Rapport centrale bank

David
TI1A
Groep 3

Kakes

Inhoud

Inleiding

De aanleiding van het schrijven van dit rapport is de opdracht die ons is gegeven, ‘hoe richt ik efficiënt de centrale bank in’. In dit rapport zal dit uitgelegd worden met behulp van vier hoofdstukken. De hoofdstukken luiden als volgt: beheren, analyseren, adviseren en ontwerpen.

1 Beheren

In dit hoofdstuk wordt beschreven hoe het maken van de bank wordt beheerd. Hieronder valt versiebeheer met GitLab, risicolog en issuetracking.

1.1 GitLab

Via GitLab zal versiebeheer worden toegepast. De code, ontwerpen en documentatie zullen op de GitLab pagina worden gezet. Link naar GitLab: [Bytegroep 3 nuggetsbv project 4 gitlab]

1.2 Risicolog en issue tracking

In het risicolog worden mogelijke risico's besproken op het gebied van zowel de samenwerking binnen de groep als de uitvoering van het project. Daarbij worden oplossing aangedragen om deze problemen tijdens het project voor te zijn. Zie tabel 1 voor het risicolog.

	Risico	Oplossing
Samenwerking	Groepslid is langdurig ziek	Zijn werk wordt overgenomen
	Deadlines worden niet behaald	Contract met gevolgen opstellen
	Langs elkaar heen werken	Wekelijks vergaderen en voortgang bijhouden
Uitvoering	Computer crashed en alle documenten gaan verloren.	Alles op git zetten
	Er gaan onderdelen van de pinautomaten kapot	Reserveonderdelen aanschaffen

Tabel 1 Risicolog

Tijdens het project kunnen er problemen ontstaan. Deze problemen worden gedurende het project bijgehouden in de issue tracking tabel, zie tabel 2 voor een voorbeeld van een probleem. De status van het issue wordt aangegeven doormiddel van een emoticon. De mogelijke emoticons met betekenis staan hieronder weergegeven:

- 😊 = opgelost
- 😐 = bezig
- ☹ = niet opgelost
- N = nieuw

#	Datum In	Issue	Verantwoordelijk)	😶	Status Log	
					Datum	**Beschrijving**
J1	14-05-2018	De bonnenprinter print achterstevoren.	Bill Clinton	:)	15-05-2018	De driver voor de printer is niet goed, op zoek gegaan naar een andere driver, maar niet gevonden
					15-05-2018	De leverancier gebeld. Zij sturen een nieuwe driver
					16-05-2018	Nieuwe driver geïnstalleerd. De printer werkt weer naar behoren.
J2						

Tabel 2 Issue tracking

2 Analyseren

In dit hoofdstuk wordt het doel van het project duidelijk gemaakt en worden alle eisen aan de pinautomaat gesteld. Tot slot worden de mogelijke communicatie en beveiligingsmethodes toegelicht.

2.1 Doel

Dit project is een gevolg van het voorafgaande project waarbij iedereen individueel een compleet werkende bank heeft opgeleverd. Hierbij kon iedereen binnen de groep gebruik maken van elkaars banken. Bij dit project staat de communicatie tussen verschillende groepsbanken centraal en wordt er gezamenlijk met de groep een pinautomaat gemaakt. Daarnaast wordt er gewerkt aan een systeem waarbij iedereen ook bij een andere groep kan pinnen. Tot slot speelt de veiligheid van de banken een belangrijke rol. Aan de hand hiervan is een onderzoekvraag geformuleerd om het doel van dit project te kunnen bereiken: *'Hoe richt ik de centrale bank in op de meest efficiënte manier?'*

2.2 Kwaliteitseisen

De 4 gekozen attributen zijn:

- Security
- Maakbaarheid
- Effectiviteit
- Bruikbaarheid

'Security' is als attribuut gekozen omdat binnen een bank geld een belangrijke rol speelt, als dit niet goed wordt beveiligd zou hier misbruik van gemaakt kunnen worden. Daarom is 'security' een topprioriteit voor een bank, wanneer er iets gebeurd waardoor de veiligheid in gevaar komt heeft dit een grote impact op bijvoorbeeld het imago van een bank.

Voor 'maakbaarheid' is gekozen omdat de tijd waarin dit project dient te worden afgerond gering is. Daardoor moet er een balans worden gevonden tussen een goed werkend product binnen de beschikbare tijd.

'Effectiviteit' koppel ik deels aan 'maakbaarheid'. Ik heb hiervoor gekozen, omdat er zoals eerder beschreven wordt een beperkte tijd is waarin het project afgerond moet worden. Daarom zal er eerst aandacht worden besteed aan wat er belangrijk is, zodat de bank in ieder geval kan doen wat er op zijn minst van verwacht wordt. Mocht er tijd over zijn dan zal er gekeken worden naar eventuele extra's. Ik kies hiervoor omdat ik het persoonlijk belangrijk vindt dat bij het maken van een product het werkt naar behoren.

Tot slot is 'bruikbaarheid' belangrijk in een banksysteem. Het moet begrijpelijk en daardoor bruikbaar zijn omdat er allerlei mensen gebruik zullen maken van het banksysteem. Als alleen de maker van het systeem het begrijpt, is het geen goed product.

2.3 Niet-functionele eisen

De niet-functionele eis is dat de code leesbaar wordt geschreven. Dit houdt bijvoorbeeld in dat er standaarden worden gebruikt bij de notatie van variabele en de volgorde van de code. Ook is het belangrijk dat bij de code uitleg wordt gegeven, zodat iedereen die eraan zou moeten werken er mee overweg kan.

2.4 Communicatie

Tussen de banken is communicatie nodig. Dit is op veel manieren te bereiken, de twee manieren die hieronder behandeld worden zijn: MQTT en AMQP.

2.4.1 MQTT

MQTT is een lichtgewicht publish/subscribe protocol, hierdoor is het mogelijk om voor apparaten te publiceren naar een broker. Clients versturen berichten naar de broker. De broker filtert de berichten en publiceert deze aan clients, die zijn gesubscribed aan het onderwerp waar het bericht naar is gestuurd.

MQTT clients kunnen een stateful session awerness maken, dit houdt in dat een client met stateful session awerness disconnect de queue manager onthoudt waar de disconnected aan gesubscribed was. Wanneer de clients opnieuw connecten zal de client al zijn suscribed channels terugkrijgen en alle berichten die zijn verstuurd, terwijl hij niet geconnect was, zullen alsnog ontvangen worden.

In MQTT zit de Last Will And Testament (LWT) functie, deze functie zorgt ervoor dat wanneer een client de connectie verliest er een bericht wordt verstuurd door de broker waarin staat wie is gedisconnect en wat er moet gebeuren. Kort gezegd is MQTT een simpel, lichtgewicht en efficiënt protocol, waarbij het mogelijk is om tussen meerdere servers met elkaar te communiceren.

2.4.2 AMQP

AMQP is ook een protocol, de voordelen van dit protocol zijn de betrouwbaarheid en de interoperabiliteit. AMQP is zwaarder en groter dan MQTT en heeft meer opties. De werking van AMQP is ingewikkelder dan MQTT.

2.5 Security

De communicatie tussen de banken moeten beveilig worden zodat niet iedereen mee kan kijken wat er gebeurt en/of bijvoorbeeld nep geld op een rekening kan storten. Hieronder worden enkele manieren van security benoemd en toegelicht.

2.5.1 Simpele beveilig

Er zijn een paar simpele methodes om te beveiligen, deze kunnen wel omzeild worden maar maken het wel al moeilijker. Deze beveiligen de verbinding niet met encryption, maar ze maken het moeilijker om met de server de verbinden. Voorbeelden hiervan zijn:

- IP- whitelisting
- Client id prefix
- Username password

IP-whitelisting is simpel, je zet iemands IP op een lijstje die wel bevoegd is om iets te sturen of te ontvangen. Dit draagt wel bij aan de veiligheid maar is op zichzelf niet veilig genoeg, omdat de lijn niet wordt beveiligd.

Client id prefix betekend dat de client id verplicht is te beginnen met vooraf bepaalde tekens. Een voorbeeld hiervan is wanneer je als prefix HRO- hebt gekozen, het client id moet beginnen met HRO-. Het client id HRO-David kan wel verbinden, client id David kan daarentegen niet verbinden.

Door een broker kan een username en password worden gevraagd, zonder transport encryptie wordt dit onbeveiligd verstuurd waardoor iedereen die data aan het opvangen is de username en password kunnen zien.

2.5.2 TLS/SSL

TLS en SSL zorgt voor veilige communicatie tussen servers. In de kern zijn TLS en SSL cryptografische protocollen die een handshake-mechanisme gebruiken om verschillende parameters te onderhandelen om een veilige verbinding tot stand te brengen tussen de client en de server. Nadat de

handshake is voltooid, wordt een gecodeerde communicatie tussen client en server tot stand gebracht en kan geen enkele aanvaller enig deel van de communicatie afluisteren. Servers bieden een X509-certificaat, meestal uitgegeven door een vertrouwde instantie, die clients gebruiken om de identiteit van de server te verifiëren.

2.5.3 Payload encryptie

Payload encryption is encryptie van specifieke data op de applicatie laag. De tekst die je stuurt wordt geëncrypt voordat deze naar de broker verstuurd wordt. De voordelen hiervan zijn:

- Beveilig end-to-end encryptie van de applicatie laag
- Werkt goed op apparaten waar geen TLS kan worden gebruikt
- Beveilig op een extra laag voor het sturen van belangrijke informatica

Nadelen zijn:

- Encryptie en de crypten kan moeilijk zijn voor kleine apparaten (denk aan een nodeMCU)
- Helpt niet tegen ‘man in the middle’ attacks.

3 Adviseren

In dit hoofdstuk wordt toegelicht voor welke communicatie en beveiliging er is gekozen. Ten eerste zal de keuzen voor de soort communicatie worden beschreven en vervolgens de keuze voor het type security.

3.1 Communicatie

Voor de communicatie is gekozen voor MQTT. De reden hiervoor is omdat MQTT lichter en makkelijker is dan AMQP. Deze keuze is gemaakt op basis van de attributen: ‘maakbaarheid’, ‘bruikbaarheid’ en ‘effectiviteit’. Voor deze attributen is het van belang dat er een makkelijk manier is om te communiceren tussen de banken. Voor het attribuut ‘maakbaarheid’ is dit belangrijk omdat het daardoor makkelijk op te zetten is in de beschikbare tijd. Naast dat het met behulp van MQTT in een korte tijd kan worden opgezet, wordt er ook voldaan aan de essentie van het project wat van belang is voor ‘effectiviteit’. Daarbij doet MQTT wat het moet doen: berichten heen en weer sturen. Tot slot is MQTT makkelijker in gebruik dan AMQP, wat ten goede komt van de ‘bruikbaarheid'.

3.2 Security

Voor de security worden er meerdere opties samengevoegd: client id prefix, payload encryptie en TLS/SSL. Een manier om payload encryptie te bereiken is door end-tot-end incryption te gebruiken, dit houdt in dat de users die vertrouwd zijn een key hebben om de payload te ontcijferen. TLS/SSL encrypt het bericht over lijn, hierdoor wordt er voor een dubbele bescherming gezorgd. Dit maakt de communicatie via het MQTT protocol op meerdere lagen veilig. Ook is dit op een makkelijk en effectieve manier te bereiken wat ten goede komt aan de attributen. In het volgende hoofdstuk wordt duidelijk hoe dit allemaal samen wordt gevoegd.

Ontwerpen