åt information i en databas på nätet, som kostar pengar. Med en federationslösning kan man då tänka sig att det enda tjänsteleverantören får veta från identitetsleverantören är om användaren jobbar på företaget X eller inte. Detta ger ett starkare skydd för den personliga integriteten. Och med pseudonymer, som finns i både persistent och transient utförande går det att lösa.

Med persistenta pseudonymer får varje användare samma pseudonym varje gång hen loggar in via identitetsleverantören.

Det innebär att tjänsteleverantören kan personanpassa användarupplevelsen, utan att veta vem användaren är. Kopplingen mellan individ och pseudonym finns bara hos identitetsleverantören, som vid behov, exempelvis vid missbruk, kan tala om för tjänsteleverantören vem som står bakom en viss pseudonym.

Transienta pseudonymer är olika vid varje inloggning och kan alltså användas i tjänster där personanpassning inte behövs.

Anvisningstjänster visar användaren vägen till inloggningen?

I en federation med två eller fler identitetsleverantörer krävs ofta en anvisningstjänst, en central lista över de identitetsleverantörer som finns och som användarna får välja bland när de ska logga in.

Tekniskt är det en lösning som fungerar, den kan också innebära problem för användarupplevelsen. I stora federationer kan det framför allt innebära att listan med tillgängliga identitetsleverantörer blir väldigt lång.

Vill man underlätta för användarna finns det några tekniska grepp att ta till:

1. Se till att användarna är identifierade redan när de kommer till tjänsten. Hos de organisationer som utnyttjar en viss tjänst går det att bygga en portal där användarna loggar in och sedan får välja bland de tjänster som finns tillgängliga.
2. Om en användare kommer direkt till tjänsteleverantören utan ett giltigt identitetsintyg kan exempelvis användarens ip-adress utnyttjas för att göra en gissning om vilken identitetsleverantör hen är ansluten till.
3. En tjänsteleverantör kan också bygga en egen anvisningstjänst som i ett standardutförande bara visar ett begränsat urval av de identitetsleverantörer som är anslutna till federationen. Denna lista kan skapas dynamiskt och utifrån olika kriterier, till exempel besökarens ip-adress, innehålla de mest sannolika alternativen.

En inloggning till alla läromedel

För en elev som vill utnyttja ett digitalt läromedel som skolan betalar för skulle inloggningen kunna gå till så här, med hjälp av Skolfederation:

1. Kajsa Karlsson knappar in förlagets webbadress i webbläsaren.
2. Förlagets webbtjänst ser att Kajsa Karlssons ip-adress stämmer överens med en av de skolor som är anslutna till Skolfederation och som dessutom är betalande kund hos förlaget.
3. I Kajsa Karlssons webbläsare dyker en inloggningsruta upp. Hon kan inte se det, men i själva verket är det här en inloggning som sker mot hennes skolas servrar. Skolan agerar nämligen identitetsleverantör i Skolfederation.
4. När Kajsa Karlsson loggat in skickar hennes skola ett identitetsintyg till läromedelsförlaget. Det innehåller två viktiga faktauppgifter: Förlaget får reda på att Kajsa faktiskt är behörig användare och i vilken årskurs hon går. Därmed kan webbtjänsten anpassas så att rätt läromedel visas. Identitetsintyget innehåller också vad som kallas för en persistent pseudonym. Läromedelsföretaget behöver inte känna till Kajsas identitet. Däremot är det bra om läromedelsföretaget känner henne under ett påhittat namn. När användare 435234xer35 loggar in vet de hur långt i historieboken personen hade kommit och kan hoppa direkt till rätt sida. Med hjälp av pseudonymer kan en federation på detta sätt stärka individens integritet samtidigt som möjligheten till en personanpassad upplevelse finns kvar.
5. I stället för att gå direkt till förlagets webbplats kan Kajsa också gå via skolans portal. Där loggar hon först in i sitt konto på skolan och blir samtidigt, utan att hon märker det, autentiserad mot Skolfederation. På portalen kan en lista med de tjänster som finns tillgängliga via federationen visas, tillsammans med tjänster som skolan upphandlat vid sidan av Skolfederation. Från listan väljer hon den tjänst hon vill använda och klickar sig vidare.

Vinster med en federation

Vad nyttan med en federation är beror på perspektiv. För användare och deras organisationer finns vissa fördelar, för tjänsteleverantörer andra. Till detta kommer också branschövergripande vinster.

- **Nytta för användare:** Rätt implementerad stärker en federation användarens integritet. Enklare lösenordshantering och ett single sign on-förfarande förenklar vardagen. Inga nya konton måste skapas.
- **Nytta för organisationer:** En förenklad administration av användarkonton när de finns samlade i en databas och inte hos alla de tjänster som användarna utnyttjar. Minskar till exempel risken för att anställda som slutat fortfarande har åtkomst till tjänster.
- **Nytta för tjänsteleverantörer:** De behöver inte längre administrera användarkonton, utan kan fokusera på sin kärnverksamhet. Säkerheten ökar eftersom en användares identitet kollas en gång, på ett tillräckligt säkert sätt.
- **Nytta för branschen:** Om flera tjänsteleverantörer och brukarorganisationer samlas i en federation kan det driva utvecklingen i branschen som helhet. En federation med många skolor anslutna kan exempelvis göra det mer attraktivt för förlag att börja jobba med digitala läromedel, eftersom tröskeln för att nå ut med dem sänks. I ett större perspektiv innebär en federation minskade kostnader, eftersom både teknik och databaser kan återanvändas.

4. Men är det inte så här det fungerar idag?

Vid första anblicken kan det vara svårt att se skillnaden mellan dagens svenska e-legitimation och en federationslösning. I båda fallen är det ju en tredje part som intygar att du är du. Det är din bank som utfärdar ett BankID du sparar på din dator och använder för att legitimera dig med.

Skillnaden är att banken bara är inblandad första gången, när BankID:t skapas. Då sätter banken sin digitala signatur på filen som användaren laddar ner till sin dator. Tjänsteleverantören verifierar bankens signatur innan de släpper in användaren, som identifierar sig genom att visa upp sitt BankID och mata in ett lösenord.

Varje gång du använder det skickas däremot information direkt mellan din egen dator och tjänsten där du vill logga in i. Dessutom är det då alltid med personnummer du legitimerar dig.

I en federationslösning kontrollerar tjänsteleverantören aldrig användarnas identitet. Det är en uppgift som ligger på identitetsleverantören. När användaren identifierat sig skickar identitetsleverantören ett intyg till tjänsteleverantören som får fatta beslut om huruvida uppgifterna är pålitliga eller inte. Allt detta sker givetvis helt automatiskt, utan att användaren märker något av vad som sker bakom kulisserna. Ibland kan personnummer ingå i identitetsintyget. Men bara när det behövs, som hos vissa myndighetstjänster till exempel.

En inloggning – flera tjänster

En identitetsfederation som är implementerad på rätt sätt kommer alltså till rätta med många av de problem som finns med identiteter kopplade till fysiska individer. Men federationen har också potential att underlätta nätvardagen för användarna.

Det har länge funnits ett önskemål om en webb där användarna inte behöver hålla koll på massor av lösenord. Som vi sett kan en identitetsfederation realisera den drömmen. Men en federation kan dessutom ta enkelheten ett steg till.

Single sign on är idén om att en inloggning ska vara giltig på flera ställen. Har du väl autentiserat dig en gång ska du inte behöva göra det igen, bara för att du besöker en ny webbplats. Om två tjänsteleverantörer använder samma identitetsleverantör som du valt att använda för din digitala identitet, då är det tänkbart att du inte kommer att behöva logga in igen, när du går från den ena till den andra. Kontrollen av din identitet kommer i stället att ske helt automatiskt i bakgrunden.

Federationer för företag, organisationer och branscher

Det är inte bara i sin roll som privatperson och medborgare man har behov av en lättanvänd digital identitet. Också som anställd på ett företag är det välkommet.

Många företag har redan idag sin personal samlad i en databas med bland annat inloggningsuppgifter för det interna datanätverket och andra resurser som finns inne på företaget. Men anställda använder allt oftare tjänster som ligger utanför det egna företagets väggar, och inte sällan behöver besökare från utsidan släppas in via nätet.

Också här uppstår ett behov av återanvändning av användaruppgifter via federering. För ett företag är det praktiskt om den interna databasen med användaruppgifter också är den som är giltig för alla tjänster på nätet som de anställda använder. Ett sådant upplägg gör vardagen enklare för personalen, eftersom det idag är möjligt att erbjuda automatisk inloggning. Har man en gång loggat in på det lokala nätverket inne på företaget släpps man automatiskt in på de tjänster som företaget utnyttjar på internet. Företaget blir alltså sin egen identitetsleverantör och registerhållare, där tjänsterna som företagets anställda utnyttjar kan verifiera deras identiteter.

Det innebär också att företaget får betydligt bättre kontroll över användaruppgifterna, eftersom de finns samlade på ett enda ställe. Det finns därmed inte någon risk att en person som slutat på företaget kan fortsätta använda tjänster på nätet bara för att man glömt radera personens användaruppgifter överallt.

Tekniska lösningar för identitetsfederationer

När en federation ska realiseras, oavsett om det är på samhällsnivå eller mellan en handfull företag, är överenskommelserna mellan identitets- och tjänsteleverantörer viktiga. De måste bestämma vilka regler som ska gälla i federationen, hur användaruppgifter ska delas mellan deltagarna i federationen, hur uppgifterna ska lämnas ut till användarna på ett kontrollerat sätt och lösa ytterligare ett antal frågor kring formalia.

Utan en teknisk lösning blir dock överenskommelserna inte mer än bokstäver på papper. Och för att det praktiska genomförandet ska gå så enkelt som möjligt behövs det standarder, det duger inte att varje företag hittar på sitt eget sätt för att verifiera användare. Det skulle då bli alldeles för kostsamt för två företag att koppla sina system till varandra.

SAML, Security Assertion Markup Language,[7] är en av de mest använda standarderna för federationer. Bland annat används den i Skolfederation, Sambi och Swamid.

SAML är ett teknikval som har potential att lösa flera av dagens problem:

- SAML är en öppen standard, vilket bland annat kan innebära att fler teknikleverantörer kan utveckla lösningar med ett lägre pris som resultat. En tänkbar utveckling är också att nya aktörer på marknaden väljer att utveckla mer lättanvända lösningar än de som finns tillgängliga idag.
- En federation ger ett fullgott skydd av den personliga integriteten, bland annat genom att personnumret inte längre ska användas annat än i situationer där det verkligen behövs. Försäkringskassan kommer fortfarande behöva den informationen, men i de flesta kontakter med näringslivet är det en detalj som är utan relevans.
- En federation byggd på SAML är teknikneutral och kan därmed användas med alla tänkbara apparater som har en internetuppkoppling och som användarna kommer vilja identifiera sig i från.
- Öppnar möjligheten för företag och myndigheter som idag ger sina anställda tjänstelegitimationer att bli en part i federationen vilket skulle innebära att tjänstelegitimationerna blir användbara på fler ställen än idag.

Eftersom det finns stora pengar investerade i den lösning som används idag är målsättningen att dagens e-legitimationer ska följa med in i det nya systemet och bli en del av federationen.

Det finns också en förhoppning om en positiv spiral där fler aktörer innebär pressade priser, att fler väljer att skaffa och använda en e-legitimation vilket i sin tur medför att de blir användbara på fler ställen på nätet.

En annan lösning är OpenID Connect.[8] OpenID Connect har dels tagit lärdom av OpenID, en lösning som gör det enkelt för användare att använda samma inloggningsuppgifter på flera tjänster men som saknar många av de övriga delarna i en federation, och av SAML. En viktig aspekt av OpenID Connect är att lösningen även är väl lämpad för appar i mobiler och surfplattor. Medan SAML främst är en teknik för webblösningar kan OpenID Connect därför erbjuda liknande funktionalitet i mer appcentrerade verksamheter och organisationer.

Skolfederation och Sambi – två svenska federationer

Swamid är en svensk federation för studenter och anställda på högskolor och universitet. Skolfederation är en motsvarighet, men för

svenska grundskolor och gymnasier. Utvecklingen av Skolfederation leds av IIS och syftet är att underlätta för alla aktörer inom svenskt skolväsende:

- För lärare och elever innebär Skolfederation att de får färre inloggningsuppgifter att hålla ordning på. De loggar in en gång, och kan sedan komma åt alla de tjänster som skolan använder. Federationen stärker dessutom elevernas och lärarnas integritet, eftersom tjänsterna de använder inte behöver få reda på vilka de är.
- För skolans administrativa personal underlättas hanteringen av användaruppgifter. Det behöver inte skapas konton på många olika ställen, med alla problem i form av bortglömda lösenord och liknande som följer med varje nytt konto.
- De företag som utvecklar digitala läromedel eller andra typer av tjänster för skolan behöver kan fokusera på sin kärnverksamhet i stället för att bygga system för användarhantering. Det förenklar den tekniska utvecklingen, men minskar också behovet av support.
- För skolsektorn som helhet skalar en federation bort många tekniska trösklar som kan försena utvecklingen av digitala verktyg för skolan.

Sambi är en federation som vill lösa samma problem som Skolfederation, men inom svensk sjukvård. Här handlar det också om att förenkla för personalen. Med tanke på de känsliga uppgifter som hanteras inom sjukvården väger de säkerhetsmässiga aspekterna av en sådan federation extra tungt.

Interfederationer är federationer av federationer

Vi har redan konstaterat att drömmen om en e-legitimation som vi använder vilka tjänster vi än vill utnyttja sannolikt inte kommer att bli verklighet. Mot detta talar bland annat integritetsaspekter och tillitsfrågor. Bland annat skulle en central identitetsleverantör som sköter alla våra inloggningar också kunna se vilka tjänster vi väljer att använda och när. Mer trolig är därför en utveckling med flera parallella federationer, var och en anpassad för sin nisch och de behov som finns där.

Men där det finns överlapp mellan två eller flera federationer finns ändå möjlighet till samarbeten som ytterligare förstärker de positiva effekterna med en federation.

Exempelvis är ett samarbete mellan Sambi och Swamid en möjlighet. De studenter som läser till läkare eller sjuksköterska skulle då kunna återanvända sina användaruppgifter från Swamid när de är på praktik och behöver komma åt system som är en del av Sambi.

Den här typen av federationssamarbeten kallas för interfederationer. Och det finns inget som hindrar att de existerar över nationsgränser. Ett exempel på en existerande interfederation är eduGain, där Swamid ingår. I eduGain är det möjligt att använda inloggningen från sitt lärosäte – som ingår i Swamid – för att komma åt tjänster i andra federationer som ingår i eduGain.

5. Ett säkrare lösenord

1l28Y9lE

8xT74iz0

2iiH3kX5

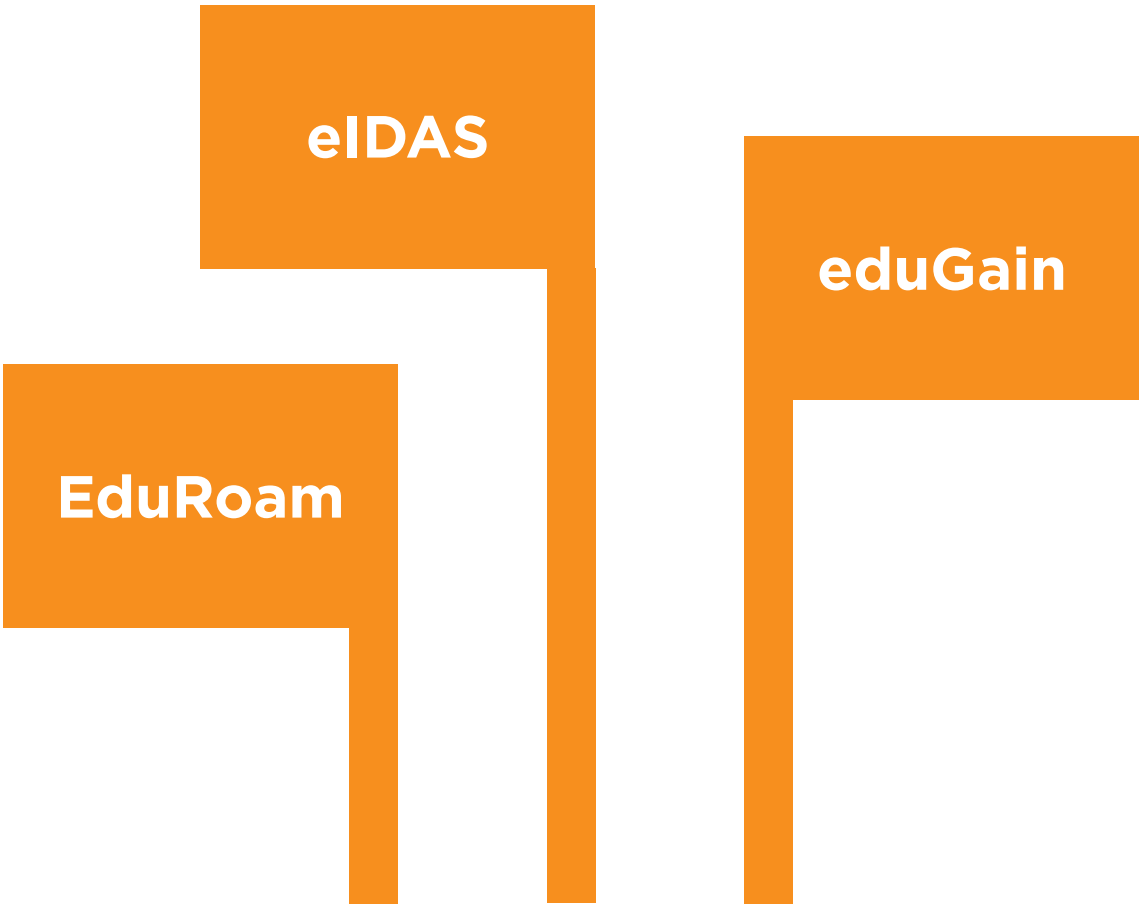
Även om det på sikt kommer att bli enklare för internetanvändarna att identifiera sig på nätet är det inte en utveckling som sker över en natt. Det innebär att den i dag dominerande lösningen med användarnamn och vanliga lösenord kommer att leva länge än. Därmed finns det också all anledning att fundera på hur du väljer och hanterar dina lösenord så att de blir så säkra som möjligt. Här följer några råd:

1. Välj inte lösenord som är lätta att gissa om man känner dig. Alltså inte barnens namn, hunden, katten, bilen, din födelsedag eller favoritlaget.
2. Välj inte ord som finns i en ordbok. Genom att låta en dator automatiskt testa lösenord går det snabbt att hitta de konton som valt riktiga ord.
3. Längden är viktig. Långa lösenord är svårare för en människa att gissa och en dator att knäcka. Genom att kombinera flera ord till en lösenfras kan det däremot vara enkelt för dig att komma ihåg.
4. Använd gärna några siffror och specialtecken, men undvik svenska tecken, så att du kan logga in även om du lånar en dator som saknar svenskt tangentbord.
5. Skriv gärna upp dina lösenord någonstans där andra inte kan hitta dem.

Om uppgiften att skapa och använda säkrare lösenord känns övermäktig, välj åtminstone ett säkert lösenord till din e-posttjänst. Har du glömt ett lösenord till en webbplats går det ofta att få ett nytt skickat via e-post. Och den som får tillgång till din e-post kan därmed också lätt skaffa sig tillgång till andra webbplatser där du har ett användarkonto.

Ett sätt att hantera lösenord är med ett hjälpprogram i datorn. Där lagras lösenord till alla de tjänster du använder på nätet. För att kunna se användaruppgifterna måste du först mata in programmets eget lösenord, ett lösenord som då väljs enligt principerna ovan.

6. Internationella projekt



Federationer är givetvis inte något som bara utvecklas i Sverige. Det finns många exempel i andra länder, både nationella och över nationsgränser. eduGain har redan nämnts som ett exempel på en internationell interfederation för högre utbildning. Ett annat exempel är Eduroam, också det en interfederation för utbildningsväsendet.

Syftet med Eduroam är att ge tillgång till internet, antingen trådlöst eller trådbundet. I Sverige drivs Eduroam av Sunet som sedan interfedererar med resten av världen. En koppling finns dessutom till Skolfederation, som satt upp en Eduroam-federation som ”interfedererar” med Sunets Eduroam-federation. Kopplingen gör det möjligt för Skolfederations medlemmar att ansluta till Eduroam, under förutsättning att den egna användarorganisationen aktiverat den möjligheten.

eIDAS

En stor europeisk federation som fått namnet eIDAS är på väg att byggas upp.[9] Enligt den ska nationella e-legitimationer som utfärdas av enskilda medlemsländer i EU börja gälla över EU:s nationsgränser senast den 29 september 2018.

Varje EU-land kommer fatta beslut om landets e-legitimationer ska gå att använda över nationsgränserna inom EU. Däremot blir det obligatoriskt för offentliga myndigheter inom EU – och i Norge, Island, Lichtenstein och Schweiz som också anslutit sig till förordningen – att acceptera e-legitimationer från andra länder. Det är alltså inget tvång att svenska e-legitimationer ska fungera utomlands, men om Sverige bestämmer att e-legitimationerna ska fungera utomlands måste myndigheter i övriga länder acceptera dem.

Kravet på de e-legitimationer som fungerar inom eIDAS är att de ska kunna spåras till endast en enskild individ och att de uppfyller tillitsnivå ”väsentlig” eller ”hög”.

Värt att notera är att det kan finnas andra lagar som sedan reglerar vilka tjänster utländska medborgare får ta del av. E-legitimationsnämnden skriver i dokumentet Introduktion till eIDAS:

”Att erkänna en utländsk e-legitimation på samma villkor som en svensk e-legitimation (till exempel Mobilt BankID eller Telia) betyder inte automatiskt en skyldighet för myndigheten att låta en individ få ta del av känslig information eller att få utföra ärenden i e-tjänsten. eIDAS har tillkommit för att underlätta ”digitalt först”, medan rättigheter och skyldigheter till service m.m. styrs av andra lagar och regler.”

I varje land kommer så kallade landsnoder att upprättas. När en EU-medborgare vill logga in på en myndighetstjänst i ett annat

land kommer den tjänsten att ta kontakt med landsnoden i sitt land. Landnoden står i sin tur för kontakten med landsnoden i det land där medborgaren bor och ser till att tjänsten får ett korrekt identitetsintyg tillbaka.

7. Ordlista

AAI
Authentication and authorization infrastructure. Används som samlingsbegrepp för tekniska lösningar för autentisering och behörighetskontroll.

Anvisningstjänst
Anvisningstjänst är en central funktion som listar de identitetsleverantörer som är anslutna till federationen och låter användarna logga in med den där deras konto finns. Ju fler identitetsleverantörer som är anslutna till federationen, desto större behov av anvisningstjänst.

Användare
De individer som använder tjänster på internet och borde ha en e-legitimation. Men i allt större utsträckning kan man också tänka sig att datorprogram, maskiner och annan teknisk utrustning får egna e-legitimationer när de kopplas till internet och behöver kommunicera med omvärlden på ett säkert sätt.

Användarorganisation
Samlingsnamn för företag, myndigheter eller andra organisationer, vars anställda utnyttjar tjänsterna i en federation.

Attribut
Uppgifter om en person i en federation. Används bland annat för att avgöra en individs behörighet i en tjänst. Attributen kan finnas lagrade hos identitetsleverantören, men också hos en tredje part, en så kallad registerhållare.

Autentisering
Att kunna visa upp och styrka sin identitet för en annan part.

Auktorisation
Att avgöra vilka rättigheter en autentiserad användare har i ett system. Kopplas ibland också till tillitsnivån som autentiseringen har genomförts med. Ett konkret exempel är nätbanker. Autentiserar kunden sig med ett lösenord är det bara möjligt att flytta pengar mellan de egna kontona, men om en engångsdosa används går det att köpa och sälja fonder och gör andra bankärenden också.

BankID
En av de idag mest spridda metoderna att använda e-legitimationer i Sverige är en fil som laddas ner från banken där användaren är kund och som tillsammans med ett lösenord kan användas för att styrka identiteten i kommunikation med bland annat myndigheter som Skatteverket och Försäkringskassan.

eIDAS
Det vardagliga namnet på EU-förordning nr 910/2014. Enligt den ska e-legitimationer börja gälla över EU:s nationsgränser den 29 september 2018.

eduGain
En europeisk interfederation för universitet och högskolor. Används för att tillhandahålla ett antal olika tjänster.

eduroam
En av tjänsterna inom eduGain. Eduroam ger personal och studenter tillgång till internetuppkoppling.

Federationsoperatör
Den part som sköter den centrala administrationen i en federation. Handlar bland annat om att tillhandahålla uppgifter till federationens parter om vilka andra som är anslutna till den.

Flerfaktorsautentisering
För att höja tillitsnivån används ibland flera olika tekniska lösningar samtidigt, exempelvis ett lösenord i kombination med en fil på datorn, som i fallet med BankID. En sådan kombination kallas för flerfaktorsautentisering.

Förlitande part
De tjänsteleverantörer som litar på en inloggning som görs via en identitetsleverantör kallas med ett annat ord för förlitande part.

Identitetsfederation
En samling identitetsleverantörer, tjänsteleverantörer och registerhållare som tillsammans utgör ett system för identiteter på nätet.

Identitetsintyg
När en användare autentiserar sig hos en identitetsleverantör i en federation skickar denna sedan ett identitetsintyg till tjänsten som användaren vill använda. Detta intyg innehåller bland annat information om att användaren är den han eller hon utger sig för att vara, och vilken teknisk lösning som har använts för autentiseringen. Det senare är viktigt för att tjänsteleverantören ska kunna avgöra vilka funktioner användaren ska få tillgång till (auktorisation).

Identitetsleverantör
De som i en identitetsfederation sitter på den grundläggande informationen om användarna och den part som också utför autentiseringen. Förkortas ofta IdP.

Interfederation
En federation av federationer. Genom att federationer samarbetar kan nyttan för användare och tjänsteleverantörer förstärkas ytterligare. Eduroam är ett sånt exempel.

LIS
En förkortning för Ledningssystem inom informationssäkerhet. Finns beskriven som en standard, ISO 27001, och används i federationssammanhang, bland annat för att säkerställa att alla parter har en gemensam vokabulär för vilka tillitsnivåer som finns och vad de innebär.

LoA
Förkortning för *Level of assurance*, ett standardiserat sätt att definiera tillitsnivåer. Anges i en fyrgradig skala, från 1 till 4. 1 är lägst, och innebär att det saknas eller bara finns en liten tillit till identiteten. I nivå 2 finns en begränsad tillit till identiteten, nivå 3 innebär hög tillit och nivå 4 mycket hög tillit till identiteten. Avgörande för LoA är bland annat hur rutinerna vid utlämnande av inloggningsuppgifter är utformade och vilka tekniska lösningar som används vid inloggning.

OAuth
En teknik som gör att hanteringen av lösenord på internet minskar. Används främst när tredjepartsprogram ska anslutas till nättjänster. Traditionellt har man då matat in sitt användarnamn och lösenord i programmet, men med OAuth kan programmen få behörighet att agera i användarens namn utan att lösenordet matas in.

OpenID
En teknik för identitetsfederationer med lägre tillitsnivå. Används främst av globala konsumenttjänster där behovet av koppling till fysisk individ saknas. Ett annat vanligt användningsområde är för kommentarer i bloggar.

OpenID Connect
En vidareutveckling av OpenID, anpassad för federationslösningar, främst för implementering i mobilappar och liknande plattformar. Detta till skillnad från SAML, som främst är en lösning för webbtjänster.

Phishing/nätfiske
Samlingsnamn för olika sätt att försöka lura användare att lämna ifrån sig information, som till exempel inloggningsuppgifter. Ofta sker det genom att falska webbplatser byggs, med ett utseende som exempelvis en känd banks. När användarna väl luras dit, via en länk i e-post eller på annat sätt, och matar in sina användaruppgifter hamnar uppgifterna i stället i händerna på individer med onda avsikter.

Registerhållare
I en identitetsfederation har identitetsleverantören den mest grundläggande informationen om användarna i sin databas. Ytterligare detaljer kan när de behövs hämtas från så kallade registerhållare. Det kan exempelvis vara Bolagsverket, som har information om svenska företags representanter, eller CSN:s register över studerande.

SAML
Den mest spridda tekniska lösningen för att bygga identitetsfederationer. Används bland annat i den federation som svenska universitet och högskolor har för att studenter och anställda ska kunna låna det trådlösa nätverket på alla anslutna lärosäten. Den federationen heter SWAMID.

Sambi
En federation för svensk sjukvård. Administreras av IIS. *Single sign on* – En lösning som innebär att användarna inte behöver mata in sitt användarnamn och lösenord på varje webbplats de besöker. Så länge alla webbplatser är anslutna till samma identitetsleverantör som användaren utnyttjar sker inloggningen automatiskt.

Skolfederation
En federation för svensk grundskola. Administreras av IIS.

Swamid
En federation för svenska universitet och högskolor. Administreras av Sunet.

Tillitsnivå
En gradering av hur pålitlig en autentisering är. Ju högre tillitsnivå, desto större sannolikhet att personen verkligen är den hen utger sig för att vara. På nätet har enkla lösenord låg tillitsnivå, eftersom de kan komma på avvägar, medan exempelvis dosor som skapar engångskoder har en högre. Det pågår ett standardiseringsarbete på global nivå för att ta fram en fyrgradig skala av tillitsnivåer.

Tjänsteleverantör
Företag eller myndigheter som tillhandahåller tjänster på internet. Har ofta ett behov att kunna identifiera sina användare. Idag sker det ofta med egna lösningar, men i en identitetsfederation ligger det ansvaret hos den identitetsleverantörer som tjänsteleverantören väljer att utnyttja.

Tvåfaktorsinlogg
En typ av flerfaktorsinloggning, där den användare som vill logga in i tjänsten på två olika sätt måste styrka sin identitet. En vanlig lösning är att ett lösenord kompletteras med en engångskod som antingen skickas till eller skapas i en app i en mobiltelefon.

Fotnoter

1. http://en.wikipedia.org/wiki/Ontheinternet,nobodyknowsyou%27readog
2. Att det sen avslöjas gång på gång på gång att den anonymitet som många upplever på nätet är långt ifrån absolut är en annan diskussion.
3. Andra begrepp för samma sak är tillitsnivå och level of assurance, ofta förkortat LoA följt av en siffra från 1 (för de mest osäkra identiteterna) till 4 (för de mest säkra).
4. Både Facebook och Twitter har dock infört något som kallas för ”verifierade konton” där företagen på olika sätt kontrollerat vem som faktiskt står bakom kontot. Ett verifierat konto kan dock inte fås av vem som helst.
5. Mer om DNS och DNSSEC i internetguiden DNS – internets vägvisare. https://www.iis.se/lar-dig-mer/guider/dns-internets-vagvisare/
6. Introduction to the Laws of Identity, http://www.identityblog.com/?p=354
7. Mer om SAML: https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language
8. Mer om OpenID Connect: http://connect2id.com/learn/openid-connect
9. E-legitimationsnämnden har publicerat ett dokument med information om eIDAS: http://www.elegnamnden.se/download/18.3810a01c150939e893f12d7b/1450693891890/E-legitimationer+enligt+eIDAS+N2015_2620_EF+2015-12-16.pdf

Skolfederation

Identitetsfederationen Skolfederation bygger på samverkan mellan dess medlemmar och är en standard för integration av skolhuvudmäns och tjänsteleverantörers system. Federationen är en gemensam infrastruktur, och alltså inte en central lösning. Därför har varje skolhuvudman valfrihet att välja sina egna leverantörer av digitala lärplattformar och verktyg. De som kan bli medlemmar i federationen är svenska skolhuvudmän, utbildningsanordnare och myndigheter, samt leverantörer av digitala tjänster till skolan.

Skolfederations lösning förenklar för elever och skolpersonal eftersom de kan få en enda inloggning till alla tjänster, både de som finns inom skolan och de som skolan nyttjar via internet.

Federationen gör det också lättare för leverantörer av digitala tjänster att erbjuda sina tjänster till skolan, genom att tillhandahålla en säker och pålitlig standardiserad inloggningsfunktion med mindre administration, och bidrar därmed på sikt till utveckling av tjänsteutbudet.

Skolfederation har tagits fram under ledning av SIS, Swedish Standards Institute och drivs av IIS, Internetstiftelsen i Sverige. Att Skolfederation har skapats är resultatet av ett större projekt, *IT-standarder för lärande*, som drivs av SIS med syftet att göra det lättare för skolan att använda digitala tjänster och digitalt innehåll med hjälp av gemensamma standarder.

Anders Thoresson

Anders Thoresson är journalist och föreläsare. Han har bevakat teknikutvecklingen sedan 1999. Först på tidningen Ny Teknik och sedan 2006 som frilans. Under åren 2011–2014 skrev han Teknikbloggen på dn.se. Han föreläser bland annat om digitalt källskydd för journalister och programmering i skolan för lärare och skolledare. Anders Thoresson har författat flera Internetguider för IIS, exempelvis om programmering för barn, it-säkerhet, webbpublicering och omvärldsbevakning. Du hittar dem här: internetguider.se

Foto: Sebastian LaMotte CC-BY ND

Digitala identiteter
Så fungerar federationer
IIS internetguide, nr 44. 2016.
Anders Thoresson

Författare: Anders Thoresson
Redaktör: Jessica Bäck
Projektledare: Jessica Bäck
Formgivning: AGoodId
Första upplagan
ISBN: 978-91-7611-855-9

Du hittar alla IIS utgivna Internetguider på internetguider.se

Vi driver internet framåt! IIS arbetar aktivt för positiv tillväxt av internet i Sverige. Det gör vi bland annat via projekt som samtliga driver utvecklingen framåt och gynnar internetanvändandet för alla. Exempel på pågående projekt är:

Bredbandskollen
Sveriges enda oberoende konsumenttjänst för kontroll av bredbandsuppkoppling. Med den kan du på ett enkelt sätt testa din bredbandshastighet. www.bredbandskollen.se

Internetdagarna
Varje höst anordnar vi Internetdagarna som är Sveriges ledande evenemang inom sitt område. Vad som för tio år sedan var ett forum för tekniker har med åren utvecklats till att omfatta samhällsfrågor och utvecklingen av innehållet på internet. www.internetdagarna.se

Internetfonden
Hos Internetfonden kan du ansöka om finansiering för fristående projekt som främjar internetutvecklingen i Sverige. Varje år genomförs två allmänna utlysningar, en i januari och en i augusti. www.internetfonden.se

Internetguider
IIS publicerar kostnadsfria guider inom en rad internetrelaterade ämnesområden, som webb, pdf eller i tryckt format och ibland med extramaterial. www.internetguider.se

Internetstatistik
Vi tar fram den årliga, stora rapporten ”Svenskarna och internet” om svenskarnas användning av internet och dessemellan ett antal mindre studier. www.soi2015.se

Webbstjärnan
Webbstjärnan är en skoltävling som ger pedagoger och elever i den svenska grund- och gymnasieskolan möjlighet att publicera sitt skolarbete på webben. www.webbstjarnan.se

Internetmuseum
I december 2014 lanserade IIS Sveriges första digitala internetmuseum. Internetmuseums besökare får följa med på en resa genom den svenska internethistorien. www.internetmuseum.se

Federationer
En identitetsfederation är en lösning på konto- och lösenordshanteringen till exempel inom skolans värld eller i vården. IIS är federationsoperatör för Skolfederation för skolan och Sambi för vård och omsorg. www.iis.se/federation

Internets infrastruktur
IIS verkar på olika sätt för att internets infrastruktur ska vara säker, stabil och skalbar för att på bästa sätt gynna användarna, bland annat genom att driva på införandet av IPv6. www.iis.se

Sajtkollen
Sajtkollen är ett verktyg som enkelt låter dig testa prestandan på en webbsida. Resultatet sammanställs i en lättbegriplig rapport. www.sajtkollen.se

Läs mer på nätet redan idag! På Internetguidernas webbplats hittar du mängder av kostnadsfria publikationer. Du kan läsa dem direkt på webben eller ladda ner pdf-versioner. Det finns guider för dig som vill lära dig mer om webbpublicering, omvärldsbevakning, it-säkerhet, nätets infrastruktur, källkritik, användaravtal, barn och unga på internet, digitalt källskydd och mycket mer. internetguider.se

Nya Internetguider!

Motverka nätmobbning!
Av: Åsa Secher

Att använda internet är lika självklart för barn och unga som att kliva upp ur sängen på morgonen. Och nätet är fantastiskt. Men när internet blir en plattform för kränkningar och mobbning är det lätt att som vuxen känna sig bortkollrad bland alla webbsidor och sociala appar.

Den här guiden vänder sig till dig som undrar vad du ska tänka på när du pratar med barn och unga om nätet, vad du kan göra om du får reda på att någon råkat illa ut, eller om någon behandlar andra illa på internet.

Guiden, som är ett samarbete med Bris, riktar sig till vuxna i barns närhet och handlar i huvudsak om barn i åldrarna 10 till 16 år.

Ungas integritet på nätet
Råd till dig som är vuxen
Av: Åsa Secher

Den här guiden belyser vad integritet på nätet betyder för unga idag. Det är ett viktigt ämne att ta sig an för att vi som vuxna ska kunna stötta och hjälpa barn och unga att känna var deras gränser går så att de inte råkar illa ut. Guiden riktar sig till vuxna i barns närhet och även om internetanvändandet börjar i tidig ålder, handlar innehållet framför allt om unga i åldrarna 10 till 16 år. Du får bland annat ta del av vad unga gör på nätet, vad grooming är, hur du som vuxen kan hjälpa unga att sätta gränser och vad Barnkonventionen säger om ungas rätt till integritet. Guiden är producerad i samarbete med Barnens Rätt i Samhället (BRIS).