Anders Thoresson

Igenkänd och identifierad

En guide om legitimationer på nätet

Igenkänd och identifierad

.SE:s Internetguide, nr 21
Version 1.0 2010

.SE klimatkompenserar för sina koldioxidutsläpp och stödjer klimatinitiativet ZeroMission. Se http://www.uwab.se/ för mer information om ZeroMission.

Författare: Anders Thoresson
Redaktör: Lennart Bonnevier
Formgivning, layout och redigering: Gunnel Olausson/FGO AB
Illustrationer: © Camilla Atterby
Första upplagan, första tryckningen.
Tryck: DanagårdsLiTHO, Ödeshög, 2010.
ISBN: 978-91-978952-3-1

Prenumerera

Du kan prenumerera på alla .SE:s Internetguider.
Skicka namn och adress till publikationer@iis.se.

.SE (Stiftelsen för Internetinfrastruktur) ansvarar för Internets svenska toppdomän. .SE är en oberoende allmännyttig organisation som verkar för en positiv utveckling av Internet i Sverige.

Organisationsnummer: 802405-0190
Besöksadress: Ringvägen 100 A, 9 tr, Stockholm
Brevledes på .SE Box 7399, 103 91 Stockholm
Telefon: +46 8 452 35 00. Fax: +46 8 452 35 02
E-post: info@iis.se www.iis.se

Förord

Jag heter Anders Thoresson. Jag är född den 9 mars 1975. Med mitt körkort är det påståenden som är lätta att bevisa i den fysiska världen.

I den digitala världen är det annorlunda.

Som många andra svenska medborgare har jag möjlighet att skaffa en e-legitimation som på samma sätt som mitt körkort intygar att jag är jag, fast på nätet.

Och skaffat en e-legitimation har jag gjort. Men nyttan av den är begränsad. Jag använder den i mina kontakter med Skatteverket och Försäkringkassan och när jag någon enstaka gång ska kolla när det är dags att besiktiga bilen. Men några andra ställen där jag har glädje av mitt BankID känner jag inte till.

Det vanligaste sättet att identifiera sig på nätet är fortfarande med ett användarnamn och lösenord. Trots att det är en kritiserad lösning med många brister.

Mängden inloggningsuppgifter som en nätanvändare idag har att hålla reda på är stor – och ökar. Dessutom säger ett enkelt användarnamn med tillhörande lösenord egentligen inget om vem jag är i den fysiska världen, eftersom få webbtjänster gör någon form av kontroll när ett nytt konto skapas. Ett enkelt lösenord duger därför sällan för tjänster där verkliga värden hanteras.

Men ny teknik är på gång. Målsättningen är att pålitlig identifiering med koppling till oss som fysiska individer ska bli tillgänglig på fler webbplatser, samtidigt som skyddet av den personliga integriteten stärks.

Den här Internetguiden handlar om elektroniska legitimationer och presenterar en del av den tekniska utveckling som pågår.

Jag vill också rikta ett tack till Fredrik Ljunggren, Leif Johansson och Anne-Marie Eklund Löwinder som bidragit med sina kunskaper på området.

Vänersborg, november 2010
Anders Thoresson

Förbättra

Om du hittar fel eller har synpunkter på denna guide kan du sända dem till publikationer@iis.se.

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 mottagare som står på kuvertet. 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.

I den fysiska världen ställer frågor om identitet sällan till några större problem. Det finns ett antal allmänt accepterade sätt att bevisa vem man är, sin ålder eller sin nationalitet. Och de fungerar lika bra i Sverige som utomlands.

”I den digitala världen saknas en universell legitimation.”

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

Istället har du ett unikt sätt att identifiera dig för nästan varje webbplats du brukar besöka. Många gånger, nästan alltid, är det med ett användarnamn och lösenord du själv valt. 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 någon universell e-legitimation hittar man i Internets 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 pappret 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 besöker 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. Om det vittnar inte minst återkommande tidningsartiklar om kändisar som drabbats av att andra människor skapat konton på Facebook eller Twitter i deras namn. Bland annat citerade flera medier ett Twitter-inlägg av Zlatan Ibrahimovic sommaren 2009 – för att senare bli uppmärksammade på att det inte alls var den riktige Zlatan som skrev att han börjat fundera på ett eventuellt klubbyte.[2]

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 givetvis viktigt att det är så nätet fungerar. Det är viktigt att de som besöker en webbplats tillåts vara anonyma och att det mesta av det de gör online inte går att koppla till dem som individer. Men det finns också många tillfällen när kopplingen till individ är oerhört 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.

Det kan vara privatpersoner som vill vara säkra på att de skickar e-post till 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 en tjänsteman på banken som finns i den andra änden. Allt oftare finns det skäl att verifiera parterna som deltar i kommunikationen på nätet.

För att lyckas med det 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

1 http://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog

2 http://www.kullin.net/2009/07/ap-quoted-fake-zlatan-on-twitter/

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.

Men två parallella tekniska förändringar är nu på väg att ge Internets användare en helt ny dimension av digital identitet.

Tekniskspår ett handlar om återanvändning. Att användarnamn och lösenord fungerar på fler än ett ställe, och att behovet av att hålla tiotals, kanske hundratals, lösenord i huvudet är på väg att försvinna. En viktig del är också att det inte bara handlar om återanvändning av inloggningsuppgifter, utan även andra delar av vår identitet. Våra vänskapsband till andra personer, inte minst. Det här är en utveckling som kommer att göra våra nätliv enklare, eftersom vi får färre användaruppgifter att hålla ordning på. Den kommer också göra nätet roligare, när fler tjänster låter oss använda dem tillsammans med våra vänner.

Men även om detta är en utveckling som kommer att göra nätlivet enklare för gemene man är det inget som ökar sannolikheten för att den som utger sig för att vara Kajsa Karlsson verkligen är Kajsa Karlsson.

Det gör däremot tekniskspår två, som handlar om just kopplingen mellan den fysiska och digitala världen.

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 som bekräftelse, 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 bekräftelsen. 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 an-

Illustration: © Camilla Atterby

vändarna ett enda lösenord till allt de sysslar med på nätet[3]. 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 2008[4] ett exempel. Det är en teknik som gör att en användares identitet på Facebook fungerar på många andra tjänster över hela nätet. Spotify, Twingly och Planeto är tre exempel på svenska företag[5] som gör livet enklare för sina användare på just det sättet. Idag finns det gott om tjänster på nätet där användarna inte behöver skapa ett nytt konto vid första besöket, utan istället kan logga in med sina användaruppgifter från Facebook.

”Idag finns det gott om tjänster på nätet där användarna inte behöver skapa ett nytt konto vid första besöket…”

Men Facebook Connect, och andra alternativ som Microsoft Live Messenger Connect och Twitter, löser bara det första problemet, att göra livet enklare för användarna. Det är lösningar som är perfekta

3 http://www.nyteknik.se/nyheter/it_telekom/allmant/article19401.ece

4 http://developers.facebook.com/blog/post/108

5 http://www.nyteknik.se/nyheter/it_telekom/allmant/article430963.ece

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. Ofta handlar det om kontakter med myndigheter eller affärsuppgörelser av olika slag. Trots att fyra miljoner svenskar har ett konto på Facebook ska vi inte förvänta oss att Skatteverket kommer börja använda Facebook Connect som inloggningsalternativ för dem som vill lämna in sin deklaration elektroniskt.

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: De är dyra att utnyttja för företag som vill identifiera användarna, de fungerar inte med alla tekniska plattformar och 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.

Även här är saker och ting på väg att hända. I den offentliga utredningen *Strategi för myndigheternas arbete med e-förvaltning*[6] som presenterades hösten 2009 ägnas det sjunde kapitlet åt e-legitimationer. Ambitionen är ett helt nytt system för e-legitimationer i Sverige, där dagens brister ska åtgärdas. Tanken är att i framtiden 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. Sommaren 2010 tillsattes en kommitté med uppdrag att ”förbereda och genomföra bildandet av en nämndmyndighet för samordning av statens och kommunernas hantering av metoder och tjänster för elektronisk identifiering och signering (e-legitimationer).”

Tillsammans är det här två utvecklingsspår som har potential att lösa stora delar av de identitetsproblem som finns på nätet.

6 http://www.sweden.gov.se/sb/d/11456/a/133813

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 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 assuransnivåer som ett sätt att avgöra hur pålitligt ett påstående om identitet är. Ett hemmagjort id-kort har en låg assuransnivå, 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 assuransnivåer gäller på nätet. Ett konto på Facebook har låg assuransnivå. 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.

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. Med ett BankID i datorn 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. Assuransnivån 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 istället 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 en fil

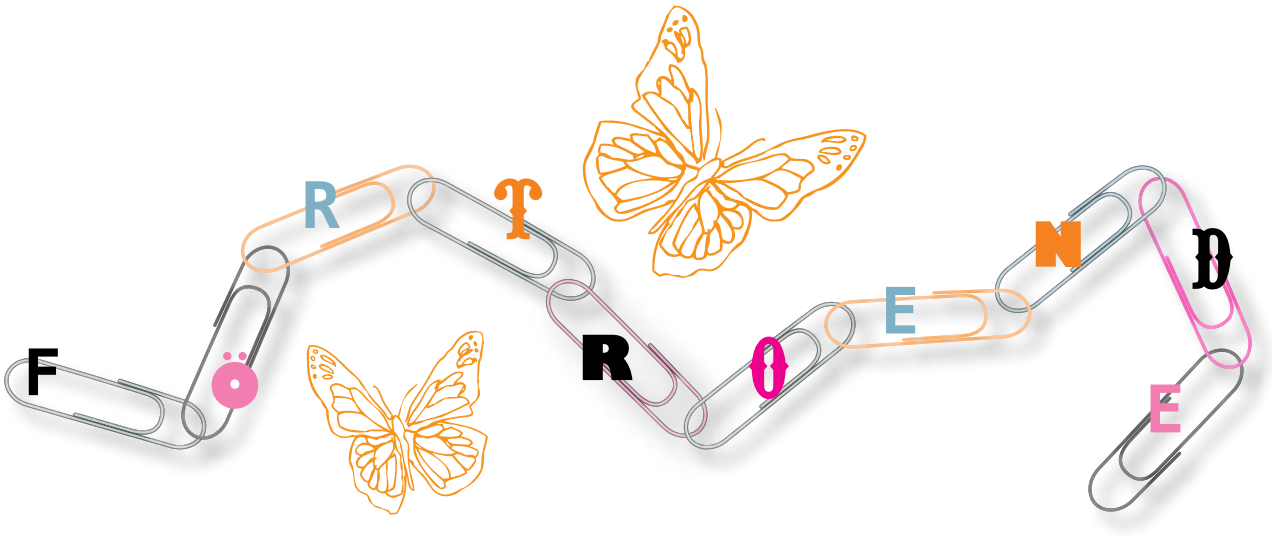


Illustration: © Camilla Atterby

som laddas ner till en dator är det en lösning som bara passar dem med en egen dator i hemmet. 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 som redan har konstaterats 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 assuransnivå. 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 assuransnivån 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 att 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 till exempel 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 trivialt krav, men alla phishingattacker på senare år visar att så inte är fallet. 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 kunder hos Nordea 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.[7] Varje webbplats på nätet har en IP-adress, en sifferkombination som talar om för webbläsaren från vilken webbserver sidan kan hämtas.

7 Mer om DNS och DNSSEC i Internetguiden *DNS – Internets vägvisare*. http://www.iis.se/Internet-for-alla/guider

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 Stiftelsen för Internetinfrastruktur har sin webbplats på en server med IP-adressen 212.247.7.221. Men det finns möjlighet att angripa även DNS-systemet och 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.

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*[8], en text med krav som ett identitetssystem bör uppfylla. Fortfarande idag är den sju punkter långa listan väl använd i diskussioner om hur framtidens lösningar för elektroniska identiteter ska 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 själva kunna ha sista ordet när det gäller vilka tjänster som får fråga efter personuppgifter och vad de tjänsterna 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 inte kommer att ha nytta av i framtiden och då 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.

8 http://www.identityblog.com/?p=354

”Den troliga utvecklingen är snarare att många id-system kommer att utvecklas, alla med sitt tänkta användningsområde.”

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 ovan (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 varit framgångsrika. Det menar 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-legitima-

tioner 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 dagens e-legitimationer långt i från optimala.

Men problemen handlar inte bara om att dagens lösning inte möter Kim Camerons sju krav. En annan nackdel är att de e-legitimationer som ges ut idag främst går att använda i kontakt med myndigheter, men inte särskilt ofta i andra fall där man som privatperson behöver legitimera sig på nätet. En förklaring till att få eller inga aktörer i det privata näringslivet har valt att ansluta sina tjänster till den befintliga infrastrukturen för e-legitimationer är att kostnaden är hög. Dessutom spelar användarnas personnummer 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 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

Illustration: © Camilla Atterby

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. Tanken är att den nya myndigheten ska starta sin verksamhet den 1 januari 2011, medan införandet av en ny nationell e-legitimation dröjer ytterligare något eller några år.

”...en ny myndighet som ska få i uppdrag att samordna det offentliga Sveriges behov av e-legitimationer.”

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 som Kim Cameron lyfter fram 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. Istället är det på juridiksidan som det behövs mycket arbete för att det ska bli möjligt.

Däremot kan man, menar Kim Cameron, hoppas på en utveckling där det blir enklare för tjänsteleverantörer på nätet att erbjuda pålitliga lösningar för identifiering av användare. Kim Camerons förhoppning är också att utvecklingen för identiteter på nätet ska följa den för datorer.

Idag behöver en programmerare inte bry sig om hur tangentbord, skärm, skrivare och andra delar som finns i eller kopplade till en dator fungerar. Det finns färdiga funktioner som de kan använda i

sina program för att tangentbord och mus ska fungera. På samma sätt önskar Kim Cameron en framtid där också funktioner för digitala identiteter är byggklossar, färdiga för utvecklare att använda.

En utspridd nätidentitet

Ska du boka en biljett med studentrabatt på ett flygbolags webbplats behöver företaget inte veta ditt personnummer. Det räcker om någon kan intyga att du faktiskt är student.

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.

Ett identitetssystem som fungerar på det här sättet, det vill säga att användaren kan välja att bara dela med sig av den information som är nödvändig i en viss situation, är möjligt 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 på en federation som redan är i drift, för att konkretisera idéerna och möjligheterna: 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 dela ut tillfälliga konton till 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 nog att använda det trådlösa nätverket på Chalmers under ett besök i Göteborg, utan att först besöka receptionen och legitimera sig där?

Så är det också. Lösningen heter SWAMID och är ett samarbete mellan svenska högskolor och universitet som gör just den resursdelningen möjlig. Skolorna har helt enkelt bestämt sig för att lita på varandras studenter och personal. Sen har en teknik som heter Eduroam använts för att bygga en lösning som gör det möjligt att

göra tillfälliga besök i vilket trådlöst nätverk som helst, utan att först skaffa ett gästkonto. Istället är det användaruppgifterna från det egna lärosätet som används för att få tillgång till det trådlösa nätet på skolan man besöker.

Identitetsfederationer brukar ofta kallas för en klubb av klubbar där medlemmarna har kommit överens om hur man ska lita på varandras användare. SWAMID är ett bra exempel på just den aspekten av en federation.

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, 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 delar ut kontouppgifter först efter legitimationskontroll fungerar federationen, men det räcker med att en part slarvar med kontrollen för att den genast ska få en svag punkt.

En överenskommelse kan bland annat omfatta:

- Gemensamma regler för hur nätverket får användas.
- Definition av begrepp som *student* och *personal*, om olika grupper av personer ska få tillgång till olika resurser.
- Regler i form av rutiner för hur lärosätena delar ut digitala identiteter till de egna studenterna. Ett lärosäte kan inte göra det på lösare boliner än de andra, till exempel utan att säkert kolla personernas identitet.

Men alla överenskommelser skulle inte bli mer än bokstäver på ett papper om de inte också omsattes i teknik. För att en students användaruppgifter ska fungera på alla lärosäten har därför deltagarna i SWAMID kommit överens om vilken teknisk lösning som ska användas.

Delarna i en federation

En identitetsfederation består av två delar. Det behövs minst en identitetsleverantör som sköter databasen med användaruppgifter och låter användarna identifiera sig. I den nya nationella identitetsfederationen är tanken att det ska finnas en myndighet som ackrediterar de företag som vill agera identitetsleverantörer. Tjänsterna de erbjuder utnyttjas sedan av tjänsteleverantörer och användare.

I en federation är det identitetsleverantören som har ansvaret för att kontrollera användarens identitet. Från identitetsleverantören får tjänsteleverantörerna reda på om användaren har identifierat sig på ett godkänt sätt.

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 tjänstens 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.

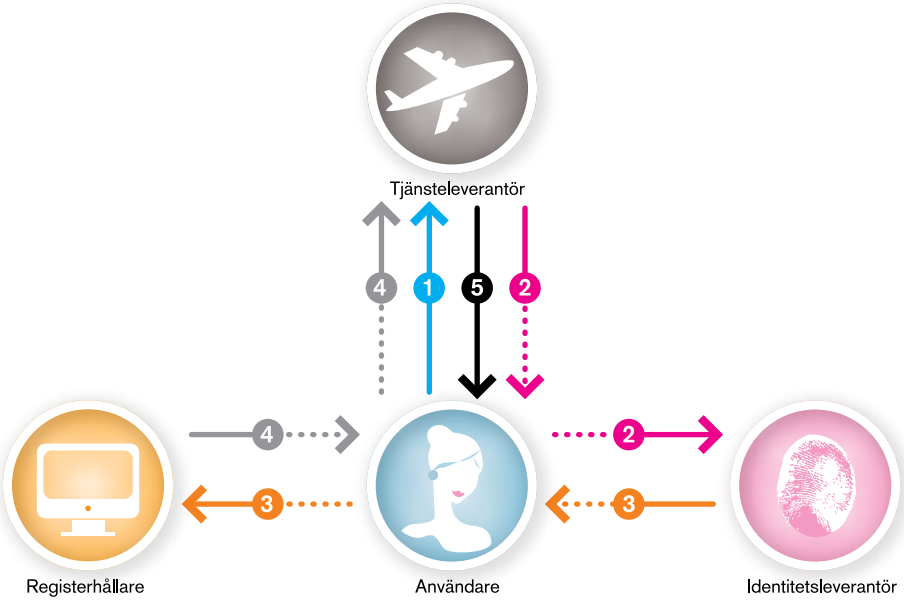
I relationen mellan identitetsleverantör och tjänsteleverantör finns en överenskommelse om hur lyckade inloggningar ska kommuniceras mellan parterna. Däremot finns inget som specificerar vilka tekniska lösningar som användarna ska kunna välja att använda för att legitimera sig. Det innebär att identitetsleverantörerna kan följa den tekniska utvecklingen och lägga till nya inloggningsmetoder i takt med att de dyker upp och får spridning på marknaden.

Vid sidan av identitets- och tjänsteleverantörer kan ytterligare

en part 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 har registerhållarna annan information med andra egenskaper om personerna lagrade, till exempel om en person är studerande eller inte.

För att göra detta mer begripligt återvänder vi till det här kapitlets inledning och personen som skulle beställa flygbiljetter med studentrabatt.

▶ Fullt utbyggd svensk identitetsfederation



I en framtid med en fullt utbyggd svensk identitetsfederation skulle det kunna, åtminstone i teorin, gå till så här:

1. Kajsa Karlsson surfar till flygbolagets webbplats, letar upp biljetten hon vill köpa och kryssar i att hon är studerande.
2. När hon bestämt sig för vilken avgång hon ska resa med och klickar på *Köp* skickar flygbolagets webbplats henne vidare till hennes identitets-

leverantör, och ställer samtidigt frågan om hon är studerande eller inte. Flygbolaget har sedan tidigare en överenskommelse med identitetsleverantören om att få göra identitetskontroller där.

3. Identitetsleverantören verifierar att användaruppgifterna stämmer. Därefter kan Kajsa vända sig till CSN, som är den registerhållare som har koll på vilka som är studerande i Sverige, och där få ett intyg på att hon verkligen är studerande.
4. När svaret från CSN kommit skickas ett paket med information tillbaka till flygbolagets webbplats: Ett *ja* eller *nej* som svar på frågan om Kajsa identifierat sig eller inte, information om hur hon har identifierat sig, om det bara varit med ett enkelt lösenord eller om en säkrare teknik har använts, och slutligen svaret på frågan om Kajsa är studerande eller inte. Detta informationspaket kallas för identitetsintyg och är bara giltigt vid detta enda tillfälle. Informationen om hur Kajsa identifierat sig är inte nödvändigtvis något som flygbolaget är intresserade av, men kommer vara användbart i många andra situationer. En banktjänst vill troligen erbjuda olika möjligheter beroende på om användarna bara identifierar sig med ett lösenord eller använder en säkrare metod.
5. Systemet på flygbolagets webbplats kontrollerar svaren som identitetsleverantören gett och avgör därefter som Kajsa ska få köpa sina flygbiljetter med studentrabatt eller inte.

Nu ska fördelarna med en federation förhoppningsvis vara tydliga:

1. Flygbolaget behöver inte hålla en egen databas med användarinformation uppdaterad, den delen står identitetsleverantören för. Det besparar företaget investeringar i teknik och kostnader för drift och underhåll av kunddatabasen, och gör att bolaget inte heller behöver lagra personuppgifter, med alla regler som omgärdar den typen av databaser.
2. Flygbolaget behöver aldrig få reda på Kajsas personnummer. Eftersom det valt att lita på identitetsleverantören nöjer sig flygbolaget med att få veta att Kajsa är den hon utger sig för att vara, och att hon verkligen är studerande och därmed berättigad till det lägre biljettpriset. Däremot används Kajsas personnummer i kommunikationen mellan identitetsleverantör och CSN. Personnumret är det unika sätt med vilket vi i Sverige skiljer individer

från varandra, och den vägen är det därför också möjligt att få svar på om Kajsa är studerande eller inte.

3. Genom att hämta information från registerhållare går det att komplettera den rena personinformationen med ytterligare egenskaper, i det här fallet huruvida Kajsa är studerande. På samma sätt skulle de två andra exemplen i kapitlets början fungera, med skillnaden att det är Skatteverkets personregister som kan lämna svar på frågor om föräldraskap och Bolagsverket som sitter på kunskap om befattningar i svenska bostadsrättsföreningar.
   Hela den här identitetskontrollen sker automatiskt i bakgrunden, utan att Kajsa märker vad som händer.

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; de 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 exemplet med Kajsa som ska köpa en flygbiljett behöver flygbolaget möjligen veta hennes namn. Men 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.

”...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.”

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.

Fördelar med federationer

Fördelar med en federationslösning är bland annat:

- Minskade kostnader, eftersom både teknik och databaser kan återanvändas.
- Ökad säkerhet, eftersom en användares identitet kollas en gång, på ett tillräckligt säkert sätt.
- Förbättrad integritet, eftersom den enskilde användaren får större kontroll över vilken information om honom eller henne som görs tillgänglig för tjänsteleverantörerna.
- Enklare för användaren, eftersom inga nya konton måste skapas och rutiner som är bekanta från en tjänst återkommer på andra.
- Enkel inloggning, om man identifierat sig för sin identitetsleverantör en gång kommer man åt alla tjänster som är anslutna till federationen, inom en viss tidsperiod.

▶ En dialog om identitet

Skulle det digitala samtalet om identitet mellan en användare och en tjänsteleverantör utspela sig i den fysiska världen idag skulle det kunna låta ungefär så här:

I en identitetsfederation skulle snacket gå ungefär så här:

Givetvis sker hela den här kommunikationen i bakgrunden, helt transparent för användaren.

En inloggning – flera tjänster

En identitetsfederation implementerad på rätt sätt kommer alltså till rätta med många av de problem som finns med identiteter kopplade till fysiska individer. Men de 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 sannolikt att du i framtiden inte kommer att behöva logga in igen, när du går från den ena till den andra. Kontrollen av din identitet kommer istället att ske helt automatiskt i bakgrunden.

Federationer för företag

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, federering, av användaruppgifter. 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 ytterligare ett antal frågor kring formalia.

Utan en teknisk lösning blir dock överenskommelserna inte mer än bokstäver på ett 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.

Idag finns två huvudsakliga val när det är dags att bygga den faktiska lösningen för federerade identiteter: SAML, *Security Assertion Markup Language*, och *Information Card*.

Vilken av de två som ska användas för den nya, svenska identitetslösningen är när detta skrivs hösten 2010 inte bestämt. Men mycket talar för att SAML blir den lösning som väljs, bland annat eftersom det är en teknik som redan är väl spridd. I Sverige är det bland annat SAML som används i högskolornas och universitetens identitetssamarbete 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.

Vid sidan av SAML och Information Card finns också en lösning som heter OpenID. Då OpenID i dagsläget saknar den starka kopplingen mellan digital och fysisk identitet lämpar den sig bäst i mer lättviktiga sammanhang på nätet. Exempel på tillämpningar är bland annat i kommentarsfunktioner i bloggar, där OpenID gör det möjligt att enkelt kommentera under ett och samma namn på många ställen.

En personligare identitet

Parallellt med teknikutvecklingen för federationer, främst som tekniklösning för situationer när en användares fysiska identitet måste verifieras på elektronisk väg, pågår en utveckling mot mer lättanvända men också mer lättviktiga identiteter. Detta gäller främst konsumenttjänster där koppling till den fysiska världen än så länge saknas, där kraven på assuransnivå är låga och den egentliga nyttan handlar om att underlätta för nätets användare.

Det främsta och bästa exemplet är just nu Facebook. Det sociala nätverket har på senare år tagit steget från att vara en egen avgränsad del av Internet till att ha en närvaro på många webbplatser runt om i världen.

Utvecklingen är en del i en trend där webben blir allt mer social, och där allt fler webbplatser bryr sig om vem du är och vilka vänner du har. Här är det inte kopplingen till den fysiska identiteten som står i fokus, utan snarare att göra nätlivet enklare och roligare.

Med Facebook Connect är det möjligt för företag på nätet att slippa utveckla egen teknik för att hantera användarinformation. Funktionen gör det möjligt för besökarna använda sina kontouppgifter från Facebook. Enkelheten i inloggningen är dock bara en av fördelarna med tekniken. En annan är att det inte bara är användarnamn och lösenord som återanvänds. Med till de tjänster som utnyttjar Facebook Connect följer dessutom de vänskapsband som användarna redan har byggt upp inne på Facebook.

Ett konkret exempel är Spotify som våren 2010 lanserade en ny version av sin musiktjänst. Målsättningen med den var att göra det enklare för vänner att dela musik med varandra. Spotify hade då två alternativ. Det ena var att bygga egen teknik för vänskapsband, så att man som Spotify-användare kan leta upp sina vänner och lägga till dem i en lista. Spotify valde att bygga en sådan lösning, men man valde också att utnyttja Facebook Connect.

Om du kopplar ditt Facebook-konto till Spotify kan den svenska

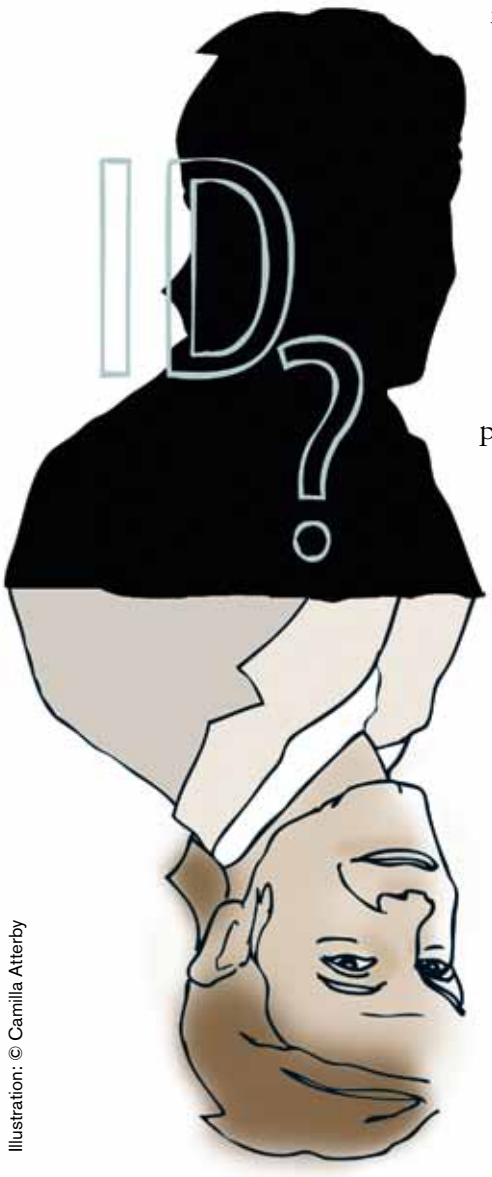


Illustration: © Camilla Atterby

musiktjänsten på egen hand leta reda på dina Facebook-vänner som också använder Spotify och lägga till dem i listan.

Facebook Connect påminner på många sätt om Microsoft Passport, en av de tekniska lösningar som var på tapeten redan på tidigt 2000-tal. Tanken med Passport var enkel: Microsoft skulle hålla en central användardatabas, andra tjänsteleverantörer skulle kunna utnyttja den för att användarna skulle slippa skapa ett nytt konto för varje webbplats de vill använda.

Men Passport fick kritik. Man såg integritetsrisker på grund av Microsofts centrala roll och möjliga affärsmässiga problem för de företag som var tänkta att utnyttja tjänsten. Passport blev heller aldrig någon stor framgång för Microsoft.

Samma kritik som riktades mot Microsofts Passport på tidigt 2000-tal förs idag fram mot Facebook Connect. Men trots det har Facebook på kort tid nått betydligt större framgångar än vad Microsoft gjorde. En stor del av förklaringen till varför ligger i möjligheten att återanvända vänskapsbanden som användarna byggt upp på Facebook, en möjlighet som saknades i Microsoft Passport. Att skapa en egen användardatabas som inte bara hade innehållit information om den enskilda användaren utan också kopplat ihop dem i en social väv hade varit tidskrävande och väldigt kostsamt. Med kopplingen till Facebook finns allt på plats första gången en användare loggar in på en ansluten tjänst.

För de inblandade parterna blir det en situationen där alla får klara fördelar:

- Tjänsteleverantörer på nätet får enklare och billigare utveckling, och tillgång till användarnas relationer. Därmed kan tjänsterna göras bättre och smartare.
- Bättre och smartare tjänster gynnar användarna, som visserligen får betala med sin integritet.
- Facebook stärker sin position på nätet, vilket på sikt kan ge dem ökade intäkter.

Facebook har alltså nått framgång där Microsoft Passport misslyckades. Men Microsoft har insett vikten av användarnas relationer och lanserade under sommaren 2010 Microsoft Live Messenger Connect. Precis som Facebook Connect handlar det om en teknik som gör det möjligt att återanvända de vänskapsband man har i Microsofts chattjänster på andra webbplatser. Liknande lösningar utvecklas på fler håll. Open Stack, som baseras på ett antal öppna standarder, är ytterligare ett exempel.

Ett säkrare lösenord

Även om framtiden ser ljus ut, och det på sikt kommer 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 är så säkra som möjligt. Här följer några råd:

1. **Välj inte lösenord som är lätta att gissa om man känner dig**. Inte barnens namn, hunden, katten, bilen, din födelsedag eller favoritlaget alltså.
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. **Välj en kombination av bokstäver, siffror och specialtecken**. Kanske ett ord eller ett namn där bokstaven *l* byts ut mot *1*, *a* mot *4* och *e* mot *3*. Och lägg till ett utropstecken på ett ställe där det passar. Undvik svenska tecken, så att du kan logga in även om du lånar en dator som saknar svenskt tangentbord.
4. **Skriv gärna upp dina lösenord någonstans där andra inte kan hitta dem**.
5. Nu kommer den svåra utmaningen: **Använd inte samma lösenord på många ställen**. Om man väljer lösenord enligt punkterna 1–3, och dessutom låter bli att skriva upp dem, hur gör man då för att komma ihåg dem? En lösning kan vara att hitta på en bokstavskombination som får utgöra basen i alla lösenord. Hette katten du hade som liten Kalle kan *k4ll3!* fungera. Sen lägger du till en kombination som är unik för varje webbplats eller tjänst som skyddas med ett lösenord. Ett förslag kan vara första och sista bokstaven i domännamnet. Finns webbplatsen på

adressen hemligtjänst.se skulle lösenordet alltså bli *k4ll3!he*. Lätt för dig att komma ihåg, men väldigt svårt för andra att gissa sig fram till.

”Om uppgiften att skapa och använda säkrare lösenord känns övermäktig, välj åtminstone ett säkert lösenord till din e-posttjänst.”

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.

Lämna inte ifrån dig ditt lösenord

Att man inte ska lämna ifrån sig sitt lösenord till andra personer är ett självklart och uppenbart råd. Men på senare år har en ny situation uppstått, när program vill veta ditt användarnamn och lösenord för att kunna ladda upp bilder till fotosajten Flickr eller skicka ett inlägg till Twitter. Att mata in sina användaruppgifter i ett program är alltid en potentiell risk, det går inte vara säker på att programmet inte skickar uppgifterna vidare till någon som inte ska ha dem.

Problemet är uppmärksammat, och en lösning finns: OAuth. OAuth är en teknik som gör det möjligt att låta program och tjänster på nätet agera i ditt namn, utan att för den sakens skull känna till ditt användarnamn och lösenord. Lite påminner tekniken om de speciella parkeringsnycklar som finns till vissa lyxbilar. Med en sådan kan hotellpersonalen köra bilen från receptionen till parkeringen, men övriga funktioner i bilen blir begränsade. Med OAuth är det möjligt att ge ett datorprogram rätt att agera i ditt ställe,

utan att behöva förse det med lösenordet som behövs för att kunna utnyttja tjänstens alla funktioner.

Finns OAuth som alternativ är det därför rekommenderat att alltid använda den möjligheten istället för att mata in användarnamn och lösenord.

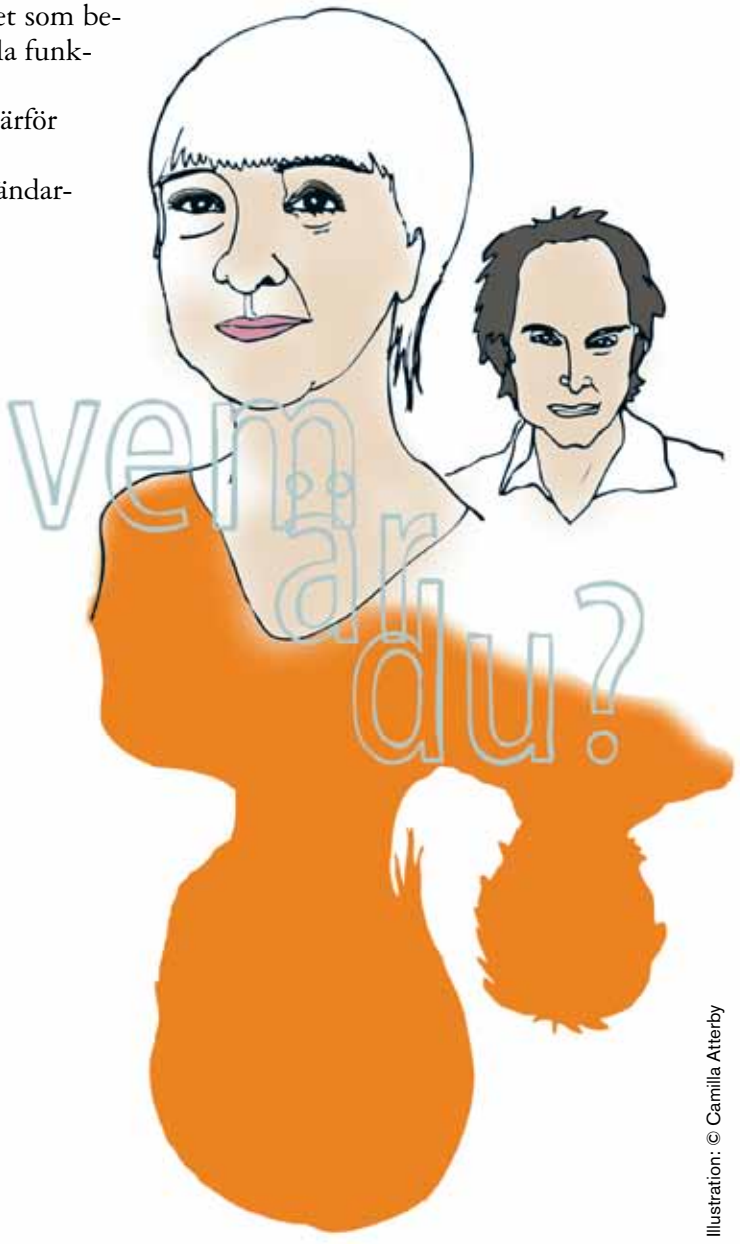


Illustration: © Camilla Atterby

Internationella projekt

Det är inte bara i Sverige som det pågår förberedelser för storskaliga, nationella identitetsfederationer. Här är två andra exempel.

EU-projektet Stork

På EU-nivå finns *Secure Identity Across Borders Linked*, förkortat Stork. Målsättningen är att utveckla tekniska lösningar och byråkratiska processer som ska bana väg för elektroniska legitimationer som ska fungera i hela Europa. Projektet har pågått sedan 2007, med fokus på både teknik och juridik.

För att få erfarenheter av att driva identitetsfederationer som sträcker sig över nationsgränser ryms fem delprojekt inom Stork, där teknik och juridik testas i praktiken:

1. *Cross-border Authentication Platform for Electronic Services* – en samling informationsportaler där besökare kan logga in. Syftet är bland annat att visa att specifikationerna som Stork arbetat fram är tillräckligt robusta för att fungera på mellannationell nivå.
2. *Safer Chat* – ett projekt för att göra nätet tryggare för barn och ungdomar, genom att göra det tydligare vilka det är som är med och chattar.
3. *Student Mobility* – syftar till att göra det lättare för utbytesstudenter att komma åt information vid universitet där de studerar, genom att använda en elektronisk legitimation från sina hemländer.
4. *Electronic Delivery* – ska visa hur elektroniska dokument på ett säkert sätt kan skickas mellan länder, vilket är ett viktigt fundament för framtida e-tjänster från myndigheter.
5. *Change of Address* – en tjänst där boende i EU kan göra flyttanmälan via nätet. Här deltar svenska Skatteverket, och det går bland annat att göra en flyttanmälan dit med hjälp av exempelvis ett spanskt e-id.

Ny amerikansk e-legitimation

Precis som i Sverige pågår just nu ett arbete i USA med att ta fram en ny, nationell e-legitimation. I ett utkast till en ny nationell strategi, *National Strategy for Trusted Identites in Cyberspace*, konstateras bland annat att över tio miljoner amerikaner drabbas av identitetsstölder varje år.

Målsättningen är att bygga ett system där privatpersoner kan komma åt information och tjänster på nätet, med mindre risk för identitetsstölder och bedrägerier än i dag, och utan att användarna behöver hantera en massa olika användarinformation.

I det amerikanska strategiutkastet nämns en mängd fördelar med identitetsfederationer: Tekniken ger ökad säkerhet, en enklare nätupplevelse när färre lösenord ska hanteras, ökad integritet när användarna får kontroll på vilka personliga uppgifter det är som används, ett större utbud av tjänster gör e-legitimationen mer attraktiv att använda och gynnar samtidigt innovation.

Ordlista

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.

Assuransnivå – En gradering av hur pålitlig en autentisering är. Ju högre assuransnivå, desto större sannolikhet att personen verkligen är den han utger sig för att vara. På nätet har enkla lösenord låg assuransnivå, 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 assuransnivåer.

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 assuransnivån 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.

Federation – Se identitetsfederation.

Flerfaktorsautentisering – För att höja assuransnivån 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.

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.

Information Card – En teknisk lösning för att bygga identitetsfederationer. Bakom den står bland andra Microsoft.

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 assuransnivå. Används främst av globala konsumenttjänster där behovet av koppling till fysisk individ saknas. Ett annat vanligt användningsområde är för kommentarer i bloggar.

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 istället 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.

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.

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.

Rekommenderad läsning

För den som vill veta mer om digitala identiteter på Internet är följande texter rekommenderad läsning:

Strategi för myndigheternas e-förvaltning, SOU 2009:86 (Kapitel 7.)
http://www.sweden.gov.se/sb/d/11456/a/133813

Federering och federerade identiteter för det offentliga IT-Sverige.
Heimore Group.
http://heimore.com/PageFiles/310/Federering.pdf

National Strategy for Trusted Identities in Cyberspace.
http://www.dhs.gov/xlibrary/assets/ns_tic.pdf

Kim Camerons *The Laws of Identity*.
http://www.identityblog.com/?p=354

Om författaren

Anders Thoresson är journalist och har under drygt tio år bevakat utvecklingen inom IT och telekom. Han har tidigare arbetat på Ny Teknik, men är idag frilans.

Adressen till hans webbplats är http://anders.thoresson.net. Han kan också nås med e-post skickad till anders@thoresson.net.

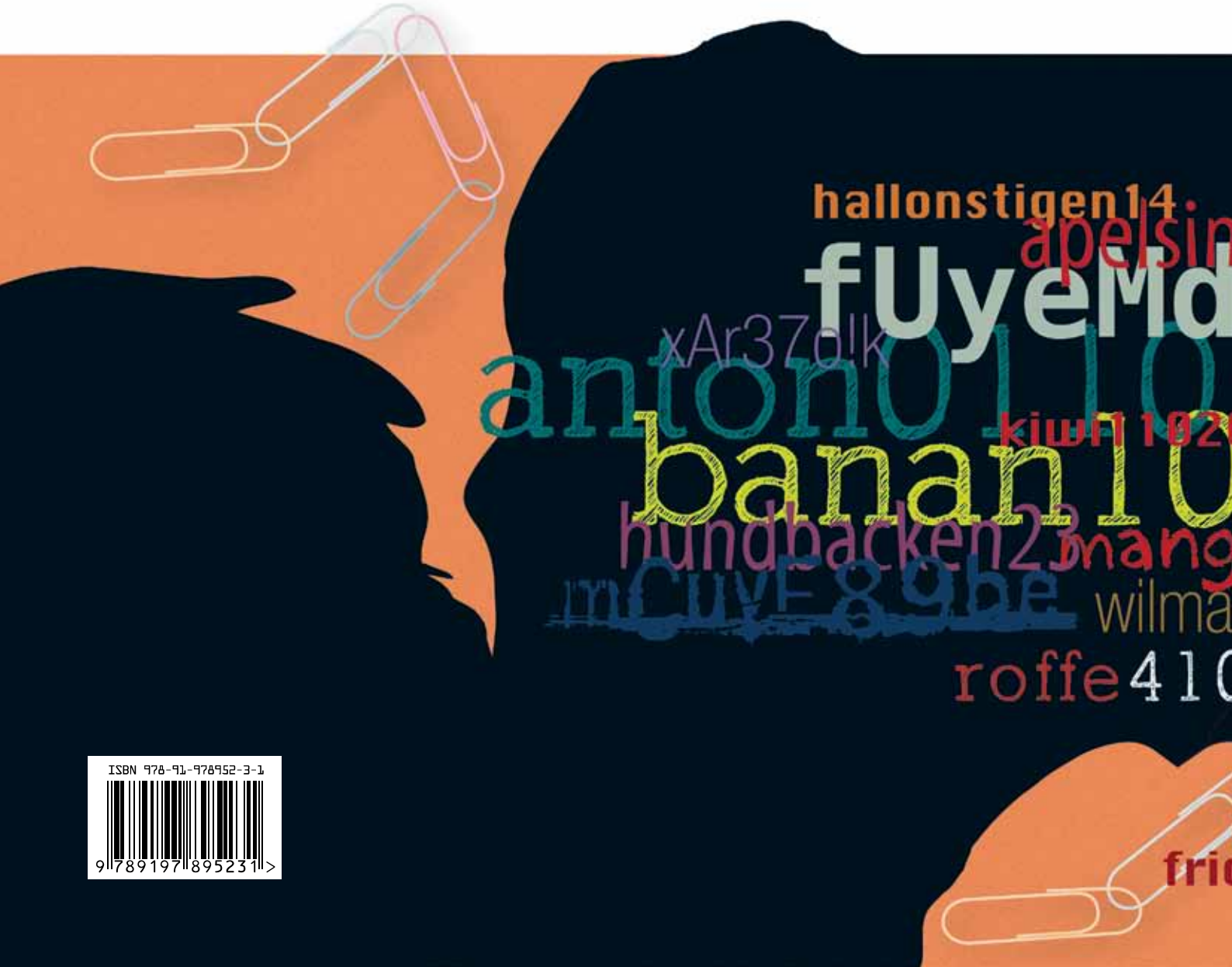
.SE (Stiftelsen för Internetinfrastruktur) är en oberoende allmännyttig organisation som verkar för en positiv utveckling av Internet i Sverige. Utöver att ansvara för Internets svenska toppdomän bedriver .SE ett omfattande utvecklingsarbete:

- **.SE:s Internetguider** är en skriftserie som riktar sig till intresserade lekmannaanvändare och behandlar olika Internetfrågor. Denna publikation ingår i serien. Läs mer: iis.se/internet-for-alla/guider.
- **Webbstjärnan** är en tävling i webbpublicering för skolan. Syftet är att dra nytta av Internets möjligheter i skolarbetet, genom att bygga en webbplats kring ett valfritt skolarbete. Läs mer: webbstjärnan.se.
- **Digital delaktighet.** .SE bidrar till olika åtgärder för att förbättra tillgängligheten till Internet för de grupper som idag inte är anslutna till nätet. Läs mer: iis.se/internet-for-alla/digital-delaktighet
- **IPv6 och DNSSEC** är två viktiga teknikprojekt som ska säkerställa att Internets infrastruktur även i fortsättningen kan vidareutvecklas och fungera säkert. Läs mer: ipv6forum.se respektive iis.se/domaner/dnssec.
- **Bredbandskollen** är ett konsumentverktyg som hjälper bredbandskunder att utvärdera sin bredbandsuppkoppling. Läs mer: bredbandskollen.se
- **Internetstatistik** .SE har tagit initiativ för att etablera ett samarbete kring statistik och fakta om Internet, vilket bland annat resulterat i den tryckta rapporten Svenskarna och Internet. Läs mer: iis.se/internet-for-alla/guider och internetstatistik.se.
- **Internetfonden** bidrar till Internetutvecklingen genom att finansiera fristående projekt. Bland uppdragstagarna finns organisationer, privatpersoner och akademiska institutioner. Läs mer: iis.se/internet-for-alla/internetfonden.
- **Internetdagarna** är .SE:s årligen återkommande konferens för alla som arbetar med Internet. Läs mer: internetdagarna.se

.se

Som en del i .SE:s arbete med Internetutveckling producerar .SE ett antal skrifter under produktnamnet .SE:s Internetguider. Guiderna behandlar olika Internetrelaterade områden och riktar sig i första hand till intresserade lekmannaanvändare. En guide kan vara såväl en praktisk handbok som en mer beskrivande rapport.

.se
Stiftelsen för Internetinfrastruktur



ISBN 978-91-978952-3-1