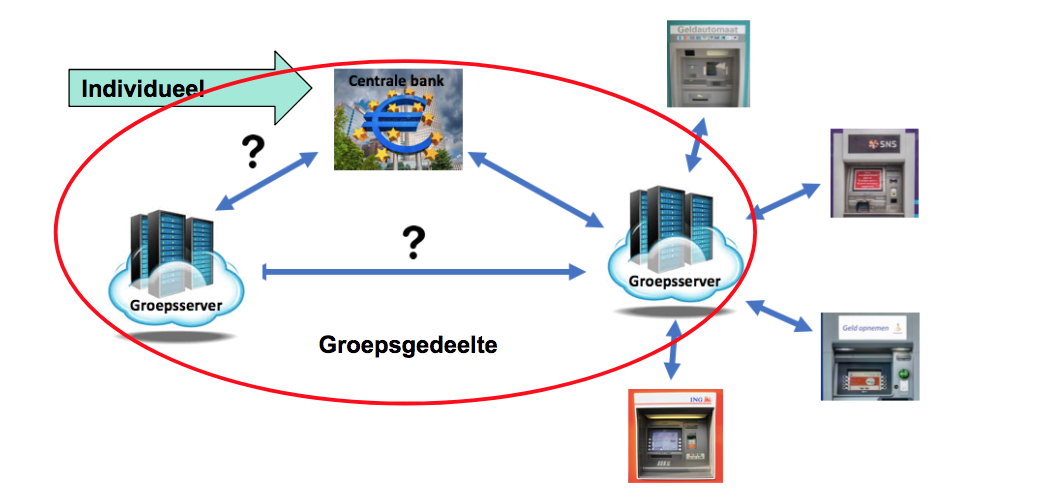
Project 4

Centrale bank advies rapport



Opgesteld door: Ilhan Delic

Studentennummer: 0914619

Groep: 4

**Inhoud**

Inleiding………………………….………………………………………………………………………………3

Productomschrijving ………………………………………………………………………………………4

Communicatie ……………………………………………………………………………………………….5

Beveiliging ……………………………………………………………………………………………………..6

advies……………………………………………………………………………………………………………..7

ontwerp…………………………………………………………………………………………………………..8

Risicolog …………………………………………………………………………………………………………10

Issue tracker …………………………………………………………………………………………………..11

Bronnenvermelding ………………………………………………………………………………………..12

**Inleiding**

Het doel van project 4 is het ontwerpen van een centrale bank voor alle banken van project 3. In project 3 heeft iedereen een individuele bank moeten maken en met de projectgroep was het doel om alle banken binnen de groep te verbinden via een lokale bank. De centrale bank gaat er voor zorgen dat alle lokale banken met elkaar verbonden zijn en kunnen communiceren.

Waarom is een centrale bank eigenlijk belangrijk? De centrale bank is belangrijk omdat deze een aantal taken moet voltooien om alle banken draaiende te houden.

Een belangrijk punt is de waarde van het geld stabiel houden. Hier wordt niet diep op in gegaan omdat dit niet zo zeer en technisch aspect is. Verder is de centrale bank daar om te zorgen dat het betalingsverkeer goed werkt zodat iedereen sneller makkelijker en veiliger elektronische betalingen kan verrichten.

Dit rapport is een advies over hoe de centrale bank efficiënt ingericht wordt.

**Productomschrijving**

Het product wat in dit rapport centraal staat is het ontwerp van een centrale bank. Deze bank moet een knooppunt zijn voor de banken die gemaakt zijn door de groepen uit het voorgaande project. Dit project is anders omdat er een ontwerp gemaakt van de communicatie tussen de banken en de centrale bank. Met het hoofddoel om de centrale bank zo efficiënt mogelijk in te richten. Hierbij komt de veiligheid van de communicatie ook bij kijken omdat er wordt gewerkt met gevoelige informatie en geld.

Om het product efficiënt in te delen moeten er een aantal attributen zijn waarover dit product moet beschikken:

* Security
* Vertrouwbaarheid
* Efficiëntie
* Maakbaarheid
* ***Security***

Bij het ontwerpen van een bank moet security een van de belangrijkste zaken zijn omdat je met het geld en vertrouwelijke informatie van mensen werkt. Als de security van een bank niet verzorgt of doordacht is dan is de kans op het binnentreden van het systeem erg groot. Dit wil je natuurlijk voorkomen.

* ***Vertrouwbaarheid***

Vertrouwbaarheid is ook een belangrijk punt bij een bank want als je de bank niet vertrouwt dan heeft het geen zin om daar je waardevolle spullen of je geld op te slaan. Daarom moet het gebruik van de bank vertrouwbaar aanvoelen voor de klanten van de bank.

* ***Efficiëntie***

Efficiëntie is nodig omdat je wilt dat je betalingen en zaken met geld zo snel en veilig mogelijk worden behandelt.

* ***Maakbaarheid***

Maakbaarheid is gekozen omdat je een tijdlimiet hebt om dit project af te ronden. In die tijd moet een goed ontwerp worden opgesteld en uitgewerkt zijn.

***De eisen***

Er zijn een aantal eisen opgesteld door de opdrachtgever deze zijn opgesteld volgens het MoSCoW systeem (must, should, could, would) om prioriteiten vaste te stellen:

-(m) het systeem moet efficiënt zijn, met een zo laag mogelijke laadtijd

-(m) het systeem moet schaalbaar zijn, andere banken moeten koppelen zonder problemen

-(m) de verbinding tussen databases en de centrale server moet beveiligd zijn

-(m) de bank moet vertrouwenwekkend zijn

**communicatie**

De communicatie is noodzakelijk zonder de communicatie kan je niks overdragen of opvragen. Daarom volgen hier onder een aantal manieren hoe je de communicatie kan regelen:

***MQTT:***

Message Queing Telemetry Transport(MQTT) is een protocol bedoelt om berichten naar elkaar te sturen. Het protocol werk als een publish/ subscribe systeem hiermee kan je apparaat informatie versturen naar andere apparaten maar het je kan het ook aanmelden om informatie van een bepaald apparaat te verkrijgen. Apparaten kunnen dan ook informatie naar de broker sturen. De broker gaat over alle verstuurde berichten deze worden door de broker gefilterd en de berichten worden naar de apparaten verstuurd die subcribed zijn.

Kort voorbeeld:

Een cliënt legt verbinding met een broker.

De cliënt heeft een unieke cliënte.

Nadat de cliënt verbinding heeft gemaakt met de broker, bevestigt de broker de connectie. De cliënt stuurt een PINGREQ en de broker zal reageren met een PINGRESP. Zo wordt de connectie levend gehouden.

Mocht de cliënt onverwachts het kanaal verlaten dan krijgt de broker een bericht van de cliënt die de broker afdrukt.

MQTT is een licht protocol en is makkelijk te gebruiken. Het is alleen niet secure maar hier komt in beveiliging een oplossing voor.

***HTTP;***

Hypertext Transfer Protocol is het protocol om cliënt met een server te laten communiceren. Dit gebeurt met een request en response. De cliënt vraagt wat bij de server en de server geeft een response. Er zijn wel een aantal nadelen met dit protocol met name dat het traag is, onbeveiligd en onzeker. Er is een onzekerheid omdat je request soms niet aankomt. Het is onbeveiligd en is er kwetsbaar tegen “man in the middle attacks” dit houd in dat er een persoon is die tussen jou en de server komt en alle info gaat eerst door de middle man waardoor deze kwetsbare informatie kan krijgen. je kan dit protocol beveiligen met een SSL/TLS certificaat

**Beveiliging**

Voor de beveiliging kan veel gebruikt worden ik pik 3 onderdelen waar ik het over wil hebben

***TLS:***

TLS (Transport Layer Security) is de nieuwe versie van SSL(Secure Sockets Layer). TLS werkt als een ingewikkelde handshake:

* De cliënt wilt verbinding met een server maken. Dit doet hij door een bericht met clientHello naar de server te sturen met daarin informatie over de TLS versie en welke encryptie algoritme er gebruikt wordt
* De server reageert met een serverhello met daarin informatie over het encryptie algoritme, de sessie ID, het certificaat van de server en de public key van de server.
* De cliënt controleert of de gegevens kloppen. Als deze kloppen dan vertrouwd de cliënt de server.
* Met dit vertrouwen stuurt de cliënt een geheime key naar de server.
* De cliënt stuurt een laatste geheime key voor voltooiing naar de server.
* De server stuurt een geheime key terug ter bevestiging.
* Nu heb je elkaar de hand geschud en kan je beginnen met informatie over te dragen

Door deze stappen te voltooien heb je een veilige verbinding en kan je gerust met je transactie beginnen.

***Pinpassen prefixen***

Omdat je pinpas in de database van je bank staat is je pas daar geregistreerd. Je bank heeft een bepaald kenmerk zodat de bank laat zien dat de passen bij de bank horen. Dit maakt het makkelijker voor de centrale bank om informatie op te halen over de pas omdat deze meteen weet waar je het moet zoeken.

***Hash functie***

Door belangrijke informatie als een pincode te hashen komen zulke belangrijke stukken data niet in de database van de bank. Hier wordt mee bedoelt dat je pincode een bepaalde code krijgt die niet te kraken is en zo staat je pincode niet in de database maar een rij met getallen en letters die samen de code voor je pincode vormen. Dit is een eenrichtingstechniek aangezien je van de code niet terug kan naar je pincode zo blijft die veilig bij de cliënt.

**Advies**

***Communicatie:***

Ik adviseer MQTT te gebruiken en http links te laten liggen. Voornamelijk omdat http traag is. Beiden zijn ze onbeveiligd en zijn ze zonder beveiliging makkelijk binnen te dringen. MQTT is een lichter programma dat door veel apparaten gebruikt kan worden. Het is makkelijk op te stellen in korte tijd en voldoet aan de attributen maakbaarheid en efficiëntie. MQTT gebruik het request en respons concept niet wat het sneller maakt dan http en door veel apparaten te gebruiken is. Ook ben je met MQTT zeker dat je bericht aankomt en dat is niet het geval bij http.

***Beveiliging:***

Bij de beveiliging adviseer ik gebruik te maken van TLS, de hash methode en de pinpassen te prefixen. Door meer veiligheidsmaatregelen toe te passen ben je er zeker van dat je systeem beter beschermt is. TLS is gekozen omdat het nieuw en veilig is de stappen die je moet voltooien om aan de slag te gaan zorgen er voor dat niemand kan meekijken naar wat je doorstuurt. Door de TLS over de MQTT te zetten heb je een simpel communicatie systeem dat goed beveiligd is. Het hashen van de pincodes zorgt ervoor dat de pincodes niet in handen kunnen komen van andere mensen zolang de cliënt de pincode niet zelf door verteld. Tenslotte door de pinpassen te prefixen kan je een stuk sneller de informatie van de pas ophalen en maakt je je systeem efficiënter.

**Ontwerp**

***Netwerkdiagram:***

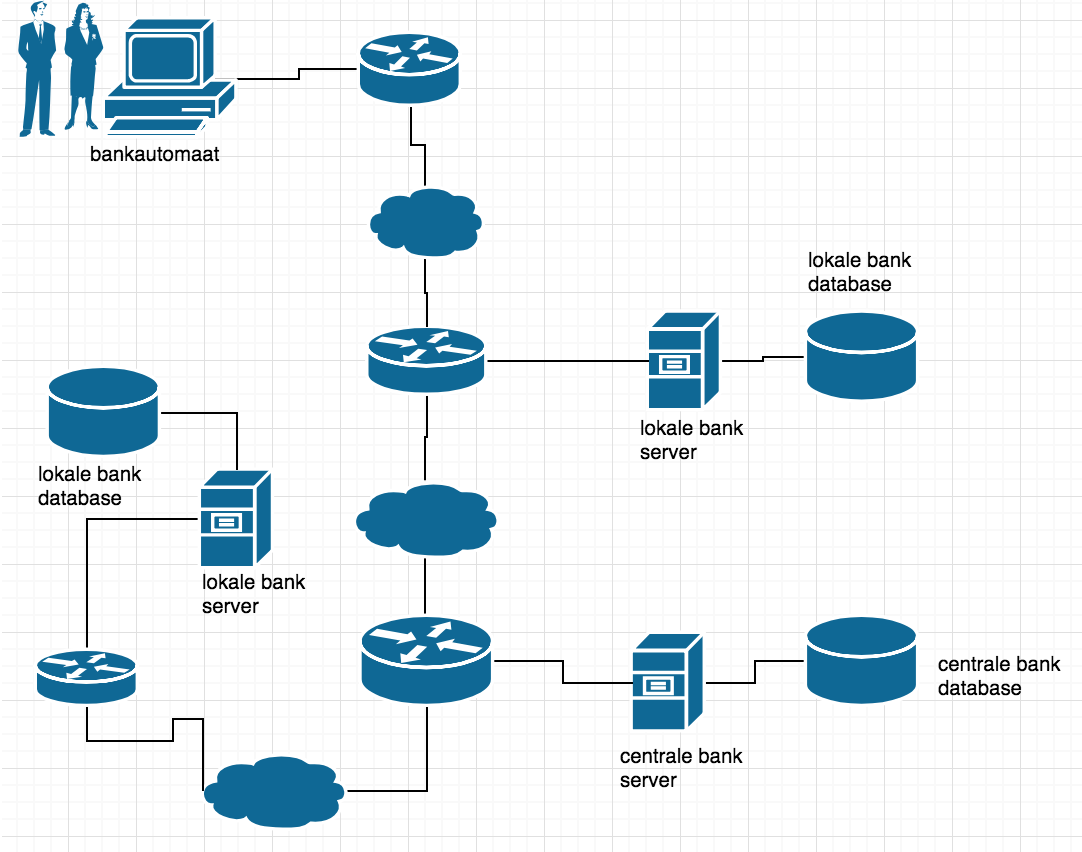


Fig.2

Zo ziet het netwerk van het bankenstelsel er uit.

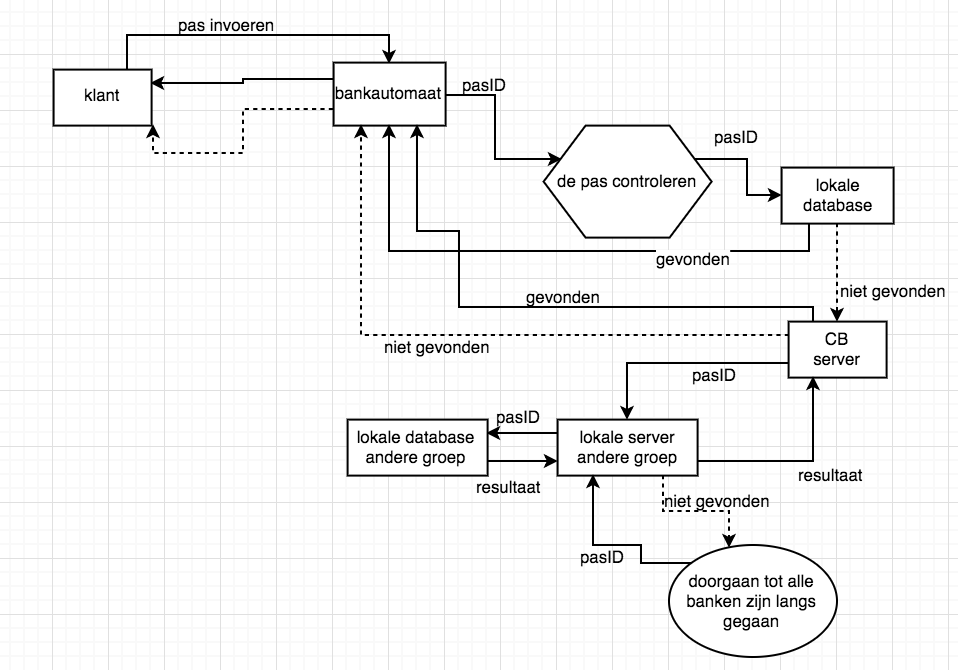
***Dataflow:***

Fig.3

**Risicolog**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **#** | **Risico Beschrijving** | **Kans** | **Impact** | **Risico\*** | **Maatregel** | **😶** | **Status Omschrijving** | **Datum** |
| R1 | Het afvallen van een groepslid | 2 | 4 | 8 | Het werk overnemen of met de begeleider bespreken hoe je groep verder gaat | N | Vorig project zijn er 2 leden afgevallen  het werk kon worden opgevangen  door de rest | 25-4-18 |
| R2 | Laptop gaat kapot | 2.5 | 5 | 9 | Maak backups, op git, drive etc. | N | Er wordt na elke aanpassing wordt  de file op geslagen en een  backup word bijgewerkt | 16-5-18 |
| R3 | Je begint te laat waardoor je je individuele deel niet af krijgt | 4 | 4 | 7 | Begin optijd en werk bepaalde stukken af over een lange periode | ☺ | Uistellen gebeurt vaak | 29-5-18 |
| R4 | Slechte communicatie met je groep | 3 | 4 | 7 | Maak een gezamelijke chat en maak afspraken om met elkaar af te spreken | ☺ | De communicatie in onze groep  verloopt goed | 23-5-18 |
| R5 | Het falen van onderdelen in het groepsdeel | 3 | 4 | 6 | Zorgen voor reserve onderdelen of een backup | 😐 | We zijn nog bezig met het bouwen  van het groepsdeel | 28-5-18 |

Tabel.1

Kans: schaal 1 (klein) t/m 5 (zeer groot)

Impact: schaal 1 (zeer lage) t/m 5 (zeer hoge)

Risico: = kans \* impact

😶: [status] :) opgelost, :| bezig; :( niet opgelost; N nieuw

Hier boven staan een aantal dingen die fout kunnen gaan tijdens het project met het response er naast.

**Issue tracker**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Datum In** | **Issue** | **Verantwoordelijk)** | **😶** | **Status Log** | |
| **Datum** | **Beschrijving** |
| J1 | 14-05-2018 | De bonnenprinter print niet goed | De printer | 😐 | 16-05-2018 | Code voor printer was getest |
| 18-05-2018 | Code aangepast |
| 23-05-2018 | Gelukt om een bonnetje te printen, de code  nog steeds aan het aanpassen |
| J2 | 23-5-18 | Onduidelijkheid over individuele deel | classroom | ☺ | 23-5-18 | Mostafa heeft ons aangesproken en aangestuurd |
| ... |  |  |  |  |  |  |

Tabel.2

😶: [status] :) opgelost, :| bezig; :( niet opgelost; N nieuw

hierboven staan issues waar we als groep tegenaan liepen.

**Bronnenvermelding**

MQTT:

<https://en.wikipedia.org/wiki/MQTT>

<https://classroom.google.com/u/1/c/MTU3MDgyMDI3MDla>

<https://www.youtube.com/watch?v=EIxdz-2rhLs>

http:

<https://nl.wikipedia.org/wiki/Hypertext_Transfer_Protocol>

<https://www.youtube.com/watch?v=po3zYOe00O4&t=276s>

TLS:

<https://nl.wikipedia.org/wiki/Transport_Layer_Security>

<https://www.youtube.com/watch?v=sEkw8ZcxtFk>

<https://hpbn.co/transport-layer-security-tls/>

HASH:

<https://en.wikipedia.org/wiki/Cryptographic_hash_function>

Tekeningen:

Fig. 2 & 3

<https://www.draw.io/>

templates van risicolog en issue tracker:

tabel.1 & 2 (fig.1 voorblad)

<https://classroom.google.com/u/1/o/MTI1NDgxNjY3NDda>