Säker identitetshantering på internet
Secure identity management online

Att minimera bedrägerier och öka konsumentens säkerhet och inflytande vid e-handel

Minimizing fraud and improving consumer security and influence in e-commerce

MATHIAS ÅKERBERG
ANDERS TIBBLING

Examensarbete inom
Datateknik,
Grundnivå, 15 hp
Handledare på KTH: Anders Lindström
Examinator: Ibrahim Orhan
TRITA-STH 2015: 2015:026

KTH
Skolan för Teknik och Hälsa
136 40 Handen, Sverige

Sammanfattning

Risken att en obehörig part kan komma över och använda en enskild konsuments identitetshandlingar är stor, samtidigt som individens möjlighet att kontrollera hur och när dess identitet används är liten. Problemformuleringen som skulle besvaras var hur identitetsstölder och bedrägerier på internet kunde minimeras samtidigt som konsumenten får ett ökat inflytande över hanteringen av sin identitet.

Målsättningen var att centralisera och skapa ett gemensamt förhållningssätt för identitetshantering på internet till förmån för konsumenterna, och på så vis minimera spridning av egna lösningar för identitetshantering hos enskilda aktörer.

Lösningen resulterade i en systemmodell med förutsättningar för att autentisera konsumenten, hantera filter för hur enskilda identitetshandlingar får användas på internet, samt för att möjliggöra kommunikation med konsumenten genom att skicka notifikationer om händelser som uppstått kopplat till en specifik identitet. Genom en användarportal skulle konsumenten kunna administrera sina filter för olika e-tjänster och webbutiker samt få en överblick över specifika händelser som inträffat.

En prototyp togs fram för att demonstrera systemmodellens grundläggande funktionalitet i praktiken. Denna kom att innefatta funktionalitet för att autentisera konsumenten, skicka notifikationer om händelser och kontrollera existerande filter för en specifik identitet. Prototypen kom att bestå av ett förenklat system enligt den modell som tagits fram, med ett tillhörande API samt två modeller motsvarande en webbutik och en betalningsväxel som skulle nyttja funktionaliteten genom att anropa systemets API.

Lösningen utvärderades baserat på det uppnådda resultatet från intervjuer med experter inom problemområdet och genomförd funktionskontroll av den framtagna prototypen. Genom utvärderingen kunde slutsatsen dras att identitetsbaserade bedrägerier med stor sannolikhet skulle sjunka drastiskt och att den enskilde konsumentens inflytande och medvetenhet skulle stärkas. Den största bidragande faktorn till slutsatsen ansågs främst vara det konsistenta och standardiserade sätt som skapats för autentisering av och kommunikation med konsumenten. På så vis skulle aktörerna själva avsätta delar av den funktionalitet och de säkerhetsrisker som ansågs finnas i anslutning till hanteringen av identiteter på internet.

Svårigheterna med den föreslagna lösningen ansågs vara att få konsumenter, webbutiker och betalningsväxlar att ansluta sig till ett centralt system då man av affärsmässiga skäl väljer att behålla särskilda delar internt.

Nyckelord

Internetbetalningar, e-handel, konsumentsäkerhet, identitetsstölder, bedrägerier.

Abstract

There's a high risk that an unauthorized party can gain access to and use a consumer's identity. This while the ability to control how and when a personal identity is used is small. The question to be answered were regarding how identity theft and online fraud could be minimized and give the consumers a greater influence and more control over the management of their identity online.

The goal was to centralize and establish a common approach for identity management online, with greater benefits for consumers. Through central service individual consumers would be able to set conditions for which online shops and services would be able to access their identities and grant access in each specific transaction. This would remove the need for non-central control of identities and as a result remove the need for independent storage of identity information.

The solution would result in a system model with the potential to authenticate the consumer, managing conditions for how individual identity documents may be used online and to provide the consumer with a online history by sending notifications of events that has occurred with regard to a specific identity.

A prototype was developed to demonstrate the basic functionality in practice. This included the functionality to authenticate the consumer with Mobile BankID, send notifications about events and check existing conditions regarding a specific identity. This prototype came to consist of a simplified system according to the model developed, an associated API, and two models representing an online store and a payment provider that would utilize the functionality of the system by calling the API.

The proposed solution was evaluated through two interviews with experts in the fields of IT Security and e-commerce. The conclusion was that identity fraud would probably drop drastically and the individual consumer influence and awareness would be fortified. The main reason for this was considered to be primarily through the consistent and standardized way for authentication of and communication with the consumer. This would remove the individual risk for online services.

The challenge with this proposed solution is believed to be getting consumers, online retailers and payment providers to accept a central solution instead of relying on internally developed and disconnected solution.

Keywords
Online payments, e-commerce, consumer security, identity thefts, frauds.

Förord

Den här rapporten avhandlar ett examensarbete som genomfördes på högskoleingenjörsprogrammet inom datateknik på Kungliga Tekniska Högskolan vårterminen 2015. Arbetet utfördes på betalningsföretaget Payer Financial Services AB och pågick från slutet av mars till och med början av juni.

Det här avsnittet tillägnas de personer som på något sätt inkluderats i det arbete som genomförts.

Ett stort tack till alla medarbetare på Payer Financial Services AB för visat tålamod och engagemang: Peder Berge (VD), Nick Elman (Marknadschef) och Inger Bergqvist (CSO).

Vi vill även tacka Björn Melinder, hjärnan bakom musiktjänsten Soundtrap, för att vi fick en möjlighet att inhämta underlag till vår utvärdering genom dig.

Dessutom vill vi rikta uppmärksamheten och tillägna ett särskilt tack till tre personer som involverats extra mycket i arbetet:

- **Björn Ihlar**: för sina kloka tips och råd samt förmåga att ständigt se nya infallsvinklar och lösningar.
- **Markus Jansson**: för sitt totala uppslukande engagemang från arbetets början till slut.
- **Anders Lindström**: vår handledare, som med sitt tålamod, sina kloka invändningar och sin känsla för struktur har varit vår ledfyr genom denna process.

Ordlista

API	Application Programming Interface, även kallat API, är ett förbestämt och ordnat sätt för applikationer att kommunicera med ett specifikt system eller mjukvara.
Betalningsväxel	Det företag som en webbutik använder för att ta betalt av sina kunder. En betalningsväxel, även kallad PSP (Payment Service Provider), agerar mellanhand mellan kund och bank.
HTTP	Hypertext Transfer Protocol är ett protokoll för att kommunicera mellan klient och server genom webbläsaren. Genom MIME-meddelanden kan specifik data efterfrågas som exempelvis en webbsida.
Token	En unik nyckel som kan användas för att binda en användare eller händelse till en specifik session.

Innehållsförteckning

1 Inledning 1
1.1 Problemformulering 1
1.2 Målsättning 2
1.2.1 Förstudie 2
1.2.2 Utformning av systemmodell 2
1.2.3 Utformning av prototyp 2
1.2.4 Funktionskontroll av prototyp 2
1.2.5 Utlåtanden kring systemmodell 2
1.2.6 Utvärdering 3
1.3 Avgränsningar 3
2 Teori och bakgrund 5
2.1 Bakgrund 5
2.2 Befintliga konsumentskydd 5
2.2.1 Allmänna konsumentskydd 6
2.2.2 Konsumentskydd vid e-handel 6
2.3 Begränsningar och hot 7
2.3.1 Begränsningar 7
2.3.2 Hot 8
2.4 Betalningsflödet och betalningsväxlar 8
2.4.1 Befintliga betalningsväxlar 8
2.4.2 Genomgång av betalningsflödet 8
2.5 Lagra och hantera personuppgifter 9
2.5.1 Personuppgiftslagen (PUL) 9
2.5.2 Skydd och säkerhet 10
2.6 Att fastställa identiteter 10
2.7 Säkerhetsaspekter i webbapplikationer 11
3 Metoder och resultat 13
3.1 Förstudie 13
3.1.1 Mål 13
3.1.2 Resultat 13

3.2 Utformning av systemmodell 16
3.2.1 Mål 16
3.2.2 Resultat 16
3.3 Utformning av prototyp 20
3.3.1 Mål 20
3.3.2 Resultat 20
3.4 Funktionskontroll av prototyp 23
3.4.1 Mål 23
3.4.2 Resultat 23
3.5 Utlåtanden kring systemmodell 24
3.5.1 Mål 24
3.5.2 Resultat 24
4 Analys och diskussion 27
4.1 Slutgiltig systemutformning 27
4.1.1 Autentisering 27
4.1.2 Kommunikation och öppenhet 27
4.1.3 Funktioner 28
4.2 Konsumentperspektiv 28
4.2.1 Användarportal 28
4.2.2 Filter 28
4.2.3 Notifikationer 29
4.2.4 Tillämpning och beteende 29
4.3 Säkerhet och riskanalys 29
4.3.1 Länkarna i autentiseringskedjan 29
4.3.2 Säkerhet i applikationen 30
4.4 Samhällsnytta 31
4.4.1 Nytta för konsumenter och privatpersoner 31
4.4.2 Branschmässiga perspektiv 31
4.4.3 Etiska aspekter 32
4.4.4 Sociala och ekonomiska aspekter 32
4.4.5 Miljö- och arbetsmiljöaspekter 33
5 Slutsatser 35

Källförteckning 37
Bilagor.....39

1 Inledning

Det här kapitlet beskriver utgångspunkten för den studie och problemlösning som har genomförts. Arbetet utfördes på betalningsföretaget Payer Financial Services AB i Stockholm.

Inledningsvis presenteras problemformuleringen kring hur känslig konsumentdata behandlas vid e-handel samt den befintliga omfattningen av individens kontroll och inflytande över dess spridning och hantering, följt av målsättningar och avgränsningar.

1.1 Problemformulering

Enligt den årliga "E-barometern" från HUI Research [1] når e-handeln i Sverige ständigt nya toppnoteringar samtidigt som identitetsstölder och bedrägerier på internet ökar. Alternativen för betalning på internet blir allt fler, och dessa förlitar sig på egna bakomliggande system för att säkerställa betalningar. Gemensamt för dessa system är att de strävar efter att göra inköp och betalningar så enkla som möjligt. Nackdelen med detta är att säkerheten ofta ses som ett hinder för en snabb och kundvänlig betalning och att balansen mellan "smidig lösning" och "säker lösning" inte är optimal varken som användare eller ur ett konverteringsperspektiv.

Då inköp och handel på internet inte kräver en fysisk närvaro är det mycket lätt att utge sig för att vara någon annan. En identitet kontrolleras mycket sällan av webbutiker, tjänster eller betalningsmottagare. I många fall är det enda som behövs för att genomföra en betalning i en webbutik ett personnummer eller annan likvärdig identitetsinformation. Då informationen i de flesta fall finns tillgänglig för allmänheten är risken stor att en obehörig part kan komma över och använda denna, samtidigt som den enskilda konsumentens möjlighet att kontrollera hur och när dess identitet används är liten.

Det finns i nuläget inget lätt sätt för konsumenten att på ett centraliserat sätt kontrollera, övervaka och godkänna användandet av dennes identitetsuppgifter på internet. Att spärra sin identitet för fakturaköp eller lån måste i nuläget ske multipelt, både hos kreditupplysningstjänster och enskilda betalningsföretag. Parterna erbjuder enbart en fullständig spärr för alla medverkande butiker och betalningsmottagare, samtidigt som en spärr av identitet ofta kan ske först efter att ett bedrägeri har skett.

Några problem att beakta vid design av ett säkert system är:

- Identiteter är i nuläget svåra att bekräfta på internet
- Identiteter är lätta att stjäla och använda
- En person blir aldrig uppmärksammad på att dennes identitet har använts
- Webbutiker förlitar sig i nuläget på sin betalningsväxel för säkerhet
- En spärrtjänst bör inte vara på konsumentens bekostnad.

1.2 Målsättning

Målsättningen med denna rapport var att utreda vad som krävs för att tillhandahålla en lösning vid e-handel som:

- Ökar konsumentens kontroll och insyn vid hantering av identitetsuppgifter
- Ger konsumenter möjligheten att reglera hur deras identitet kan användas och av vem
- Ger internettjänster ett centralt system för att underlätta säkerhet och kundhantering
- Minimerar möjligheter till identitetsstölder och bedrägerier vid e-handel
- Kan implementeras i redan etablerade e-handels- och betalsystem utan att påverka befintliga flöden.

Denna utredning skulle komma att resultera i en teoretisk systemmodell samt en prototyp som påvisade att denna gick att tillämpa i praktiken.

1.2.1 Förstudie

Initialt genomfördes en utredning för att inhämta underlag till utformningen av den påtänkta lösningen. Relevanta frågor som skulle undersökas var exempelvis brister i de redan existerande lösningarna, krav för ökat konsumentinflytande, befintlig identifieringsteknik samt hur lösningen görs attraktiv och på ett enkelt sätt kan integreras i redan befintliga system och flöden.

1.2.2 Utformning av systemmodell

Baserat på underlaget som inhämtats genom den utförda förstudien skulle en systemmodell tas fram med funktionalitet för att besvara de angivna målsättningarna i Avsnitt 1.2.

1.2.3 Utformning av prototyp

En förenklad prototyp togs fram med syftet att demonstrera systemmodellen i praktiken. Ett system med ett tillhörande API samt två förenklade modeller av en webbutik och en betalningsväxel implementerades för att påvisa detta. Prototypen skulle senare komma att ligga till grund för den tilltänkta utvärderingen av lösningen.

1.2.4 Funktionskontroll av prototyp

Baserat på den implementerade prototypen av systemmodellen genomfördes en funktionskontroll av prototypen. Genom denna skulle funktionaliteterna verifieras enligt de målsättningar som angivits för systemmodellen samt inhämta underlag för en senare slutgiltig utvärdering av lösningen.

1.2.5 Utlåtanden kring systemmodell

För att inhämta ytterligare underlag för den slutgiltiga utvärderingen behövde tekniskt kunniga inom problemområdet intervjuas för att verifiera systemmodellens funktioner och målsättningar. Genom dessa intervjuer skulle underlag inhämtas för att verifiera:

- Säkerhetsrisker vid e-handel
- Konsumentens inflytande och kontroll över betalningsflöden
- Säkerhet vid identitetshantering på internet
- Den föreslagna lösningens gångbarhet jämfört med redan befintliga lösningar inom problemområdet
- Tillvägagångssätten för att få genomslag på marknaden

1.2.6 Utvärdering

En slutgiltig utvärdering av den föreslagna systemmodellen genomfördes baserat på det underlag som inhämtats genom intervjuer med experter inom problemområdet och utförd funktionskontroll av framtagen prototyp. Utvärderingen genomfördes med hänsyn tagen till de givna målsättningarna i Avsnitt 3.2.

1.3 Avgränsningar

Prototypen skulle fokusera på betalningstransaktioner och hantering av identiteter vid e-handel. Övrigt potentiellt nyttjande av lösningen, inom områden för exempelvis kreditupplysning och adressändring, implementerades ej i prototypen.

En möjlighet för slutanvändaren att genom en användarportal kunna hantera filter samt få en översikt över händelser som inträffat kopplat till sin identitet inkluderades inte i prototypen.

De säkerhetskrav som ställdes på ett verktyg av detta slag ansågs viktiga men så pass omfattande att dess fullständiga utredning inte kunde inkluderas i denna rapport. En kortare redovisning av de vanligaste säkerhetshoten inkluderades dock tillsammans med föreslagna åtgärder. Denna redovisning ansågs kunna ligga till grund för en fullständig utvärdering av de säkerhetsrisker systemet måste ta ställning till och de åtgärder dessa i så fall krävde.

Även en marknadsundersökning med fokus på konsumenternas och webbutikernas intressen och behov ansågs nödvändigt för den slutgiltiga implementationen. En sådan undersökning befann sig dock utanför de tekniska aspekterna kring systemmodellen denna rapport avhandlar.

2 Teori och bakgrund

Inledningsvis beskrivs den befintliga marknaden och den problematik som fanns kopplat till den givna problemformuleringen gällande ökad konsumentsäkerhet på internet. Därefter följer en omvärldsanalys där den befintliga marknaden inom problemområdet undersöks. Intressanta områden för analysen innefattar bland annat en överblick över befintliga konsumentskydd vid e-handel, säkerhetsaspekter kring dessa samt eventuella begränsningar.

Dessutom nämns befintliga betalningsväxlar, vilka vid tidpunkten ansågs vara de största aktörerna på marknaden, samt en genomgång av det generella betalningsflödet.

Avslutningsvis introduceras riktlinjer för personuppgiftshantering, exempel på populära tekniker för autentisering på internet samt säkerhetsaspekter för webbapplikationer i anslutning till problemområdet.

2.1 Bakgrund

I Sverige blir betalningsalternativen och betalningsväxlarna för e-handel allt fler. Samtidigt ökar det enskilda intresset hos företagen för att vidare lagra information om sina kunder.

Hos betalningsväxlarna utformas och hanteras betalningstransaktionerna i sin tur på ett sådant sätt som är bäst lämpat efter betalningsväxlarnas givna förutsättningar. De olika delmomenten i transaktionsflödet kan komma att innebära kommunikation med ytterligare parter för exempelvis autentisering, tillståndskontroller och kreditupplysningar. Hur denna uppdelning sker kan variera då vissa betalningsväxlar istället försöker behålla så många delar av flödet som möjligt internt. Vilken metod som används beror oftast på ekonomiska faktorer eller att flödet medvetet utformats på ett sådant sätt som bäst gynnar affärsutvecklingen. Genom att analysera insamlad och lagrad kunddata kan organisationsprocesser och framtida resultat effektiviseras.

Ett exempel på detta är betaltjänsten *Klarna,* som har växt till att bli en av landets ledande och största betalningsväxlar, vilken lagrar information om de kunder som nyttjar deras tjänster [2]. Informationen används exempelvis för analys inom områden för affärsutveckling och användarinteraktion, i samverkan med externa partners och aktörer eller i kommersiella och marknadsföringsmässiga syften.

Enligt kreditföretaget EasyCredit [3] har antalet bedrägerier och identitetsstölder på internet årligen ökat, vilket skulle kunna kopplas till den informationsspridning som sker genom olika tjänster på internet. Konsumentens nyttjande av olika e-tjänster kan leda till att ID-handlingar kommer i orätta händer och används på oönskade sätt.

2.2 Befintliga konsumentskydd

Till viss del tillhandahålls idag tjänster för att skydda individens identitet på internet och öka kontrollen över vad som är tillåtet att göra med denna. I dessa redan etablerade tjänster finns försök till att lösa olika delar i problematiken kring behandlingen av individens identitet.

2.2.1 Allmänna konsumentskydd

I takt med att antalet identitetsstölder och bedrägerier ökar växer allt fler verktyg fram i hopp om att minimera dessa. Verktygen i sig riktar sig till att värna om individens integritet genom att exempelvis notifiera om händelser som inträffat kopplat till dennes identitet eller att erbjuda kompensation till konsumenter som utsatts för bedrägeri.

Reaktiva konsumentförsäkringar

Att i efterhand erbjuda konsumenter upprättelse och ersättning vid bedrägeri är beroende av vilken betaltjänst, betalningsmetod och webbutik som använts. Flertalet betalningsväxlar erbjuder bedrägeriskydd som försäkrar webbutiker ersättning om tveksamma betalningar gått igenom. Dessa träder dock i kraft efter att ett bedrägeri redan utförts.

UC ID-Skydd

UC ID-Skydd är en tjänst från UpplysningsCentralen (UC). För en månadskostnad får konsumenten ett enkelt skydd över sina offentliga uppgifter. Genom SMS eller e-post notifieras konsumenten vid en händelse som skulle kunna innebära en ID-kapning. Exempelvis vid en adressändring, om en kreditupplysning skett eller om någon försökt ansöka om lån i dennes namn.

UC ID-Skydd meddelar alltså konsumenten efter att ett bedrägeri eller ett bedrägeriförsök har ägt rum och erbjuder sedan en rad tjänster för att minimera dess skadliga följder.

UC ägs av de sex storbankerna SEB, Swedbank, Nordea, Handelsbanken, Danske Bank och Länsförsäkringar [4].

KeyCode ID-Skydd

KeyCode är ytterligare ett identitetsskydd [5], i samverkan med Bisnode, som genom SMS eller e-post notifierar användaren om händelser som uppstått kopplat till dennes identitet. Funktionen är i sin utformning mycket lik ID-skyddet från UC.

Bedrägerispärr

En tjänst från UC som förhindrar att en kreditupplysning kan begäras ut på en person. För att kunna utnyttja bedrägerispärren krävs att ett bedrägeri har begåtts som i sin tur måste styrkas med en polisanmälan.

2.2.2 Konsumentskydd vid e-handel

Under detta avsnitt presenteras redan existerande verktyg som är koncentrerade till att hantera bedrägerier, specifikt kopplat till e-handel. Exempel på skydd kan vara ökat konsumentinflytande genom att kunna styra över vad ens identitet får användas till samt hur autentisering hanteras.

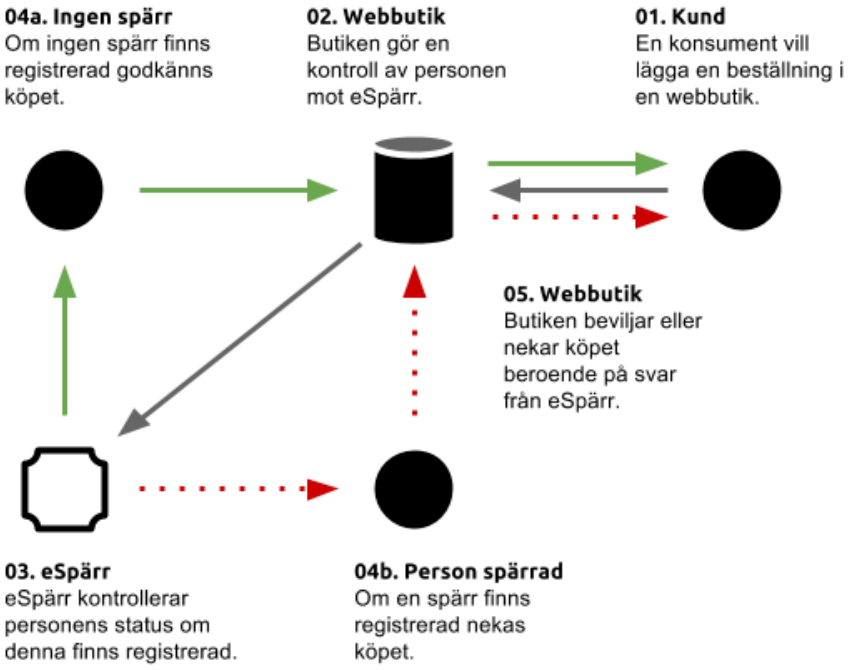
3DSecure

Vid betalning med kort finns från kortföretagets sida ytterligare säkerhetsåtgärder i form av personliga koder för autentisering som behöver anges i samband med ett onlineköp. Verified by Visa och MasterCard SecureCode är två av de vanligaste exemplen på dessa lösningar.

eSpärr

Även e-Spärr är en tjänst från UC, dess syfte [6] är att uppnå högre konsumentsäkerhet vid betalningar. Konsumenten kan genom denna tjänst skapa en begränsad profil som beskriver vilka webbutiker som har rättigheter att genomföra köp i individens namn. Webbutikerna kan i sin tur ansluta sig till eSpärr för ökad konsumentsäkerhet.

Innan en betalningstransaktion initieras hos en betalväxel, gör butiken först en förfrågan till tjänsten som returnerar ett svar om ett köp från denna butik är berättigat, se Figur 2.1.



Figur 2.1: Flödesbeskrivning av e-Spärr [6]

2.3 Begränsningar och hot

Trots en rad redan existerande konsumentskydd på internet ställs branschen ständigt inför nya utmaningar i området. Här presenteras förekommande begränsningar i de befintliga lösningarna inom problemområdet samt generella hot mot konsumenter på internet.

2.3.1 Begränsningar

Den övergripande problematiken kring existerande lösningar är bristen på ett öppet, centraliserat och heltäckande ramverk som sätter konsumenten främst, genom att kunna överblicka och kontrollera delar i flödet, och som samtidigt kan tillhandahålla de olika verktygen i en och samma plattform. Exempel på intressanta moment som kan hanteras är insamling av händelsehistorik (betalningar, kreditupplysningar, adressändringar med mera),

autentisering och behörighetshantering kopplat till en specifik e-identitet, oberoende av vilken e-tjänst som används.

2.3.2 Hot

Det enskilt största hotet mot konsumenter på internet idag är identitetsstölder. Personuppgifter är lätta att komma över då dessa är offentliga handlingar. En skyddad identitet är det närmaste man kan komma en spärrning av faktiska personuppgifter. En stulen ID-handling eller ett kastat brev med personuppgifter från en myndighet eller bank brukar nämnas som vanliga sätt för en bedragare att komma över en identitet.

En beställning i en webbutik kan sedan göras med dessa personuppgifter. Här finns det andra lagret av skydd i form av den kreditupplysning som görs i samband med fakturaköp. De tidigare nämnda tjänsterna (UC ID-skydd och eSpärr) kan blockera en kreditupplysning eller notifiera när en sådan gjorts. Kreditupplysningens huvuduppgift är dock att informera om huruvida en person kan tänkas fullfölja en betalning - inte att uppmärksamma betalningsmottagaren om att beställarens identitet används olovligen.

2.4 Betalningsflödet och betalningsväxlar

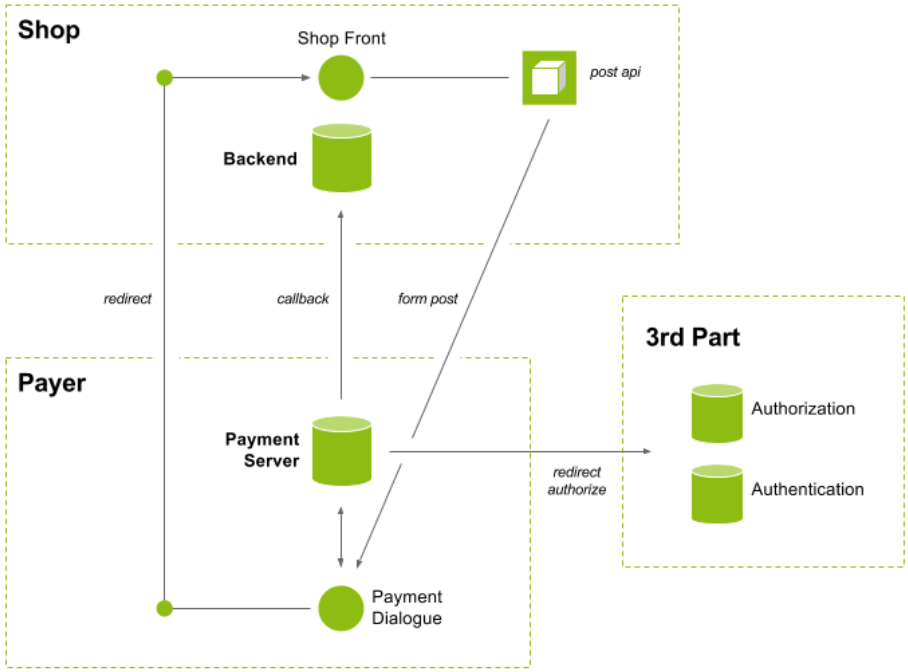
I det traditionella betalningsflödet ingår kommunikation mellan flera olika parter från att en betalning initierats tills dess att betalningen slutligen har genomförts. En av dessa parter representerar en betalningsväxel, vilken är transaktionens centrala punkt och agerar som en mellanhand mellan kund och bank.

2.4.1 Befintliga betalningsväxlar

Existerande aktörer på marknaden är exempelvis Klarna, DIBS Payment Services, PayPal, Paynova, PaySon och Payer, vilka stödjer betalningsalternativ som kort, delbetalning, faktura, mobil- och direktbanksbetalning.

2.4.2 Genomgång av betalningsflödet

Det generella flödet vid betalningar på internet är relativt komplext då det kan komma att innehålla kommunikation mellan flera olika parter innan det slutgiltiga köpet är genomfört. Hur betalningstransaktionerna hos enskilda betalningsväxlar utformas kan variera, men flödet och de inblandade komponenterna från att en första initiering skett till att alla delmoment i processkedjan genomförts kan i de flesta fall beskrivas enligt Figur 2.2.



Figur 2.2: En översikt av komponenterna som utgör betalningsflödet [7]

I det första skedet initierar konsumenten betalningen i webbutiken, vilken anropar betalningsväxelns API. Konsumenten omdirigeras till ett betalningsfönster hos betalningsväxeln där själva betalningstransaktionen initieras.

Transaktionen består oftast av ett flertal delmoment som ska hanteras, som exempelvis innefattar autentisering och tillståndshantering, innan själva betalningen mot den förutbestämda betalningsaktören påbörjas.

I slutskedet dirigeras konsumenten tillbaka till butiken där ordern uppdateras med betalningens slutgiltiga status och konsumenten upplyses om att ordern är betald och klar att levereras.

2.5 Lagra och hantera personuppgifter

Vid behandling av uppgifter kopplat till en individs identitet fanns en rad faktorer att ta hänsyn till. Exempelvis hur personuppgifter enligt lag får hanteras, lagras, spridas och tillgängliggöras samt hur säkerheten kring dessa kan garanteras.

2.5.1 Personuppgiftslagen (PUL)

Enligt PUL [8], utformad i samverkan med EU enligt det så kallade *dataskyddsdirektivet,* måste vissa riktlinjer följas vid behandlingen av känsliga personuppgifter för att på så vis motverka att den personliga integriteten kränks.

Vilka delar som berörs och dess omfattning kan variera beroende på hur informationen struktureras. Att lagra personuppgifter i en databas eller i ett register omfattas generellt av

fler skyldigheter och regler än om dessa nyttjas i mer lösa sammanhang (exempelvis i löpande texter eller i e-postmeddelanden).

Några viktiga riktlinjer för hantering av personuppgifter:

- Personuppgiftslagen gäller vid manuell hantering av personuppgifter som ingår i en strukturerad samling och vid automatiserad behandling
- Lagring av personuppgifter får ske i särskilda ändamål som är uttryckligt angivna och berättigade, det vill säga när uppgiftsägaren har lämnat sitt samtycke
- Personuppgiftsägaren ska informeras om att hans eller hennes uppgifter behandlas
- Personuppgifter ska inte lagras under en längre tid än vad som är avsatt för det specifika ändamålet.

2.5.2 Skydd och säkerhet

Att kunna säkerställa att känsliga uppgifter inte görs tillgängliga för obehöriga är en viktig säkerhetsaspekt att ta hänsyn till vid utformandet av e-tjänster. Enligt riktlinjer från Datainspektionen [9], för ökad säkerhet vid e-tjänster, kan det åstadkommas genom att:

- Fastställa identiteten hos användaren
- Säkerställa dataöverföringen genom kryptering
- Se till så att data hålls intakt och lagras på ett säkert sätt.

2.6 Att fastställa identiteter

Det finns en tydlig skillnad mellan ett fastställande av identitet och ett godkännande av transaktion, vilka är av högsta vikt för de tjänster och processer som denna rapport avhandlar.

Vid autentisering på internet tillhandahålls ett flertal olika verktyg och tillvägagångssätt. Vanliga metoder för att säkerställa identiteter kan åstadkommas i varierande grad genom exempelvis engångslösenord, ett användarnamn och lösenord eller e-legitimation [9]. Vilken teknik som används varierar med den säkerhet som ställs på tjänsten.

Vid internetbetalningar är det inte ett krav att fastställa identitet. De betaltjänster som nyttjar två- eller trepartsautentisering via lösenord och/eller externa applikationer godkänner oftast bara att en betalning genomförs, medan identiteten på den som godkänner betalningen fortfarande inte är säkerställd. Endast ett godkänt kort och eventuella extra säkerhetsåtgärd i form av till exempel 3DSecure, behövs för en kortbetalning. Vid beställning mot faktura finns ett behov av identitetsbekräftelse men detta är inget krav. Däremot finns en praxis i branschen om att fakturaadress och leveransadress bör stämma överens för att försvåra bedrägeri.

BankID

Enligt Finansiell ID-Teknik [10] var e-legitimationssystemet BankID under år 2014 Sveriges mest använda lösning för att bekräfta identitet, med över sex miljoner aktiva användare. Tekniken ägs av flera svenska storbanker och går att nyttja på tre olika sätt: BankID på fil,

BankID på kort och Mobilt BankID. Skillnaden mellan dessa tre ligger i plattformen på vilken de används. På fil i persondatorer, på fysiskt kort eller som en app i en smartphone.

Enligt en rapport från *Finansiell ID-Teknik BID AB*, vilka förvaltar BankID, finns en tydligt uppåtgående trend i användandet av BankID i takt med att internettransaktionerna ökar [10]. Intresset och användandet av Mobilt BankID fick en explosiv ökning under 2014, vilken nästintill har sexdubblat användandet sedan samma period året innan.

Genom Mobilt BankIDs applikation i mobiltelefonen verifierar slutanvändaren sin identitet genom att ange sin säkerhetskod i kombination med ett utfärdat certifikat. Certifikatet har i sin tur intygats genom en ansluten bank.

BankID är godkänd som legitimation på internet och godtas hos flera myndigheter som legitimation, bland annat av Skatteverket och Transportstyrelsen.

Telia e-legitimation

Telia e-legitimation [11] är ett e-legitimationssystem som funnits tillgängligt sedan tidigt 2000-tal, vars funktionalitet liknar BankID. Användning och implementation speglar lösningen för BankID och kontroll och program implementeras på samma sätt.

Till skillnad från BankID finns dock ingen lösning för mobiler eller surfplattor tillgänglig, inte heller är användarbasens omfattning i samma storleksklass då marknadsandelen 2012 enligt e-legitimationsnämnden [12] var nio procentenheter. Vid samma mätning hade BankID (som då innefattar Swedbank, Nordea och Handelsbanken) resterande marknad.

E-legitimationsnämnden

Sedan januari 2001 finns E-legitimationsnämnden i Sverige som bildades för att lyfta och utveckla teknik, riktlinjer och tillämpningar kring legitimering på internet. De har ännu inte någon tillgänglig lösning för e-legitimation men planerar att lansera detta tillsammans med sveriges storbanker under 2016 [13].

Egen säkerställning av identitet

Ett egenutvecklat system för identifiering skulle kräva identifiering av person via redan utgiven legitimation (till exempel ett körkort eller pass) som utnyttjas vid registrering av användare. En användare måste i detta fall alltså vid skapandet av ett konto styrka sin identitet som sedan översätts till en för systemet intern identitet.

2.7 Säkerhetsaspekter i webbapplikationer

I en sammanställning från OWASP (Open Web Application Security Project), en global organisation som arbetar aktivt för ökad säkerhet i applikationer, från år 2013 [14] nämns några av de mest kritiska säkerhetsriskerna att ta hänsyn till i implementeringen för att säkerställa att de vanligaste kryphålen undanröjs. Dessa motsvarar bland annat:

- **XSS (Cross-Site Scripting):** I en applikation kan brister i valideringen av otillförlitlig data utnyttjas och på så vis, utan klientens kännedom, lyckas göra skadliga eller otillåtna handlingar genom att manipulera kod i offrets webbläsare.

- **CSRF (Cross-Site Request Forgery):** En användares sessionsuppgifter utnyttjas av obehöriga, och kan på så vis utföra otillåtna handlingar genom att utge sig för att vara någon man inte är.
- **Injection:** Ingående data i en applikation innehåller information som av systemet tolkas som exempelvis ett kommando eller en databasfråga. På så vis kan användaren förstöra, manipulera eller ges obehörig åtkomst till information.
- **Sensitive Data Exposure:** Obehöriga får åtkomst till känslig data på grund av bristande kryptering.

3 Metoder och resultat

I det här avsnittet beskrivs den metodik samt de lösningsmetoder och modeller som användes som tillvägagångssätt i den föreslagna lösningen till den i Avsnitt 1.1 angivna problemformuleringen.

Initialt genomfördes en förstudie, en utredning inom ämnesområdet, som skulle komma att ligga till grund för utformningen av den systemmodell som representerar det föreslagna lösningförslaget till problemformuleringen. Detta lösningsförslag utgjorde sedan basen för den systemmodell och prototyp med tillhörande modeller som utformades för att bekräfta att målsättningarna i Avsnitt 1.2 hade uppnåtts.

3.1 Förstudie

Studien skulle ge en överblick av, och beslutsunderlag till, tillgängliga tekniker och lösningar. För att kunna göra en bedömning av vilka tekniker som bör ligga till grund för systemets utformning samt vad som redan fanns att inkludera utan egen utveckling.

3.1.1 Mål

Studiens huvudsakliga frågeställningar var:

- Vilka slutsatser kan dras i anslutning till de redan existerande lösningarna?
- Vad kan göras för att öka konsumenternas insyn och kontroll över sin identitet?
- Vilken teknik bör användas för identifiering?
- I vilka delar av tjänsters flöden kan lösningen implementeras?
- Hur bör systemet kommunicera med användare och externa system?
- Kan systemet utformas på ett långsiktigt användbart sätt, med minimerade beroenden av existerande teknik och betalningsflödenas utformning?
- Vilka funktioner kan göra systemet attraktivt för intressenter som exempelvis betalningsväxlar, kreditbolag med flera?

3.1.2 Resultat

Befintliga konsumentskydd

De befintliga tekniker som fanns för att öka konsumentens säkerhet och skydd varierade. De allmänna skydden syftade till att notifiera slutanvändaren om händelser som uppstått kopplat till dennes identitet samt tillhandahålla konsumentförsäkringar som vid bedrägerier möjliggör kompensation av förlorat belopp.

De skydd som var specifikt kopplade till e-handel och som var relevanta för just e-handel var tredjepartslösningar som användes av antingen webbutiken själv eller i betalningsflödet hos betalningsväxeln, för exempelvis autentisering eller tillståndskontroller kopplat till en specifik identitet.

Tjänsten e-Spärr som webbutikerna kunde integrera för utökad säkerhet redan på butikssidan, innan slutanvändaren slussas vidare till vald betalningsväxel, ansågs relevant för lös-

ningen. Specifikt genom att låta slutanvändaren styra över hur ens identitets används. Genom tjänsten kan webbutiken göra slagningar mot en extern databas och fråga om en specifik handling är tillåten att göra. Utformningen ansågs även uppfylla de skalbarhetskrav som ställdes på systemet, vilket gjorde det enkelt att implementera i redan befintliga flöden.

Även funktionaliteten i de befintliga ID-skydden var av intresse då notifieringen om uppstådda händelser ansågs högst relevant för att bidra till konsumentens ökade inflytande och kontroll över sin identitet.

Problematiken som ansågs finnas med de redan befintliga konsumentskydden var egentligen inte skydden som sådana, utan snarare de enskilda utformningarna av dessa. Med andra ord skulle ett gemensamt och centralt system istället vara att föredra då det skulle öka möjligheterna för att hanteringen av identitetsuppgifter då sker på ett konsistent och kontrollerat sätt.

Att många av de befintliga konsumentskydden dessutom inte är kostnadsfria att använda försvårar även möjligheterna ytterligare med att nå ut till den stora skaran med skyddet. Syftet verkar i dessa fall främst vara att generera intäkter än att bidra med ett hållbart och standardiserat konsumentskydd.

Konsumentfördelar

För att utöka skyddet kring identiteter på internet bör hanterandet av dessa göras synligt för konsumenten genom att skapa en möjlighet att se vad som har gjorts, när detta genomförts och av vem (vilken tjänst eller webbutik). En överblick av detta gör det lättare för konsumenten att avgöra om någonting felaktigt har skett kopplat till sin identitet. En notifikation per SMS eller e-post kan även vara intressant för att direkt påkalla konsumentens uppmärksamhet när identiteten har använts, och kan på så vis vidta åtgärder för utökat skydd.

I nuläget finns möjligheten att spärra (genom ett filter) identiteten på internet via tidigare i rapporten nämnda tjänster. En sådan spärr är ofta reaktiv, och om det är möjligheten till kreditupplysning som spärrats gäller den samtliga eventuella förfrågningar. Denna spärrning bör istället göras proaktiv. Genom att konsumenten själv ges möjligheten till att godkänna en förfrågan ökar säkerheten drastiskt. Konsumentens identitet blir skyddad men tillgänglig vid behov; istället för totalt spärrad.

Likt det proaktiva godkännandet av kreditupplysning vid fakturaköp kan andra betalsätt eller helt skilda tjänster godkännas på ett liknande sätt. Detta flyttar ansvaret för hanteringen, godkännandet och genomförandet av handlingar som använder en konsuments identitet, eller som kan tänkas öka säkerhet genom en autentisering till den tilltänkta konsumenten/användaren, istället för att vila på webbutiken eller internettjänsten.

Att säkerställa en identitet

För att säkerställa en identitet måste systemet lita på ett tidigare fastställande. Att vid registrering fysiskt legitimera kräver resurser som inte är önskvärda för varken systemets drift eller för slutanvändaren. Istället måste ett alternativ till egen registrering användas.

Verktyg för autentisering

Då den mest använda och utbredda tjänsten för identitetsbekräftande för närvarande är BankID, som innefattar Mobilt BankID, finns få anledningar att utveckla ett eget system och en egen infrastruktur för detta. Alternativ till BankID finns men är antingen inte aktuella ännu eller har inte samma marknadsandel. Genom att utnyttja denna redan etablerade standard undviks även den svagaste delen i förtroendeetableringen, den inledande processen med utfärdande av identitetshandling. På samma vis undviker tjänsten att belasta slutanvändaren med ytterligare en enskild inloggning och de säkerhetsrisker detta medför. Eftersom BankID även sörjer för sin egen säkerhet, då detta är dess huvudpunkt, kommer framtida stärkningar i denna säkerhet inkluderas i en eventuell lösning utan extra utveckling.

Betalningsflödens utformning, skalbarhet och implementation

Vilka delar som ingår i betalsystemets flöde kan variera beroende på omfattningen av de tjänster som tillhandahålls. Eftersom utvecklingen ständigt går framåt, och nya hjälpmedel och verktyg kommer till, kan särskilda delar över tid behöva bytas ut till förmån för ökad prestanda eller för att tillgodose ytterligare intressen och behov.

För att möjliggöra och förenkla underhållsarbetet i komplexa betalsystem, ställs höga krav på skalbarhet. För att uppnå detta bör kommunikation och integrering med externa system enbart hanteras som ett extra anrop i transaktionen, som i sig själv inte påverkar övriga delar i betalningsflödet.

Genom att de redan tillgängliga lösningarna skräddarsyr och sprider ut integritetsskydden för enskilda tjänster och ändamål skapas en avsaknad av ett konsistent och gemensamt förhållningssätt. Ur säkerhetssynpunkt blir detta på bekostnad av konsumentens kontroll och integritet då ansvaret för vidare behandling lämnas över till den frågande parten (betalningsväxel, webbutik eller annan e-tjänst). Ur ett konsumentperspektiv blir det på så vis svårare att garantera den fortsatta säkerheten, varför en centralisering av identitetshanteringen ansågs vara nödvändig. Det möjliggör behandling av identiteter på ett och samma ställe, vilket skapar förutsättningar för individer att kunna kontrollera händelser, flöden och transaktioners status.

Med en centralisering skulle behandling av identiteter samt integritetsskydd, som exempelvis filter för att spärra enskilda webbutiker från att utföra köp, förflyttas till en central punkt. I betalningstransaktioner görs då externa förfrågningar till denna centrala punkt för att exempelvis säkerställa identiteten genom BankID, få tillgång till personuppgifter efter att identiteten har säkerställts, kontrollera filter för en specifik identitet med mera.

En långsiktig utformning

Att göra det möjligt att implementera skilda lösningar för att styrka sin identitet skulle göra systemet lämpat även för andra marknader eller för tjänster där högsta säkerhet inte är av lika stor vikt. I Sverige är BankID den dominerande lösningen medan exempelvis Norge har ett snarlikt system. Då en anpassning av systemet enbart behöver ske vid funktionaliteten för autentisering är systemet för detta tämligen flexibelt. Systemets användning av olika autentiseringstyper är osynligt för de tjänster som utnyttjar det; då ingången mot systemet är densamma.

Ytterligare framtida flexibilitet ansågs ligga i de förutsättningar som skapas för att på sikt helt kunna införa och nyttja personliga tokens istället för personnummer när en identitet används på internet. En sådan lösning skulle helt kunna avveckla det direkta användandet av exempelvis ett personnummer i en webbutik och låta användaren vara anonym men samtidigt med pålitlig identitet.

Att göra lösningen attraktiv

För att få användandet av systemet att komma igång och ge konsumenter, webbutiker och betalningsväxlar en anledning att ansluta sig behöver det erbjuda ett mervärde. Konsumenternas huvudanledning till att använda systemet är säkerheten, någonting som webbutikerna måste vara anslutna till för att kunna erbjuda. För webbutikerna är möjligheten att helt eliminera bedrägerier av identitetsstöldskaraktär den stora punkten. För betalningsväxlarna kommer säkerheten på köpet om både konsumenter och webbutiker redan är anslutna då autentisering och filterkontroller redan gjorts. Betalningsväxlarna kan dock kontrollera att identiteten för transaktionen har säkerställts, vilket för betalningsväxeln kan användas som beslutsunderlag för handlingar, exempelvis som en rutinkontroll innan köpet slutligen genomförs.

För webbutikerna kan ytterligare mervärde skapas genom att erbjuda funktionalitet som förenklar identitetshanteringen. Exempelvis kan ett objekt innehållande personuppgifter returneras för den identitet som säkerställts. På så vis minimeras antalet manuella steg som konsumenten måste ta sig igenom innan köpet kan genomföras, vilket kan bidra till ökad konvertering. Ytterligare skulle konsumenten kunna ha olika sparade profiler, exempelvis skilda leveransadresser, i detta centrala system. Dessa skulle kunna väljas vid autentiseringstillfället för att skapa utökad flexibilitet för konsumenten. De vanliga riskerna vid skilda leverans- och betaladresser, till exempel att det inte är den som betalar fakturan som får leveransen, är vid detta förfarande eliminerat då betalaren redan har styrkt sin identitet.

3.2 Utformning av systemmodell

En teoretisk modell för systemet skulle tas fram med underlag baserat i resultatet från förstudien och som skulle uppfylla de krav som presenterades i problemformuleringen i Avsnitt 1.1.

3.2.1 Mål

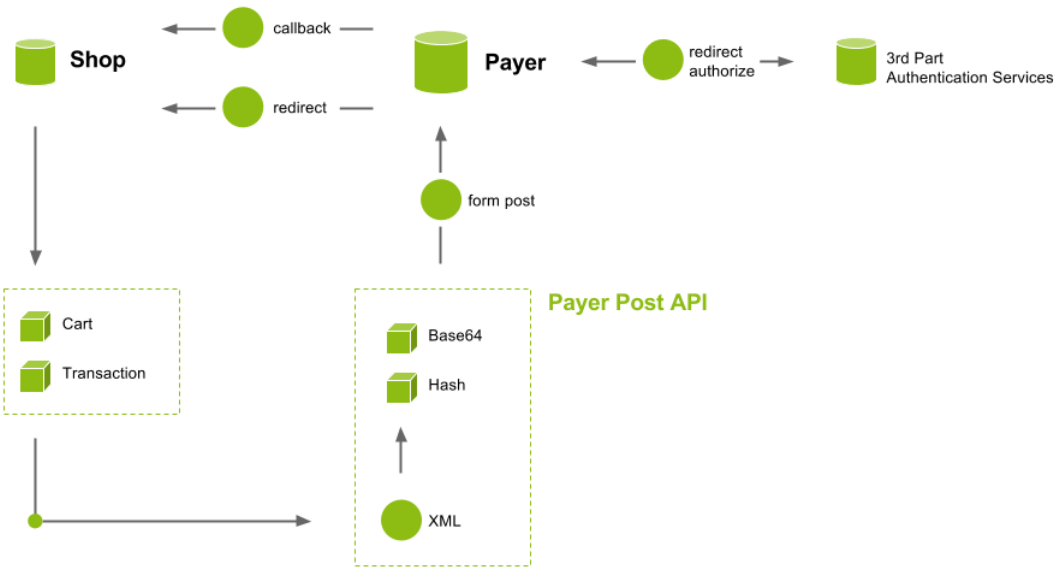
Utformningen ska vara så utförlig som möjligt för att kunna ligga till grund för en prototyp som implementerade delar av modellen. Enbart den funktionella utformningen hanteras i modellen, inte säkerhet och andra eventuella punkter utanför det funktionella området.

Resultatet presenteras som en systemöversikt med beskrivningar och illustrationer av utformning, redovisning av flöden och beskrivning av systemets interaktionspunkter och kommunikationskanaler.

3.2.2 Resultat

För att lösningen skulle fungera med redan existerande betalningsväxlar behövde den på ett enkelt sätt kunna nyttjas av system utan att påverka befintliga flöden. Nyttjandet av lösningen skulle endast komma att hanteras som ett extra anrop i det enskilda flödet, och skulle på så vis erhålla låga kopplingar och undvika direkta beroenden.

I Figur 3.1 visas flödet av Payers betalningssystem vilket omfattar den grundläggande kommunikationen mellan Payer och webbutiken. Figuren påvisar det typiska upplägget, vilket denna rapport refererar till som *betalningsflöde*. I en fullständig redovisning av betalningsflödet tillkommer ytterligare kommunikation med nödvändiga tredje-parter för att kunna genomföra hela betalningstransaktionen.



Figur 3.1: En översikt över Payers betalningsflöde [7]

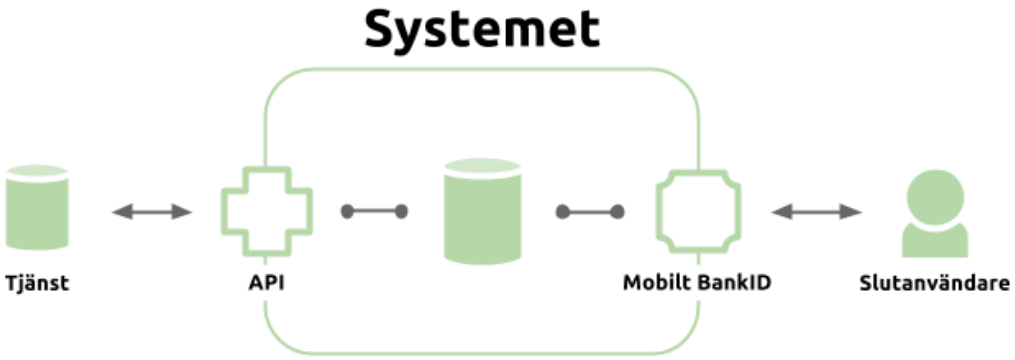
Då de skilda parterna (Payer och webbutiken) är fristående och ses som enskilda delar i transaktionen kan dessa på egen hand utföra ett obestämt antal arbeten transparent. Det slutgiltiga resultatet förväntas ändå bli detsamma. På så vis kan ytterligare arbeten läggas till eller tas bort i de enskilda delarna i flödet.

Lösningen som föreslogs består i sitt enklaste utförande av ett centralt system som genom ett gemensamt API kan hantera anrop från registrerade tjänster som exempelvis webbutiker, betalningsväxlar eller kreditupplysningar.

Systemmodellen skulle komma att innehålla funktionalitet för att:

- Initiera autentisering av slutanvändaren genom BankID.
- Lagra och hantera personuppgifter.
- Reglera filter för hur en specifik identitet får användas på internet.
- Kontrollera filter kopplat till en identitet.
- Kontrollera att en identitet har säkerställts.
- Låta externa tjänster skicka notifikationer till systemet.

Den slutgiltiga lösningen presenteras i Figur 3.2.



Figur 3.2: Systemets grundutförande

Autentisering

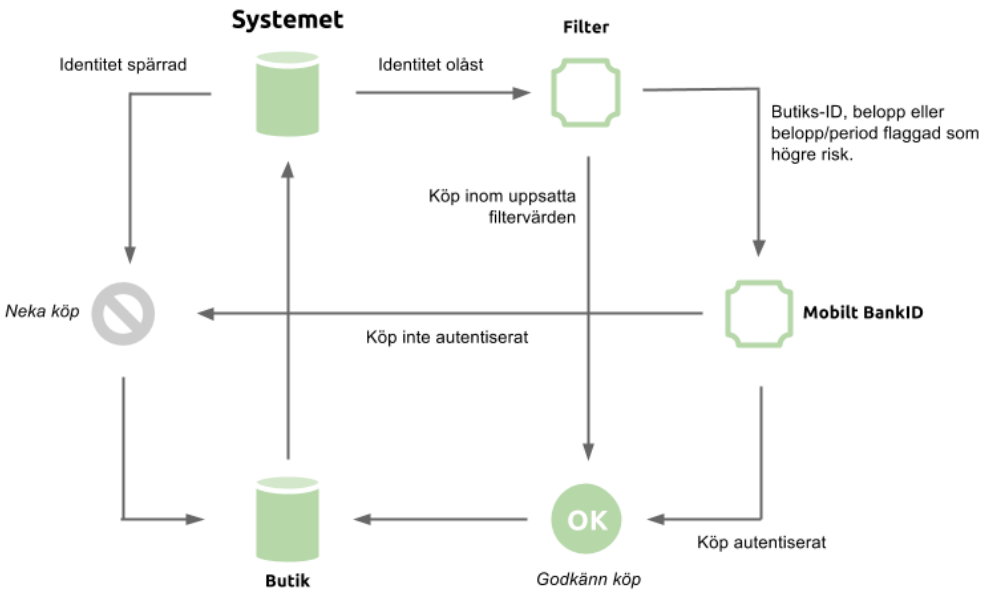
All funktionalitet i systemet ansågs grunda sig i säkerställandet av slutanvändarens identitet. Med andra ord skulle ingen övrig funktionalitet kunna tillhandahållas om identiteten på slutanvändaren inte har säkerställts, då det i dessa fall inte skulle finnas någon tydlig koppling till en specifik identitet. Därför ansågs autentiseringsmomentet högst relevant för att övriga delar ur systemet skulle kunna tillgodoses.

Mervärde och behandling av identitetshandlingar

För att kunna skapa ytterligare mervärde i tjänsten, samt till förmån för konsumenten, tillhandahålla ett säkert sätt att hantera personuppgifter på, bör förutsättningar finnas implementerade för att på ett säkert sätt lagra identitetshandlingar för en specifik slutanvändare.

Exempelvis kan de returnerade svaren från ett autentiseringsanrop genom systemets API kombineras med personuppgifter, vilket för konsumenten minimerar antalet manuella steg i webbutiken, samtidigt som det för webbutikens del säkerställs att verifierade personuppgifter tillhandahålls.

Ytterligare tjänster som kan hakas på ger ytterligare mervärde. Till exempel kan ett inkluderat kreditvärdighetsbetyg ligga till grund för en butiks beslut huruvida en kund bör få handla mot faktura. Ett annat exempel som detta system skulle kunna ligga till grund för är när flera underskrifter (verifierade identiteter) behövs, till exempel signering av kontrakt.



Figur 3.3: Filterfunktionens flöde

Filter

Genom att låta konsumenten styra över hur dennes identitet används ökar konsumentens inflytande och säkerhet.

Specifika regler för enskilda aktörer kan bestämmas, exempelvis att enbart betalningstransaktioner innehållande ett visst belopp från en specifik webbutik får initieras. Vid avsaknad av den aktuella aktören i användarens filter faller systemet tillbaka på de standardinställningar som är satta; även dessa kan bestämmas av användaren. Till exempel skulle en användare kunna låta alla belopp under 500 kronor gå igenom utan vidare identifiering så länge köpfrekvensen håller sig under fyra köp i veckan, alternativt kräva att alla frågor som rör identitet kräver ett godkännande.

Flödet för filterfunktionen finns illustrerad i Figur 3.3. Notera att enda gången ett köp nekas automatiskt är om en spärr finns på identiteten. I det fall att beloppet, köpen under en period eller någon annan av de justerbara variablerna överstigs frågar systemet istället efter en autentisering innan ett godkännande skickas tillbaka till webbutiken.

Notifikationer

Konsumentens insyn och kontroll vid hantering av identitetshandlingar uppnås genom att tillhandahålla funktionalitet för notifikationer. Funktionen kan nyttjas av aktörer som exempelvis kreditupplysningsbolag eller webbutiker för att meddela slutanvändaren om att en kreditupplysning eller ett köp har genomförts.

Ingång för slutanvändare

Slutanvändaren bör på ett enkelt sätt kunna ta del av lagrad persondata, händelsehistorik samt ha en möjlighet att kunna hantera filter för enskilda webbutiker och e-tjänster. Förslagsvis genom en användarportal där en verifierad slutanvändare kan få en översikt över inkomna notifikationer samt kunna hantera filter.

Genom att implementera denna funktionalitet med samma identitetsbekräftelse som resten av systemet för inloggning, framför en lösning som kräver användarnamn och lösenord, hålls systemet konsistent för användarna och ingen övrig registrering krävs.

3.3 Utformning av prototyp

En begränsad prototyp med tillhörande modeller, motsvarade en webbutik och en betalningsväxel, implementerades för att påvisa systemmodellens funktionalitet i praktiken. Säkerheten hade inte en framträdande roll då enbart funktionaliteten och möjligheten till implementation med externa, redan existerande system, var av intresse.

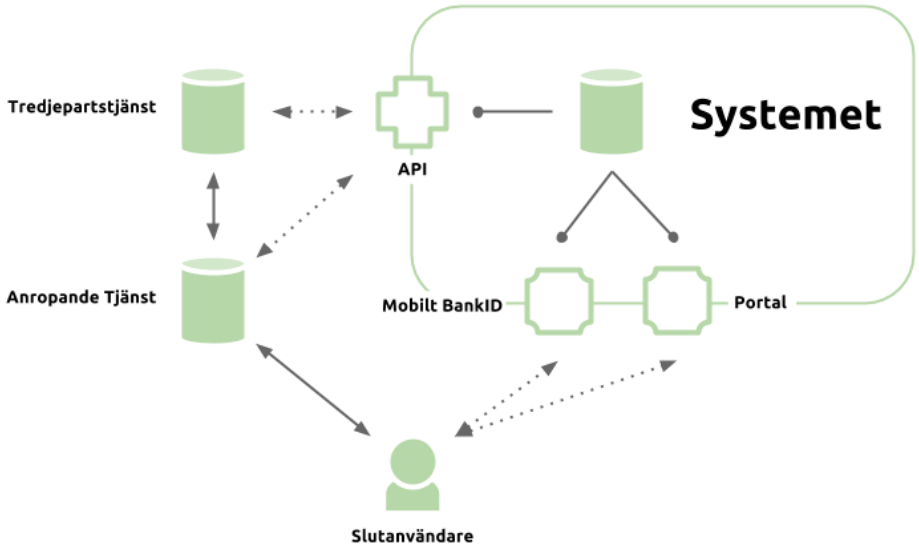
3.3.1 Mål

Den slutgiltiga prototypen skulle kunna kommunicera med webbutik, betalningsväxlar och slutanvändare på ett sätt som understödjer målsättningarna presenterade i Avsnitt 1.2. Med de givna målsättningarna skulle implementationen påvisa dessa i praktiken genom:

- Autentisering av slutanvändaren.
- Identifiering av den frågande parten.
- Att i ett senare skede i flödet möjliggöra kontroll av att slutanvändarens identitet är säkerställd.
- Kontroll av slutanvändarens filter mot enskilda webbutiker.
- Notifikationer till systemet som upplyser slutanvändaren om händelser som inträffat kopplat till dennes identitet.

3.3.2 Resultat

Prototypen kom att bestå av fyra skilda delar för att påvisa den föreslagna lösningen: ett grundläggande system med tillhörande API som kommunicerar mot detta samt en webbutik och en betalningsväxel som anropar systemets API. Figur 3.4 illustrerar den slutgiltiga prototypens olika komponenter samt flödet mellan dessa.



Figur 3.4: Systemets grundutförande och flöde

Implementation av systemmodell

Den utformade systemmodellen implementerades i programmeringsspråket Java med Tomcat som servletmotor. Som databashanterare användes MySQL för att lagra information om autentiseringssessioner, notifikationer, slutanvändarens filter för e-tjänster och webbutiker, personuppgifter med mera.

Implementationen av systemmodellen bestod huvudsakligen av två lager: ett logik-lager för att hantera inkommande förfrågningar och ett databas-lager för kommunikation mot den uppsatta databasmiljön. Logik-lagret utformades för att kunna ta emot HTTP-förfrågningar och hantera funktionalitet enligt de angivna målsättningarna i Avsnitt 3.3.1.

En testversion av BankID för utvecklare integrerades för att säkerställa identiteten på slutanvändaren. I testversionen skapades fiktiva användare av utvecklarna själva så att inga verkliga identiteter fanns att tillgå. Förfarandet och utformningen ansågs dock vara densamma.

Alla förfrågningar mot systemet förutsatte att aktörer som nyttjar tjänsten hade registrerats. En registrerad och giltig aktör tilldelas ett unikt token som måste skickas med vid ett anrop, för att verifiera avsändaren och godkänna att handlingen genomförs i sin helhet.

En förenklad filtreringsmöjlighet implementerades för att kunna påvisa den kontrollfråga som skulle kunna ställas av en verifierad aktör. Filtret utformades för att på ett enkelt sätt kunna ställa en fråga till systemet och kontrollera om ett köp, upp till ett visst belopp, från en specifik webbutik är tillåtet utan att vidare autentisering av konsumenten krävs. I annat fall ansågs det vara önskvärt att ha en autentiseringsfunktion att falla tillbaka på om ett köp nekas på grund av ett filter.

Även funktionalitet för att hantera notifikationer kopplat till en specifik identitet implementerades. Genom ett HTTP-anrop till systemets logik-lager kunde ett meddelande kopplat till en specifik identitet tas emot och lagras. Ett sådant meddelande skulle sedan kunna presenteras för slutanvändaren som en händelse i ett gränssnitt.

Avgränsningar i prototypen

Syftet med prototypen var enbart att verifiera den funktionalitet i systemmodellen som krävdes för att kunna besvara problemformuleringen i Avsnitt.1.1, därför valdes viss funktionalitet att utelämnas i implementationen av prototypen. Exempel på funktionalitet som inte producerades, men som ansågs nödvändig i en fullskalig implementation, var:

- En fullskalig portal med tillhörande gränssnitt där slutanvändaren kan logga in för att på ett enkelt sätt kunna ta del av notifikationer, lagrade identitetshandlingar samt hantera filter för enskilda e-tjänster och webbutiker
- Utökade filtreringsmöjligheter, exempelvis för att reglera kreditupplysningar, adressändringar med mera
- En funktion att falla tillbaka på om ett köp nekas på grund av ett uppsatt filter, vilken automatiskt initierar autentisering av slutanvändaren för att vidare kunna genomföra köpet

- Signering av värdehandlingar och andra utökade mervärdesfunktioner

API

Genom systemets API möjliggjordes direkt kommunikation mot det uppsatta systemet, vilken skulle kunna nyttjas av parter som tilldelats en giltig token. Kommunikationen skedde mot systemets logik-lager över *HTTP*.

Den slutgiltiga implementationen i prototypen kom att inkludera ett flertal funktioner med varierande antal argument och returdata, se Tabell 3.1.

Tabell 3:1 En sammanställning över funktioner i systemets API.

Funktion	Argument	Returdata
authenticate	1: ProviderToken, 2: SSN	JSON (String)
authenticate	1: ProviderToken, 2: OrderId, 3: SSN	JSON (String)
filter	1: ProviderToken, 2: Amount, 3: SSN	true/false (boolean)
notify	1: ProviderToken, 2: SSN, 3: Message	true/false (boolean)
authorize	1: ProviderToken, 2: AuthenticationToken, 3: OrderId	true/false (boolean)

Vid ett anrop till API:t krävs en giltig token som första argument för att verifiera avsändaren (*ProviderToken).* Med en giltig token har avsändaren full tillåtelse att använda systemets funktionalitet.

Två olika autentiseringsanrop implementerades i systemmodellens API för att kunna tillhandahålla både en renodlad autentiseringsmöjlighet, men även en möjlighet för att kunna autentisera en slutanvändare kopplad till en specifik transaktion eller order. Vid exempelvis e-handel skulle en autentiseringskontroll med dessa förutsättningar kunna göras för att säkerställa att identiteten på konsumenten verifierats, som ett sista steg innan ett eventuellt köp hos bank initieras.

En sådan kontrollfråga implementerades i API:t under funktionsnamnet *authorize,* vilken förutom avsändarens egna token som första argument även kräver en token specifikt kopplad till den part som ansvarar för att slutanvändarens identitet har verifierats. På så vis knyts en enskild transaktion eller order till en specifik aktör. Som tredje argument förväntas det ID-nummer som använts vid autentiseringen i transaktionen, som vid e-handel troligen skulle motsvara ett ordernummer.

Vid en lyckad verifiering av slutanvändarens identitet, genom ett autentiseringsanrop till systemmodellens API, inkluderades delar av den verifierade slutanvändarens identitetsinformation i det returnerade svaret för att påvisa det mervärde som kan skapas genom att centralisera hanteringen av dessa identitetshandlingar.

För att göra de returnerade svaren plattformsoberoende och lätta att använda för vidare behandling inom de egna systemen hos användarna av systemet (verifierade aktörer), utformades svaren som ett textformaterat JSON-objekt.

Modell av webbutik

För att illustrera hur lösningen skulle kunna komma att integreras i praktiken implementerades en modell av en webbutik. Webbutikens roll var att säkerställa identiteten på konsumenten genom ett autentiseringsanrop till systemmodellens API samt hantera konsumentens order och initiera denna till betalningsväxeln.

Autentiseringsanropet skulle komma att aktivera autentiseringsprocessen genom BankID; som efter ett godkännande från konsumenten skickar tillbaka ett svar om processens slutgiltiga status.

Vid en lyckad autentisering inkluderade det returnerade svaret ett textformaterat JSON-objekt med konsumentens personuppgifter för att på så vis illustrera det mervärde som tjänsten kan tillhandahålla. På så vis slipper konsumenten själv ange sina personuppgifter, vilket förenklar själva utcheckningssteget i webbutiken.

Modell av betalningsväxel

En förenklad variant av en betalningsväxel implementerades för att påvisa dess roll i betalningsflödet och hur denna part skulle kunna komma att använda systemmodellens funktionalitet i praktiken.

Den simplifierade betalningsväxeln kunde, med det ordernummer som genererats vid autentiseringstillfället i webbutiken, göra ett *authorize*-anrop mot API:et för att säkerställa att en autentisering tidigare har genomförts för den specifika ordern.

Om identiteten har säkerställts ställs ytterligare en förfrågan genom API:t för att kontrollera om eventuella filter har satts upp av konsumenten för den specifika webbutiken. Om transaktionen i detta skede passerar filtreringen kan själva köpet hos banken initieras. I annat fall nekas köpet redan i betalningsväxeln, vilket skulle innebära att ett skarpt köp inte hade kunnat fullföljas och vidare kommunikation mot bank förmodligen inte hade påbörjats (vilken handling som görs är högst individuellt och beslutas av den enskilde aktören).

3.4 Funktionskontroll av prototyp

3.4.1 Mål

En utvärdering av den framtagna prototypen skulle verifiera att den tekniska implementation som önskades av systemet var genomförbar enligt de målsättningar som angivits i Avsnitt 1.2 och 3.3.

3.4.2 Resultat

Autentiseringen av slutanvändaren kunde efterfrågas i prototypen genom ett anrop till systemets API. Vilket returnerade personuppgifter kopplat till den verifierade identiteten vid fullföljd autentisering. Funktionaliteten kunde verifieras i modellen för webbutiker.

Autentiseringsfunktionen implementerades utan att hindra webbutikens vanliga flöde i någon större utsträckning; genom att anropet till autentiseringen placerades i slutskedet av detta orderflöde. På så vis hindrade konsumenten från att slussas vidare till betalning vid ett negativt svar.

En förfrågan om huruvida konsumenten genomgått en lyckad autentisering kunde sedan ställas genom den implementerade kontrollfunktionen (authorize) i systemets API. En demonstration av funktionaliteten implementerades i modellen för betalningsväxeln.

Anrop till prototypens filterfunktion gav förväntat svar och nivåerna för dessa filter kunde justeras manuellt.

Prototypen påvisade att den tekniska funktionalitet och implementation som eftersträvades i den slutgiltiga systemmodellen var fullt genomförbar.

3.5 Utlåtanden kring systemmodell

För att utvärdera modellens funktioner och målsättningar gentemot de angivna punkterna i Avsnitt 1.2.3, genomfördes intervjuer med personer som ansågs besitta tillräckliga kunskaper inom områdena IT-säkerhet och/eller e-handel. De personer som intervjuades var Björn Ihlar (CTO på Payer Financial Services AB) och Björn Melinder (CTO på Soundtrap AB), som båda har avlagd examen inom datateknik och systemutveckling samt bred erfarenhet av att arbeta med och utforma komplexa distribuerade system. Sådana system innefattas av höga säkerhetskrav både ur system- och användarsynpunkt, varför de utvalda personerna ansågs högst relevanta för ändamålet.

3.5.1 Mål

De frågor som berördes var:

- De största säkerhetsriskerna vid e-handel
- Konsumentens inflytande och kontroll över betalningsflöden som baseras på befintlig teknik
- Vilken säkerhet som garanteras vid identitetshantering på internet
- Skillnaderna mellan den föreslagna lösningen och redan befintliga lösningar
- Hur den föreslagna lösningen kan få genomslag på marknaden
- Alternativa lösningar.

Intervjun delades upp i två delar samt en presentation av vår föreslagna lösning. Den inledande intervjuhälften orienterades kring det allmänna läget vid e-handel samt identitetshantering på internet. Sedan presenterades vår föreslagna lösning innan den avslutande intervjuhalvan avhandlade lösningens utformning, funktioner och eventuella brister.

3.5.2 Resultat

Inledningsvis var de intervjuade överens om att identitetskapning och identitetsbedrägeri är ett stort problem vid e-handel och en av de stora punkterna som branschen bör försöka att komma till rätta med.

Björn Melinder ansåg att många, sig själv inkluderad, förlitade sig på de försäkringar betalningsväxlar och banker erbjuder vid identitetsstölder; och att dessa två parter antagligen skulle vara mest angelägna om att eliminera riskerna. Björn Ihlar var däremot kritisk till den öppna hanteringen av identiteter och var angelägen om att flytta detta ansvar till konsumenterna själva. Som exempel ställde han sig frågande till att den enda gången en kunds identitet kontrolleras vid köp mot faktura är vid själva utlämningstillfället, då inköp, transporten och avisering till slutkund sker utan att en identitet har fastställts. Det är alltså först i

slutet av kedjan som konsumenten faktiskt måste legitimera sig. Någonting som skapar höga merkostnader för alla inblandade parter vid ett bedrägeri. Därtill tillkommer risken att den som fått sin identitet kapad blir varse om detta först i och med ett brev med ett inkasso-krav dyker upp.

Att flytta identifieringen av konsumenten till ett inledande led i köpförloppet upplevdes som någonting mycket positivt. Med ett öppet API fanns inte längre ansvaret att bevaka sin egen identitet hos konsumenten då webbutiker och andra tjänster kan välja att enbart hantera verifierade identiteter. Björn Melinder påpekade även möjligheten till en extern användarhantering, där säkerheten garanteras, genom detta föreslagna system.

Att erbjuda liknande tjänster men mot ett pris som konsumenten själv fick betala ansågs vara förlegat - som att företagen tog betalt för en lösning till ett problem som de själva skapat. Systemet uppfattades som ett lätt sätt för handlare att sänka sin risk; vilket enligt Björn Ihlar borde vara självbetalande.

4 Analys och diskussion

I det här avsnittet presenteras den analys och utvärdering som genomfördes av den föreslagna lösningen med hänsyn tagen till de givna målsättningarna som presenterades i Avsnitt 1.2.

Utvärderingen baseras huvudsakligen på det resultat som inhämtats från genomförd funktionskontroll av prototyp i Avsnitt 3.4.2, samt det sammanställda resultatet från de intervjuer som genomfördes med kunniga personer inom problemområdet i Avsnitt 3.5.2.

Inledningsvis presenteras analysen och utvärderingens slutsatser kring systemets utformning, vars funktionalitet verifierats genom prototypens implementation. Därefter följs avsnittet av ett konsumentperspektiv, en säkerhet- och riskanalys samt slutligen lösningens samhällsnytta.

4.1 Slutgiltig systemutformning

Den teoretiska modell som analyseras här baseras på systemets tilltänka komponenter i Avsnitt 3.2.2.

4.1.1 Autentisering

Autentiseringen ansågs ligga till grund för lösningens relevans och utgöra den bas som all annan funktionalitet kom att vila på. Att välja BankID framför en egenutvecklad lösning var naturligt med tanke på dess spridning och breda användarbas. En redan etablerad, säker lösning som används av statliga myndigheter och stöttas av banker ger en trovärdighet och säkerhet som är svår att arbeta fram på egen hand. Det breda genomslag Mobilt BankID har haft bidrog även det till att detta blev den valda tekniken.

Genom att göra kopplingen mot BankID till en relativt frikopplad komponent i systemet kan ytterligare autentiseringsverktyg inkluderas utan att systemet i sin helhet behöver modelleras om. Användningen av Mobilt BankID är utbredd i Sverige medan andra marknader använder sig av andra lösningar. Lösningar som systemet tack vare sin utformning kan kompletteras med och genast ge anslutna tjänster tillgång till denna expanderade marknad. I förlängningen skulle användare själva kunna välja vilket autentiseringsverktyg de vill använda sig av, förutsatt att det finns implementerat i systemet. De tjänster som nyttjar systemet är oberoende av vad användarna på andra sidan väljer att använda, de förlitar sig på den garanti som systemet levererar.

4.1.2 Kommunikation och öppenhet

Den öppna ingången som API:t utgjorde för webbutiker, betalningsväxlar och andra tjänster erbjuder ett lätt sätt att eliminera risk och användarhantering för de enskilda parterna. Detta samtidigt som slutanvändarnas insyn och kontroll stärks då autentiseringar alltid innebär ett godkännande från användarens sida, och utan en identifierad användare skulle inga behö-

righeter eller meddelandet kunna hanteras. Möjligheten att i en central portal överblicka historik för köp och efterfrågade autentiseringar ökar denna medvetenhet ytterligare.

Centraliseringen av autentiseringen är särskilt viktig att poängtera. Hanteringen av autentiseringen har förflyttats från enskilda aktörer till att istället hanteras i en gemensam och central punkt, vilken genom ett anrop till det öppna API:t kan nyttjas av vem som helst. Genom att tillåta öppna förfrågningar har man tagit ett första steg mot en standardisering av någonting som ger konsumenter en mycket säkrare internethandel. Dessutom blir en stor del av den komplexitet, som ett system av denna natur kräver, osynligt både för de anslutna tjänsterna och slutanvändarna.

Systemet skulle komma att behöva implementeras på ett sådant sätt att vilken verifierad aktör som helst, som erhållit en token, kan dra nytta av systemets tjänster. Målsättningen med utformningen var främst att göra tjänsterna lättillgängliga genom ett API, med skilda kopplingar och minimala beroenden mellan anropen, för att på så vis kunna integreras på ett enkelt sätt i redan befintliga flöden hos enskilda aktörer. Med den utformade prototypen kunde detta förfarande verifieras tämligen oproblematiskt genom de funktionsanrop som fanns att tillgå i systemets API.

4.1.3 Funktioner

Tack vare de öppna ingångarna behöver systemet aldrig vara låst till ett specifikt användningsområde. Denna rapport har i första hand avhandlat e-handel som tillämpning men redan med det enkla API som implementerats i prototypen kan systemet användas för användarhantering hos andra tjänster eller som signeringsverktyg för dokument. Ett exempel som lyftes fram av Björn Ihlar var försäljning av begagnade bilar mellan privatpersoner; där en enkel tjänst för att logga in och skapa ett dubbelt anrop till både säljare och köpare kan genereras.

4.2 Konsumentperspektiv

En utvärdering av de grundläggande funktionaliteter som ansågs vara nödvändiga ur ett konsumentperspektiv enligt de målsättningar som ställts på lösningen presenteras i detta avsnitt.

4.2.1 Användarportal

Konsumenterna kan med ett system enligt den föreslagna systemmodellen på en central plats överblicka hanteringen av sin identitet på internet. Med en autentiseringsmetod som de med största sannolikhet redan har tillgänglig. I förlängningen kan autentiseringen medelst detta system underlätta internethandel, genom att tillhandahålla användarens personuppgifter i det returnerade svaret till webbutiken utan manuell inmatning, och samtidigt minimera risken för bedrägeri.

4.2.2 Filter

Den flexibilitet som filterfunktionaliteten erbjuder tillåter konsumenten att själv balansera risken för bedrägeri och ett smidigt betalningsflöde. Samtidigt kan systemet se till att omfattningen av ett bedrägeri minimeras och tillhandahålla ett filter som konsumenten själv har kontroll över.

4.2.3 Notifikationer
Genom att skapa en möjlighet för konsumenten att på ett enkelt sätt kunna ta del av meddelanden via en potentiell användarportal, SMS eller e-post, kan viktig information kopplat till individens identitet göras lättillgänglig. På så vis skapas en möjlighet för konsumenten att agera på en otillåten handling som uppstått med dennes identitetshandlingar.

4.2.4 Tillämpning och beteende
Det finns en risk för att den extra procedur som detta systems autentiseringsförfrågan innebär upplevs som ett onödigt och krångligt moment i en webbutiks betalningsskede. Björn Melinder påpekade de försäkringar som redan finns etablerade för att skydda konsumenter från bedrägerier, där risken istället hanteras av betalningsväxlar. Konsumenten är alltså i många fall skyddad från de rent ekonomiska risker som ett bedrägeri kan innebära; om denna kan bevisa att det är ett bedrägeri. Det finns alltså en falsk trygghet etablerad i och med att de som ansvarar för att betalningen skett på ett riktigt sätt kompenserar de som blivit utsatta för bedrägeri. Utmaningen här ligger i att göra konsumenterna riskmedvetna och villiga att skydda sin (online-) identitet med de i denna rapport föreslagna verktygen.

På ett liknande sätt är det viktigt att konsumenterna förstår de fördelar ett system de själva kan kontrollera för med sig. Om webbutiker implementerar ett system konsumenterna inte känner till, och detta efterfrågar en manuell inställning av filter, spärrar, inställningar och autentiseringar, kommer systemet snabbt att upplevas som ett hinder istället för ett användbart verktyg.

4.3 Säkerhet och riskanalys
I en fullskalig utformning av den föreslagna systemmodellen behöver säkerheten garanteras för både konsumenter och de nyttjande tjänsterna. Den analys som följer i detta avsnitt går igenom några av systemets svaga punkter, de vanligaste attackerna samt möjliga åtgärder som bör ses som en grund för ett fortsatt säkerhetsarbete.

4.3.1 Länkarna i autentiseringskedjan
Implementationen av BankID gör att systemet förlitar sig helt på detta vid autentisering. Ingen egen kontroll av identitet görs. Denna punkt befinner sig således utanför systemets inflytande, och är någonting som inte kan garanteras förutom av BankID.

Vid en eventuell åtkomst till en användares BankID av en otillåten part finns inte längre någon säkerhet garanterad i systemet. De notifikationer som utgår från systemet skulle dock erbjuda en viss form av skydd, då användaren omedelbart skulle uppmärksammas på otillåtna händelser och handlingar.

Utformningen av BankID och den dubbla autentiseringen denna innebär, genom certifikat tillsammans med personlig kod, minimerar dock denna risk avsevärt.

Ytterligare säkerhetsåtgärder för att förhindra det nämnda scenariot ovan kan utformas, men då dessa förlitar sig på de instanser som utfärdar BankID blir de överflödiga. Om ett specifikt BankID eller användare av BankID spärras återspeglas denna åtgärd genom systemets uppbyggnad genast även här.

4.3.2 Säkerhet i applikationen

En utvärdering av de mest kritiska säkerhetsåtgärderna i systemmodellen på applikationsnivå, vilka beskrevs i anslutning till Avsnitt 2.7.

Utöver dessa kritiska punkter är felkonfigureringar i distribueringsmiljön, brist på tillståndskontroller samt felaktig implementering av funktionalitet för autentisering- och sessionshantering andra viktiga kryphål som man ansåg bör säkras i en fullskalig implementation av lösningen.

Cross-Site Scripting

En korrekt validering av in- och utgående data bör implementeras i en fullskalig lösning för att minimera risken för att användare utsätts för XSS-attacker.

Syftet med detta är att säkerställa att data som skickas till och från systemet är giltig och endast inkluderar innehåll som anses vara tillåtet. På så vis kan risken för att obehöriga kommer åt känslig information minimeras.

Cross-Site Request Forgery

För att kunna nyttja systemets funktionalitet krävs att en aktör är registrerad och har en giltig token. En token skickas med som parameter vid anrop genom systemets API, vilket knyter frågan till en specifik avsändare.

Den svaga länken i denna typ av implementation är att identitetssäkerställandet endast sker i ett steg, vilket innebär att så länge avsändaren känner till vilken token som ska skickas med i anropet kan momentet utföras i sin helhet. Att implementera ytterligare ett steg för att verifiera avsändaren skulle minimera denna typ av problematik. Om en token registreras tillsammans med ett eller flera IP-nummer, eller förfrågningens ursprung på annat sätt kan kontrolleras, stärks denna säkerhet ytterligare.

En implementation kräver även att en token och andra nycklar som tillhandahålls i tjänsten hålls utom slutanvändarens räckhåll. Ingen sårbar del av systemets anropsstruktur ska således förläggas tillgängligt för klienten (till exempel slutanvändarens webbläsare) via inkludering i JavaScript eller annan offentlig kod.

För prototypens del valdes detta att implementeras genom en statisk satt token i klientens webbläsare för att illustrera tankegångarna kring hur detta skulle komma att behöva hanteras i en eventuell framtida fullskalig implementation. Då koden som körs i webbläsaren hos klienten är öppen för manipulation bör genereringen av denna token ske från servern och låta denna kontrollera sessionens giltighet och livslängd.

Injection

Hot i form av Injections kunde i stor utsträckning förebyggas genom att återanvända färdig funktionalitet från bibliotek i utvecklingsmiljön (Java). Genom dessa kunde viss säkerhet garanteras eftersom de redan testats av en bred publik. Ett alternativ hade varit att utforma egna lösningar för ändamålet, vilket dock ansågs vara onödigt tidskrävande.

Sensitive Data Exposure
På grund av tidsbrist och icke-relevans för problemformuleringens huvudsakliga besvarande, valdes denna del att utelämnas i den utformade prototypen. Ett skydd för att inte låta obehöriga ta del av eller manipulera data i kommunikationsvägarna ansågs vara en särskilt viktig säkerhetsaspekt att ta hänsyn till i en fullskalig implementation av lösningen.

Genom att skydda data i kommunikationsvägarna med kryptering samt eventuella kontrollsummor för att kontrollera att data som färdats hållits intakt, kan obehörigas åtkomst och manipulering minimeras.

4.4 Samhällsnytta
Lösningen av problemformuleringen i Avsnitt 1.1 kom att bidra till en rad samhällsmässiga aspekter som konsument- och branschnytta samt etiska, miljö, sociala och ekonomiska aspekter.

4.4.1 Nytta för konsumenter och privatpersoner
Med den givna lösningen som en potentiell framtida standard för webbhandel och tjänster på internet, ansågs bedrägerier kunna minimeras drastiskt då kontrollen över identitetshandlingar förflyttas från de enskilda aktörerna till individen själv.

I lösningen kan konsumenten enkelt överblicka inträffade händelser kopplat till sin identitet samtidigt som en ingång för att kunna reglera hur ens identitet får användas hade skapats.

Den grundläggande problematiken kring de befintliga lösningarna ansågs vara att konsumenten kom i andra hand och till stor del lämnades utanför de faktiska handlingarna vid e-handel. En problematik som man nu ansåg fått en potentiell lösning.

De sparade kostnaderna för enskilda privatpersoner ansågs också vara en klar fördel då tjänsten som sådan skulle finnas att tillgå kostnadsfritt, vilket existerande konsumentskydd inte kunde leva upp till.

Ur konsumentens perspektiv skulle dock den givna lösningen kunna bli sedd som ytterligare ett krångligt moment beroende på hur webbutiken väljer att nyttja systemets tjänster. Då det finns en möjlighet för webbutiken att vid ett autentiseringsanrop genom systemets API erhålla uppgifter om den identifierade användaren, kan utcheckningsprocessen i webbutiken effektiviseras då användaren slipper ange uppgifter om sig själv i ytterligare ett steg. I annat fall kommer konsumenten behöva ha ett steg för autentisering och ett steg för inmatning av personuppgifter. Denna tröskel anses dock minska med tiden, om konsumenterna uppfattar detta som standarden för utcheckning och webbhandel.

4.4.2 Branschmässiga perspektiv
Den nytta som branschen (webbutiker, betalningsväxlar, kreditföretag med flera) har av den givna lösningen är den minimerade risken för identitetsstölder och bedrägerier. Genom att skapa ett gemensamt förhållningssätt och en gemensam ingång för att autentisera av slutanvändaren samt skapa förutsättningar för att låta denne kunna reglera behandlingen av ens identitet (genom filter), kan risken minimeras.

Då maximal säkerhet alltid är något som efterfrågas, i detta fall förhöjd konsumentsäkerhet, skulle denna lösning kunna besvara en stor del av de krav som ställs på webbtjänster. Det som krävs är dock att samtliga aktörer beslutar att förhålla sig till det gemensamma systemet, och därmed går med på att delvis lämna ute vissa delar av sin befintliga hantering som exempelvis interna autentiseringssystem och behörighetskontroller.

Fördelarna skulle främst bli tidsbesparingar och kostnadseffektiviseringar i form av minskad administration och utveckling. Förmodligen skulle detta även på sikt kunna gynna affärsutvecklingen genom ökad konvertering i och med att fler skulle känna sig trygga i att handla på internet. Omvänt skulle aktörer delvis förlora kontrollen i delar av flödet då vissa moment istället utelämnas till en extern aktör, vilket potentiellt skulle kunna bli en fallgrop för marknadsetableringen av systemet.

Att få tillgång till ett centralt system som tidigt kan upptäcka bedrägeriförsök genom att analysera notifikationer från flera webbutiker och betalningsväxlar skulle även bidra till utökad säkerhet. Det delade och på så sätt utökade underlaget kommer komma alla anslutna tjänster till gagn, då uppslag alltid kan göras mot uppdaterad data som finns tillgänglig centralt. De filter och bedrägeriåtgärder som finns i dagsläget är oftast separata och anslutna webbutiker eller användare kan därför behöva kontrollera eller notifiera flera tjänster innan skydd är tillgängligt.

4.4.3 Etiska aspekter

Denna föreslagna tjänst är ännu en i raden system som hanterar persondata och kan användas för att kartlägga beteenden på nätet; ännu mer centralt än vad enstaka webbutiker och betalningslösningar hittills har haft möjlighet till. Om detta ska upplevas som någonting positivt istället för bara ett nödvändigt ont för användaren bör så mycket som möjligt av hanteringen och tjänsterna vara transparenta. Användaren måste få en inblick i hur, var och när identiteten används och själv avgöra detta skeende.

Även det tillåtna användandet av denna personliga information bör tidigt etableras och kommuniceras till slutanvändaren. Riktad reklam eller annan sorts profilerat innehåll som kan generera utökade intäkter vid en kommersialisering av systemet bör noggrant ses över.

4.4.4 Sociala och ekonomiska aspekter

Den huvudsakliga målsättningen med den givna lösningen var att minimera antalet bedrägerier på internet, vilket ur ett konsumentperspektiv skulle bidra till ökat ekonomiskt skydd för den enskilde individen. Då lösningen tillhandahåller både autentisering och notifikationstjänster finns flera lösningar på hur bedrägerier kan förhindras.

Ur ett företagsperspektiv, det vill säga för de enskilda aktörer som nyttjar tjänsten, skulle en integration kunna leda till besparingar inom områden för identitetshantering genom den administrativa avlastning detta skulle leda till. På så vis skulle företagets arbete istället kunna koncentreras mer till den faktiska kärnverksamheten.

Dessutom leder bedrägerier oftast till höga merkostnader för samtliga inblandade parter, vilka även skulle kunna minimeras genom den föreslagna lösningen i och med dess syfte att motverka potentiella hot.

4.4.5 Miljö- och arbetsmiljöaspekter

Som en följd av dagens alltmer digitaliserade samhälle minimeras onödiga miljöbelastningar i allt större utsträckning genom att exempelvis låta postförsändelser skickas direkt till mottagaren på webben istället.

Med den givna lösningen skapas förutsättningar för att på sikt låta exempelvis manuella kreditutdrag och signeringar (autentiseringar) nyttja systemet som en mellanhand mellan aktör och konsument. På så vis kan man som konsument enkelt ta del av värdehandlingar som exempelvis kreditutdrag genom att logga in i användarportalen, samt få en notis via SMS eller/och e-post om specifika händelser.

Med BankID som kompatibel autentiseringsmetod skapas även förutsättningar för att på sikt kunna hantera enskilda eller multipla signeringar (flera inblandade parter). Exempelvis skulle förhandlingar som kräver multipel signering kunna digitaliseras helt.

Med dessa förutsättningar skapas goda möjligheter för att på sikt minimera onödiga miljöbelastningar i hantering som ännu sker genom någon form av manuell pappershantering. Dessutom skulle en sådan hantering innebära att stora delar av det arbete som i anslutning till detta utförs manuellt, istället kunna automatiseras och på så vis minimera onödig arbetsbelastning genom lägre andel manuell hantering och administration.

5 Slutsatser

I dagens e-handel, där identitetsstölder och bedrägerier är ett allt för vanligt förekommande, bör allas strävan (oavsett aktör) vara att se till så att tjänster tillhandahålls under så säkra omständigheter som möjligt. Med andra ord är det ett delat ansvar att se till så att direkta hot mot enskilda individer kan elimineras.

Genom att centralisera och skapa ett gemensamt förhållningssätt för behandling av identitetsuppgifter på internet kan en avsevärd risk för identitetsstölder och bedrägerier minimeras.

Så länge de föreslagna lösningarna inom problemområdet omfattas av affärs- och marknadsmässiga syften kommer det vara svårt att skapa tillräcklig trovärdighet och en långsiktig hållbarhet. Det behövs med andra ord en konkret och opartisk lösning som tagits fram till förmån för konsumentens bästa.

För att hitta en lösning inom problemområdet måste alla parter vara beredda att ta sitt ansvar och släppa på viss hantering som idag hanteras internt, till förmån för en tryggare e-handel.

Genom att integrera den föreslagna lösningen i exempelvis en webbutik kan en garanti för att slutanvändaren autentiseras innan köp tillhandahållas. Detta, i kombination med konsumentens möjlighet att hållas informerad om händelser som uppstår kopplat till sin identitet, skulle kunna få en kraftfull effekt i avseendet att minimera bedrägerier.

Konsumenten får i den föreslagna lösningen allt större inflytande och kontroll över vad som faktiskt sker med ens identitet i betalningsflödet, vilket skapar goda förutsättningar för att eventuella hot på ett mer lättillgängligt sätt, och i realtid, kan upptäckas.

Webbutiker skulle troligen affärsmässigt gynnas av att kunna stoltsera med att de enbart hanterar säkra transaktioner med verifierade konsumenter. På samma sätt för övriga aktörer som betalningsväxlar och kreditbolag.

För att ta lösningen ytterligare ett steg i rätt riktning bör en användarportal (där konsumenten på ett enkelt sätt kan hantera filter och få en överblick över notifikationer) implementeras i kombination med ytterligare filtreringsmöjligheter. Exempelvis filter för att tillåta eller inte tillåta kreditupplysningar, adressändringar eller andra transaktioner från enskilda aktörer. Dessutom multipel signering där ett flertal parter kan signera ett delat dokument, vilket kan vara effektivt vid hantering av exempelvis dödsbon, bilköp med mera.

Det här arbetet har visat att det med nuvarande teknik går att ta fram en central, öppen lösning och integrera den med redan etablerade flöden på internet, oavsett om det gäller e-handel eller andra tillämpningsområden. Den stora utmaningen ligger i att få varje enskild aktör att se en nytta med att ansluta sig till en gemensam lösning.

Källförteckning

[1] HUI Resarch, “E-barometern”,
http://www.hui.se/statistik-rapporter/index-och-barometrar/e-barometern
Publicerad: 2015, Hämtad: 2015-03-22

[2] Klarna, “Dataskydd på Klarna AB”,
https://cdn.klarna.com/1.0/shared/content/legal/sv_se/privacy_statement.pdf
Publicerad: 2015, Hämtad: 2015-03-28

[3] EasyCredit, “Identitetskapning”,
https://www.easycredit.se/nyheter/2014/identitetskapning/
Publicerad: 2014-09-11, Hämtad: 2015-03-23

[4] UC, “UC ID-Skydd”,
https://www.minuc.se/minUC/tjanster/uc-id-skydd.html
Publicerad: 2015, Hämtad: 2015-03-27

[5] KeyCode, “ID-Skydd”,
http://keycode.se/produkt/shop_privat/id-skydd-2/
Publicerad: 2015, Hämtad: 2015-03-27

[6] UC, “eSpärr”,
https://www.esparr.se/skydd-mot-idkapning-och-bedrageri
Publicerad: 2015, Hämtad: 2015-03-27

[7] Payer Financial Services AB, “Betalningsflöde”,
http://payer.se/wp-content/uploads/2015/03/payer_system_payflow.pdf
Publicerad: 2015, Hämtad: 2015-03-29

[8] Datainspektionen, “Personuppgiftslagen”,
http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen
Hämtad: 2015-03-30

[9] Datainspektionen, “IT-säkerhet vid införande av e-tjänster”,
http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/e-forvaltning/it-sakerhet-vid-inforande-av-e-tjanster/
Hämtad: 2015-03-30

[10] BankID, “Statistik 2015”,
https://www.bankid.com/sv/Statistik/Statistik-2015/
Publicerad: 2015, Hämtad: 2015-03-30

[11] Telia.se, "Telia e-legitimation"
http://www.telia.se/privat/bredband/tjanster/produkt/e-legitimation
Publicerad: 2015 , Hämtad: 2015-04-13

[12] E-legitimationsnämnden, C. Ekberg,
"Marknaden år 2012 för elektronisk legitimering och underskrift inom offentlig sektor"
http://www.elegnamnden.se/download/18.34f3b0b713e2cf5455b8eb/1366975458554/Marknad+för+elektronisk+legitimering+och+underskrift+2012.pdf
Publicerad: 2013-04-26 , Hämtad: 2015-05-11

[13] E-legitimation.se, "BankID och Svensk E-legitimation"
http://www.elegnamnden.se/nyheter/2015/nyhetsarkiv/bankidochsvenskelegitimation.5.3528414214b3f8758051f3c.html
Publicerad: februari 2015 , Hämtad: 2015-04-13

[14] OWASP, "OWASP Top 10 2013",
http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013.pdf

Bilagor

1. Intervjuer om säkerhet och utvärdering av lösningen

Följande punkter utformades för att ligga till grund för de intervjuer som gjordes för att utvärdera den färdiga systemmodellen.

Innan presentation:

- Handlar du mycket på internet i dagsläget?
- Är du medveten om riskerna med e-handel?
- Vet du vad som kan göras med din personliga information/identitet av en bedragare?
- Hur skyddar du dig mot identitetsstölder eller bedrägerier på internet?
- Vet du hur du ska handla när/om du upptäcker ett bedrägeri med din identitet?
- Hur uppfattar du det inflytande du som konsument har vid ett internetköp?
    - Vet du vad som görs med din identitet?
    - Är du medveten om vilka som hanterar din identitet?

Efter presentation:

- Denna lösning flyttar ansvaret från respektive internettjänst till slutkunden, hur uppfattar du detta? (som konsument respektive tjänst)
- Tror du att ett personligt filter för webbutiker och beloppsgränser är en önskad lösning?
- Anser du (som tjänst) att ett system som identifierar dina användare är nödvändigt?
- Finns det några säkerhetsaspekter som oroar dig med denna föreslagna lösning?
- Vad tror du behövs för att denna lösning ska få genomslag på marknaden?

Björn Ihlar, CTO, Payer Financial Services AB

https://drive.google.com/file/d/0B97RtgrU3glEVzRZUnRuTW9CNUU/view?usp=sharing
2015-05-19

Björn Melinder, CTO, Soundtrap AB

https://drive.google.com/file/d/0B97RtgrU3glEVS1uY1dNVlN2Zk0/view?usp=sharing
2015-05-27