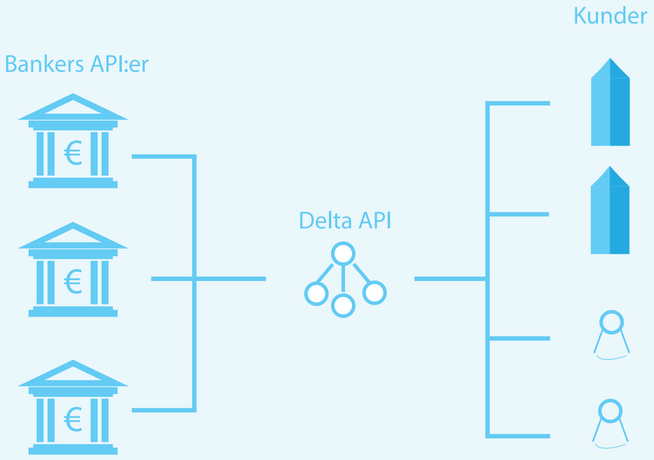
Ola Nilsson & Jacob Petersson

PSD2 I PRAKTIKEN

Utvecklingen av ett API som sammanfogar bankers Open Banking API:er

INLEDNING

Europarlamentet och Europeiska unionens råd har antagit direktivet *2015/2366 om betaltjänster på den inre marknaden* vid namn PSD2 som tvingar banker att öppna upp API:er om kunders kontoinformation till tredjepartsutvecklare. Examensarbetets syfte var att sammanfoga dessa så kallade Open Banking API:er till ett generellt API (se Delta API **figur 1**) för att underlätta utvecklingen av applikationer för företaget som arbetet utförs i samarbete med. Arbetet inkluderade en kartläggning av PSD2-direktivet och bankers Open Banking API:er, en undersökning av tekniker och integrationsplattformar samt utvecklingen av det generella API:et, döpt till Delta API.



Figur 1. Figur som visar hur API:et ska fungera och kommunicera med olika aktörer

MÅL

Målet med examensarbetet var att kartlägga PSD2 och utveckla ett fungerande API med minst två europeiska banker integrerade. API:et är tänkt att användas som en prototyp för en produktionsversion.

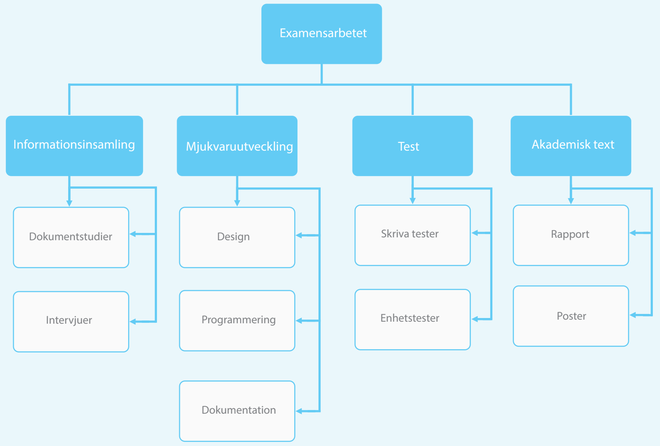
PROBLEM

Det finns idag få produkter som utnyttjar PSD2 och inget generellt API som slår samman bankernas olika API:er. Inom ramen för detta examensarbete skulle därför ett API utvecklas som är en sammanslagning av olika bankers API:er.

Rapporten syftade till att besvara följande frågeställningar:

- Hur ska vi kartlägga PSD2 och bankers Open Banking API:er?
- Kan vi utveckla vårt API på ett sätt som gör det möjligt för Smart Refill att lägga till nya banker i framtiden?
- Finns det färdiga integrationsplattformar tillgängliga och kan de användas för att underlätta utvecklingen?
- Hur hanteras personuppgifter med PSD2 och hur fungerar det tillsammans med GDPR?

METOD



Figur 2. Figur som visar examensarbetets *work breakdown structure*

Utvecklingen och skrivandet av rapporten utfördes löpande och de fyra huvudfaserna (se **figur 2**) var överlappande och bestående genom hela arbetet. Informationsinsamlingsfasen var av större vikt i början av arbetet då kunskap behövde samlas in om vad PSD2 var och om bankernas Open Banking API:er. Utfrågningar om PSD2 och diskussioner om API med relevanta personer på Smart Refill hölls också framför allt i arbetets tidiga skede för att förstå uppgiften bättre och för att samla in bestående kunskap.

Mjukvaruutvecklingsfasen pågick kontinuerligt under hela arbetet. I början av fasen var målet att experimentera med bankernas API:er och att göra ett eget API som fungerade med några enkla testanrop. Fortsatt utveckling gjordes av API:et med syfte att kunna ta emot svar från förfrågningar till bankernas API:er. API:et utvecklades först med fokus på funktionalitet. När API:et fungerade som det skulle gjordes en mer utförlig klassdesign av koden med programmeringsprinciper- och mönster i åtanke.

Testfasen inleddes i samband med utvecklingen för att veta om Delta API fungerade som det skulle. Ett testpaket gjordes med tillhörande klasser som testade de olika funktionerna av API:et. Testerna användes även som regressionstestning då det kunde uppstå problem med bankernas API:er som inte berodde på källkoden för Delta API.

Fasen för akademisk text pågick också kontinuerligt, men med större vikt på att kartlägga PSD2 och bankernas API:er i början, för att i senare skede vara mer fokuserat på att dokumentera teknikerna och själva API:et.

Som utvecklingsprocess användes en kombination av två olika agila processer kallad "Scrumban", från Scrum och Kanban. Från Kanban användes en kanbantavla och pågående-gränser för kolumnerna på tavlan, och från Scrum användes sprintar med en längd på sju dagar, sprintplanering samt sprint retrospectives.

LÖSNING

För att uppnå målet om att utveckla ett sammanslaget API användes många olika tekniker. En del tekniker var krav eller önskemål från uppdragsgivaren. De tekniker som lösningen skulle basera sig på är att följande:

- Applikationen ska utvecklas i NODE.js eller Java.
- Applikationen ska kunna köras i en Docker-behållare.
- Applikationen ska behandla OAuth2 flödet mellan kunden och banken.
- Applikationen ska returnera svar på HTTP-förfrågningar med data i JSON-format.
- Applikationen ska uppfylla villkoren för ett REST API.

Dessa krav uppfylldes i API:et med hjälp av olika tekniker. Några tekniker som användes är följande:

- REST
- Spring Boot
- Docker
- Programmeringsmönster- och principer (OCP, FACTORY, SRP, DIP, DRY)

Problemet som API:et skulle lösa var att en utvecklare bara skulle behöva göra anrop till ett API istället för flera olika. Huvudkravet var därför följande:

- Utvecklare ska kunna lägga till nya banker utan att modifiera nuvarande källkod (Open Closed Principle).

Detta löstes genom att använda olika programmeringsprinciper- och mönster. Ett krav från Smart Refill var att det skulle vara enkelt att lägga till nya bankers Open Banking API:er utan att påverka implementationen eller HTTP-svaren för andra banker. Detta innebar att koden skulle följa en programmeringsprincip vid namn OCP, vilket innebär att koden är skriven på ett sådant sätt att den är öppen för tillägg och stängd för modifiering. Den stängda modifieringen syftar i detta fall på de RestControllers som sköter förfrågningarna till API:et som inte ska modifieras utan se likadana ut för alla förfrågningar oavsett vilken bank som förfrågningen skickas till. Det öppna tillägget syftar på de banker som måste läggas till i den existerande koden. För att uppnå generalitet i RestControllers användes bland annat Factory-mönstret för att skapa rätt instans av det objekt med den information som användaren efterfrågar. Med hjälp av Factory-mönstret kan också nya banker läggas till på ett enkelt sätt och en implementering kan exempelvis göras för enbart kontoinformation och inte för transaktionsdata.

RESULTAT

Resultatet av examensarbetet är en kartläggning av PSD2 och bankernas Open Banking API:er. Ett fungerande API utvecklades även inom ramen för examensarbetet och är kopplat till bankerna Swedbank- och Nordeas Account Information Services API:er, samt respektive OAuth2 autentiserings-API:er. Delta API sammanfogar bankernas API:er till en HTTP-förfrågan och kan uthämta data om en kunds konton och transaktioner. Utvecklingen har påverkats av att Swedbank och Nordea inte har implementerat funktioner, i sina API:er, som hanterar personuppgifter. På grund av detta är det heller inte aktuellt med GDPR eftersom att inga personuppgifter behöver behandlas i Delta API. Utöver att Delta API fungerar så är applikationen inkapslad i en Docker-behållare som underlättar integrationen av mikrotjänsten i Smart Refills back-end.

Genom att bankerna måste släppa kontoinformation om deras kunder om de så önskar kan nya tjänster utvecklas och erbjudas, tjänster som gynnar kunden och erbjuder lösningar på ekonomiska problem som kunden kan tänkas ha. Detta innebär även konkurrens, vilket innebär billigare produkter av högre kvalitet. API:et som utvecklats är tänkt att användas i nämnda tjänster som gynnar slutkunden.

Bankerna utvecklar fortfarande sina Open Banking API:er och vissa banker har inte ens en sandboxmiljö tillgänglig ännu. Detta betyder att Delta API måste uppdateras i samband med kommande testversioner och produktionsversioner av bankernas API:er.