Facebook eller eID för inloggningen?

Låt skyddsvärdet avgöra säkerhetsläget

2010-06-10: Sven-Håkan Olsson

RÄTT TRÖSKEL Riktigt hög säkerhet innebär krångel för användaren. Även om användandet av e-legitimationen fått snurr är nog de flesta överens om att e-legitimation till minsta e-tjänst innebär mer krångel än vad informationen är värd. Man måste helt enkelt noga överväga vad det är för information man skyddar och till vilket pris när det gäller bekvämlighet.

I många fall är hög säkerhet vid den identitetskontroll (autenticering) som sker vid inloggning helt nödvändig. Om till exempel en bankgirobetalning i internetbanken ska godkännas eller om en myndighet ska kunna acceptera en e-ansökan som annars hade krävt underskrift med bläckpenna, ja då behövs hög trovärdighet kring vem personen som sitter vid webbläsaren verkligen är.

Men säkerhetsnivån kostar bekvämlighet. Riktigt hög säkerhet kräver både teknisk precision och organisatorisk noggrannhet (läs: byråkrati).Tänk till exempel på hur mycket krångligare kreditkortsbetalningarna i webbutiker blivit på den senaste tiden, på grund av att kortbolagen velat höja säkerheten.

eID bra men matchar inte våra beteenden

E-legitimationen (eID), som definierades via ramavtalsupphandlingar och detaljutformades av bankerna, har fått ett bra genomslag inom den offentliga sektorn. Jag tycker absolut att sajter bör erbjuda sådan inloggning, inte minst eftersom det nu finns ett stort antal miljoner medborgare som har ett aktivt eID. Det är också bra att det har utvecklats en juridisk konvention för när eID duger för inloggning eller e-underskrift och inte. Det minskar nervositeten och obeslutsamheten kring att skapa nya, nyttiga e-tjänster.

E-legitimationen får idag anses hyfsat bekväm. Men det finns förstås invändningar. Det ska vanligen installeras något på klientdatorn som kan krångla och vars dialoger är tämligen obegripliga för gemene man. Man får ännu en liten ikon bland allt skräp nere på statusraden som tar kapacitet och gör datorstarten långsam.

Många användare av företagsdatorer har inte rätt att installera mjukvara och då kanske eID faller helt. Personer använder ofta flera datorer, mediadatorn vid teven hemma, den bärbara, den gamla men fortfarande fungerande reservdatorn som behövs när barnen behöver den snabba nya datorn för att köra spel – och i alla dessa datorer ska man då ha ett tillräckligt färskt eID nerladdat (som man dessutom ska komma ihåg lösenordet till).

Tillfälligt använda datorer i internetcaféet, på biblioteket, i medborgarkontoret eller i hotellobbyn fungerar

vanligen inte alls med eID. Och yngre personer kan inte få eID.

Vad som är ännu viktigare är att vi redan idag vill nå Internet från så många fler sorters enheter än traditionella persondatorer, och mängden enheter accelererar. Även enkla mobiltelefoner är internetklienter, iPhones och andra smartphones är det i ännu högre grad. Surfplattor, iPads och vad det kan vara dyker upp. Mp3-spelaren. En Spotify-funktion i stereon? Kylskåpet får en skärm på framsidan. Spelkonsolerna. GPS-navigatorn. Dessa enheter klarar knappast eID.

Även om fler enheter framöver kan få stöd för eID och att eID säkert vidareutvecklas över tiden, så kan vi vara säkra på att det hela tiden utvecklas nya prylar som kommunicerar via Internet och som inte kommer att ha möjlighet att använda en högsäkerhetsplattform som eID.

Medborgarna kommer att vilja nå myndigheternas, landstingens och kommunernas e-tjänster från de här enheterna. Det blir obegripligt varför jag kan använda e-post, Google Maps och Spotify i mobilen men inte kolla upp om det gått framåt med byggnadstillståndet eller med lagningen av hålet i gatan som jag anmält. Inte nog med det, eID behöver i framtiden bli ännu säkrare än i dag och det är osannolikt att krångligheten därvid skulle minska.

eID till allt är som att skjuta mygg med kanon

Man rekommenderar ibland att kräva eID för vareviga sorts e-tjänst, oavsett vilket skyddsvärde informationen och funktionen i tjänsten kräver. Detta är att skjuta mygg med kanon. Tvärtom kan man ofta erbjuda enklare inloggningskvalitet parallellt för att skapa större bekvämlighet.

Visserligen ger det en viss kostnad att implementera flera inloggningssätt, men en del av dem är väldigt enkla att montera in. Det kan också vara en viss pedagogisk utmaning att få det begripligt med flera inloggningssätt, så man måste lägga lite jobb på användarvänligheten.

Observera att eID bör finnas tillgänglig parallellt med enklare inloggningar i applikationen. För den som råkar sitta vid en dator där personligt eID finns installerat är just eID ofta det bekvämaste.

Vem utfärdar identitet – och via vadå?

Ibland blir det lite rörigt eftersom man blandar ihop två saker, federeringsmekanism och identitetsutställare. Båda dessa måste ha en bra kvalitet för att höja säkerheten.

Federeringsmekanismen är någon form av tekniklösning som gör att informationen om en aktiv inloggning går att överföra från en sajt (exempelvis Facebook) till sajten som användaren därefter vill gå in på. Ibland används begreppet single-sign-on, SSO.

Identitetsutställaren, ibland kallad Identity Provider Idp, är den som säger att surfaren är en viss person. Men hur säkert gör identitetsutställaren detta?

I samband med dagens eID är det oftast bankerna som garanterar identiteten och de kräver att ett gammalt hederligt id-kort visas upp när någon ska teckna ett bankkonto.

För Facebook, Hotmail, Google och alla sådana tjänster finns egentligen ingen säkerhet kring vem som är vem. Och nu påstår jag att vi ska lita på de identiteterna, åtminstone till en viss säkerhetsnivå? Jo, vi kan tänka oss att en

kommun har en pappersblankett att fylla i och underteckna där medborgaren själv anger personnummer och vilket Facebook-konto denne har!

Då har vi på hyfsad säkerhetsnivå löst att kommunsajten kan veta vem som kommer surfande via en inloggning på Facebook. Federeringsmekanismen FacebookConnect är i sig skapligt säker och koppling till personnummer är gjord. Och det är ju precis det vi önskar ibland, högre bekvämlighet om än med lite enklare säkerhet.

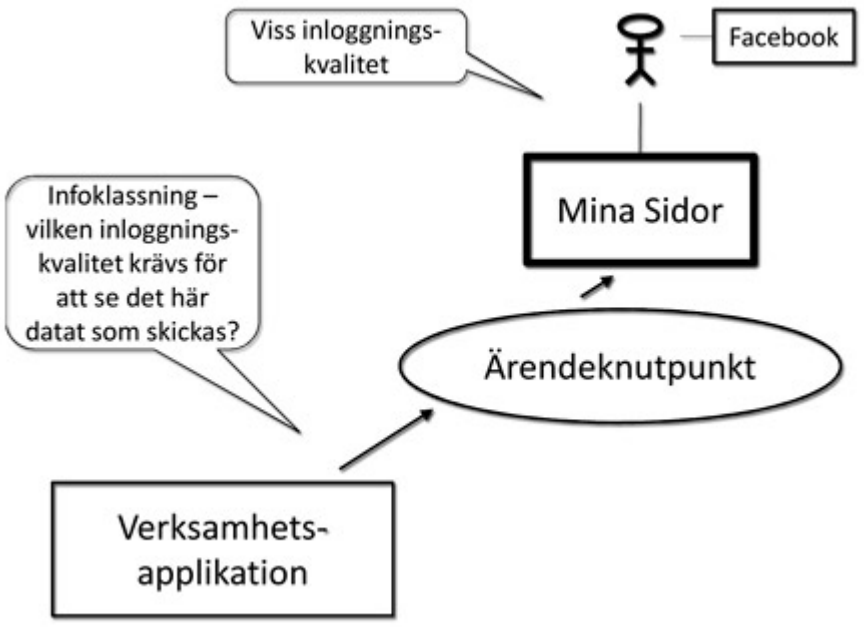
Den kvarvarande invändningen är kanske den där omoderna pappersblanketten jag förutsatte, även om det är en engångsföreteelse. Men då kan jag väl vid tillfälle logga in med bättre säkerhet via eID och i en dialog ange kontaktuppgifter såsom mitt Facebook-kontonamn så det ska kunna funka vid kommande inloggningar ifall säkerhetsbehoven är enklare?

Här får man tyvärr anse rättsläget lite oklart. Delvis står kommersiella avtalsformuleringar för eID emot konkurrenslagstiftningen. Men om jag själv vore sajtansvarig skulle jag nog våga mig på att erbjuda inmatning under eID-inloggning av sådana kontaktuppgifter som Facebook-kontonamn. Eller uppgift om någon välspridd konkurrent till Facebook.

När behövs vilken säkerhet?

Alltid när man skapar interaktiva sajter bör man utreda vilket skyddsvärde informationen och funktionen i tjänsten har. Det är självklart att ett socialärende har mycket högre sekretesskrav än att kolla hur det går med lagningen av gatan.

Om man arbetar med Mina Sidor, ihopkopplade ärendesystem, ärendeknutpunkter och liknande så är ofta information om ärendehändelser skickad från någon verksamhetsapplikation, och det är personerna som kan den applikationen som är bäst lämpade att bedöma informationsklassningen.



Jag har uppdrag åt Sambruk (en förening som består av 80-talet kommuner i hela Sverige som samarbetar) och där har jag föreslagit nedanstående nivåer av säkerhet. Tanken är att en sändande applikation ska kunna ange vilken inloggningssäkerhet som minst behövs för att någon ska få tillgång till just det datat som skickas. Tanken är också att nivåerna ska vara mycket konkreta och lättförståeliga.

I enstaka sammanhang kan det därmed behövas en mer komplex säkerhetsstruktur än så, men förhoppningen är att nivåerna nedan täcker in alla de vanliga fallen. Vad jag vet finns det inte definitioner skapade sedan tidigare av detta konkreta och enkla slag. Men kontakta mig gärna ifall ni känner till alternativ eller hittar invändningar!

Observera att om federeringsmekanismen är av bra kvalitet är det inloggningskvaliteten hos sajten som man förlitar sig på som avgör vilken resulterande nivå det blir. Det alltså den svagaste kedjan i länken som avgör. Mitt återkommande exempel med Facebook har inloggning med ett ganska starkt användarnamn/lösenord så nivån enligt tabellen torde bli 3300.

Förkortning för nivån av inloggning	Kod-värde för nivån	Kommentar	Typ av inloggning (s.k. "faktor")
SBKStarktBioID3F	7600	Enligt SBKStarktBioID men dessutom krävs kombination med både "något jag HAR "och "något jag VET"	Något jag ÄR och HAR och VET
SBKStarktBioID2F	7300	Enligt SBKStarktBioID men dessutom krävs kombination med "något jag VET"	Något jag ÄR och VET
SBKStarktBioID	7000	Någon av de underliggande nivåerna, kombinerat med biologisk igenkänning (fingeravtryck, ögonscanning etc).	Något jag ÄR
SBKStarktID	6000	Koddosa, hårt eID, annat smartcard etc utdelat under motsvarande säkerhet som eID. För denna nivå krävs kombination med "något jag VET".	Något jag HAR
SBKMobilEngangskod	5000	Engångskod via mobiltel el motsv. För denna nivå krävs kombination med "något jag VET".	Något jag HAR
SBKMjuktCert	4000	Mjukt eID (eller annat liknande cert utdelat under motsvarande säkerhet som eID). För denna nivå krävs kombination med "något jag VET".	Något jag HAR
SBKAnvLosenStarktIDKoll	3600	Användarnamn och starkt lösenord enligt underliggande nivå men dessutom utlämning med id-koll	Något jag VET
SBKAnvLosenStarkt	3300	Användarnamn och starkt lösenord (dvs i stil med minimum 8 pos, minst en versal, minst en gemen, minst en siffra, minst ett specialtecken)	Något jag VET
SBKAnvLosenSvagt	3000	Användarnamn och svagt lösenord	Något jag VET
SBKAnvPIN6	2500	Användaramn och 6 pos PIN	Något jag VET
SBKAnvPIN8	2000	Användaramn och 4 pos PIN	Något jag VET
SBKAnonym	0100	Användaren har identifierat sig men identiteten är inte bekräftad genom eID, manuell kontroll av id-kort etc utan är endast ett "anonymt" värde. Identiteten är dock användbar för att användaren ska kunna återkomma och identifiera sig på nytt, t.ex för att skriva bloggkommentarer. Exempelvis kan en icke-kontrollerad mailadress som initialt angivits av användaren senare användas tillsammans med svagt lösen.	Något jag VET
SBKIngaInloggnKrav	0000	Öppen info, ingen inloggning alls krävs	Ingen

I en nära framtid tänker jag mig alltså att två nivåer kunde bli extra vanliga för informationens krav på medborgarnas inloggningssäkerhet: 4000, vilket motsvarar vanligt eID och 3300, som motsvarar en användning av FacebookConnect eller deras konkurrenter (på det sätt som jag beskrivit ovan).

Nummerserien ovan har ”hål” så att det ska gå att infoga fler nivåer när nya tekniker som vi inte vet om idag utvecklas.

Se även anknytande trendspaningar som publicerats i ämnet, som Betrodda identitetsplattformar federeras fram och Det är aldrig för sent att ändra sig – som tur är.

Sven-Håkan Olsson är en fristående konsult som särskilt arbetar med att kombinera verksamhetsnytta med teknikhöjd. Han har en lång karriär sedan 70-talet som it-konsult (it-arkitektur, systemdesign, programmering, reviewer, utredningar, kursledning). Sven-Håkan är också medgrundare av Know IT och var dess teknikchef 1990-2003. Han utsågs till en av "Sveriges topputvecklare" av Computer Sweden 2008.

Sven-Håkan håller regelbundet kurser åt Dataföreningen Kompetens, till exempel ”Cloud Computing integration och migration”. Läs gärna mer på hans blogg www.definitivus.se.

Sven-Håkan Olsson