PROJECT 4
INRICHTING CENTRALE BANK

Mirthe Tiggelman
0944158
Bytegroep 2

INHOUD

- Doel van het project
- Advies voor Centrale Bank
- Niet-functionele eisen
- Netwerk Diagram
- Data Flow Diagram
- Kwaliteitspunten
- Security
- Privacy
- Bruikbaarheid
- Efficiency
- Risicolog
- Issue Tracking
- Bronnen

DOEL VAN HET PROJECT

- Het doel van het project is om een idee te bedenken hoe je een centrale bank op kan zetten.
- Dit doe je door alle lokale banken met elkaar te verbinden zodat een klant bij elke pinautomaat bij zijn eigen rekening kan.

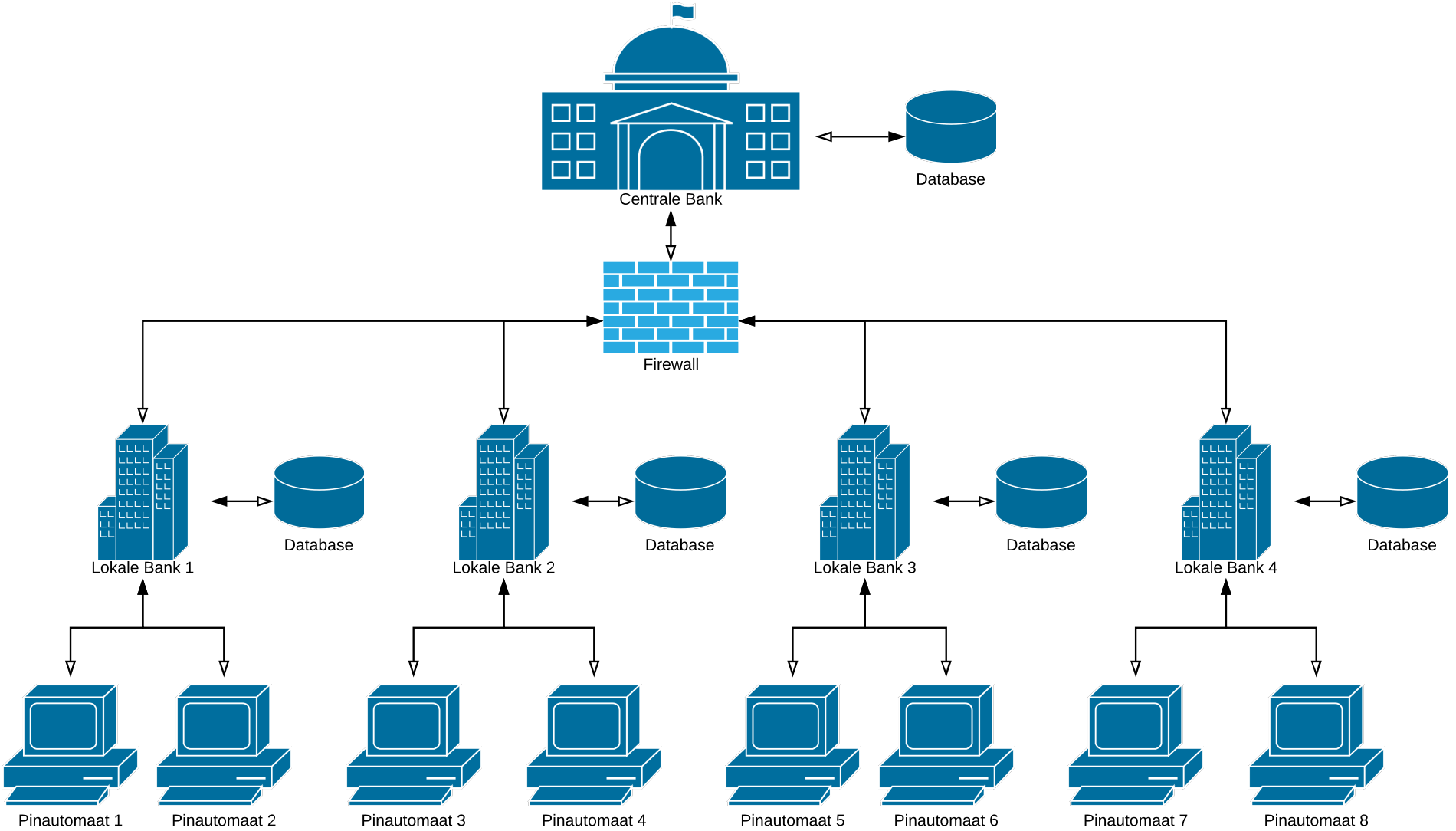
ADVIES VOOR DE CENTRALE BANK

- Hoe ga ik de centrale bank opzetten?
- Alle pinautomaten zijn verbonden met de lokale bank waar ze bij horen. Als je gaat pinnen en jouw pasnummer wordt niet gevonden bij de lokale bank (dus bijvoorbeeld je pint met een ING-pasje bij een Rabobank pinautomaat), dan wordt het pasnummer doorgestuurd naar de centrale bank
- De centrale bank heeft een database met alle pasnummers en houdt bij welk pasnummer bij welke lokale bank hoort. Hierna worden de juiste gegevens bij de juiste bank opgehaald en wordt dit doorgestuurd naar de pinautomaat.

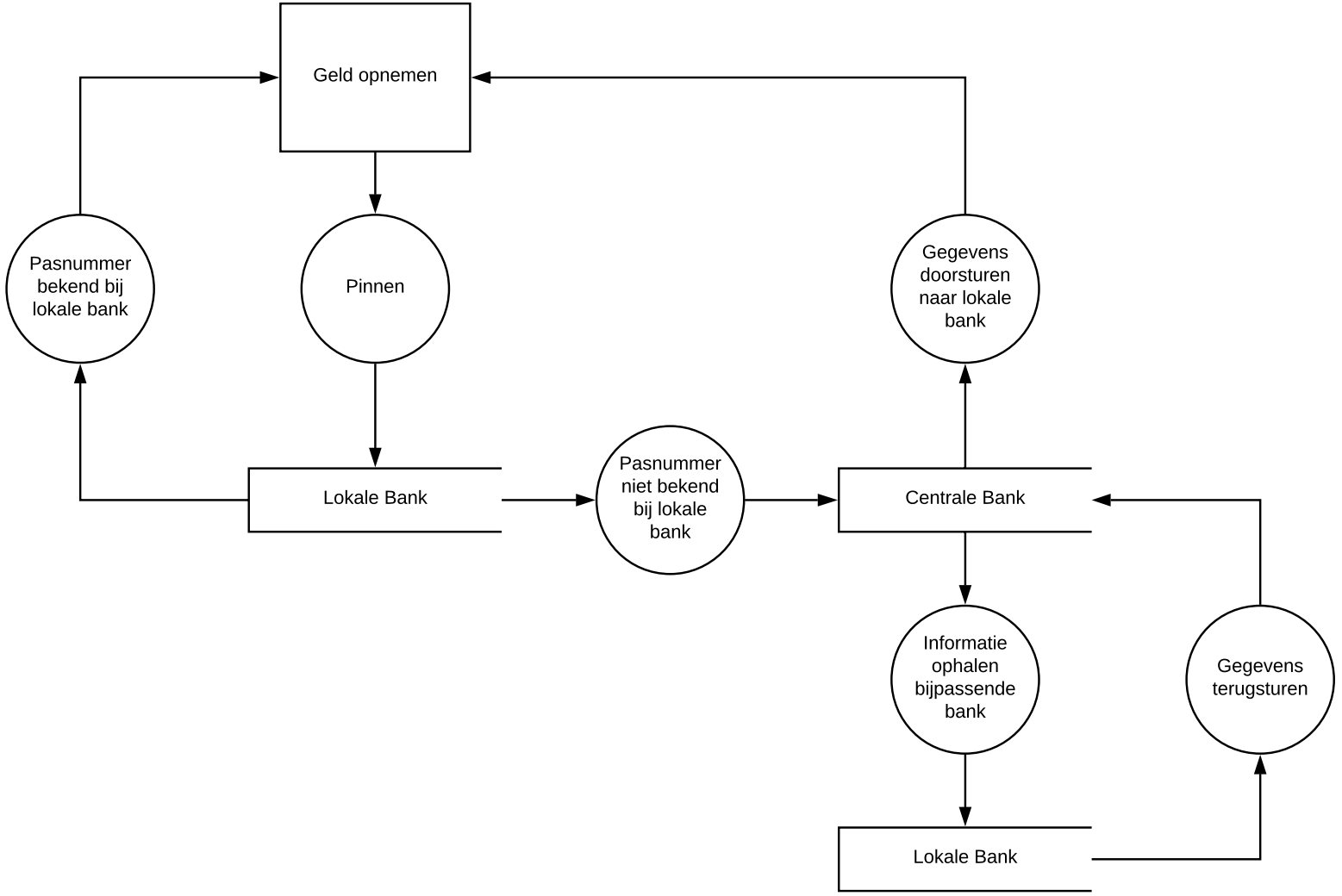
NIET-FUNCTIONELE EISEN

- Gegevens uit de centrale database zijn geëncrypt
- Alle communicatie is beveiligd
- Er worden geen onnodige dingen/gegevens opgeslagen.

NETWERK DIAGRAM



DATA FLOW DIAGRAM



KWALITEITSPUNTEN

- Ik heb gekozen voor de kwaliteiten **security en privacy**. Omdat banken veel gevoelige en belangrijke informatie beheren moet het goed beveiligd zijn zodat deze gegevens niet zomaar door iedereen gelezen kunnen worden. Ook met privacy zorg je ervoor dat de gegevens van de cliënten beter beschermd worden omdat er geen onnodige gegevens worden gebruikt.
- Daarbij heb ik ook nog gekozen voor **bruikbaarheid en efficiency.** Een pinautomaat moet gewoon makkelijk en goed te bedienen zijn zodat iedereen geld kan pinnen. Ook moet het zo efficiënt mogelijk zijn omdat dat weer veel tijd scheelt.

SECURITY

- Gegevens uit de database wordt geëncrypt met asymmetrische encryptie. Stel dat er een lek is bij de database dan zorgt dit ervoor dat het vrijwel onmogelijk is om de gegevens te achterhalen en alle gegevens dus alsnog veilig zijn.
- De communicatie tussen de Javaprogramma's wordt beveiligd door middel van een TLS-verbinding. Dit is om te voorkomen dat data kan worden gelezen of gewijzigd. TLS maakt gebruik van zowel asymmetrische encryptie als symmetrische encryptie. Hiermee wordt de server gecontroleerd terwijl de cliënt onbekend blijft. Waarmee je dus ook voor extra privacy zorgt.
- Ook bevat de server een firewall die bepaalt welke gegevens worden doorgestuurd en welke niet.

PRIVACY

- Om te zorgen dat er privacy is, worden er maar 2 dingen opgeslagen in de database van de Centrale Bank. Dit zijn het pasnummer en bij welke Lokale Bank dat pasnummer hoort. Hiermee heb je in principe alles wat nodig is om de Centrale Bank goed te laten werken. Er worden dus verder geen persoonlijke gegevens opgeslagen in de database.

BRUIKBAARHEID

- De Centrale bank is klaar voor gebruik als de server eenmaal werkt. Er hoeft verder ook niks gedaan te worden voor de Centrale bank omdat alle communicatie tussen de Lokale banken loopt. De Lokale banken sturen data door en ontvangen dit ook weer. Echter hangt de bruikbaarheid vooral af van de pinautomaten zelf en of dat deze makkelijk te bedienen zijn.

EFFICIENCY

- Het hele systeem werkt vrij efficiënt. Dit komt ook doordat er eigenlijk geen verkeerde data doorgestuurd kan worden. Alle data die binnenkomt wordt nuttig gebruikt. Er zijn eigenlijk maar 3 processen bezig: Lokale bank vraagt data op, Centrale bank en de Lokale bank versturen data. Als er wordt gepind bij een Lokale bank en dit pasnummer is niet aanwezig in de Lokale database dan wordt deze informatie doorgestuurd naar de Centrale bank en deze kijkt wat de bijbehorende Lokale bank is en stuurt deze gegevens weer terug.
- Het kan ook zo zijn dat het pasnummer ook niet aanwezig is in de Centrale database, deze stuurt dan een foutmelding naar alle Lokale banken en daar wordt dan gecontroleerd of dat het pasnummer echt niet in de database staat.

RISICOLOG

#	Risico beschrijving	Kans	Impact	Risico	Maatregel	😶	Status omschrijving	Datum
R1	Tijdsnood	3	5	15	Goed plannen	:|	Er is een planning gemaakt	25-04-2018
R2	Veel lessen vallen uit	4	3	12	Meer vrije tijd in steken	:|	Er is een planning gemaakt	25-04-2018
R3	Bestanden zijn weg	1	5	5	Op GIT opslaan	:)	Op GIT opslaan	25-04-2018
R4	Server valt uit	1	5	5	Regelmatig controleren of hij nog werkt.	:|	N.v.t.	25-04-2018

ISSUE TRACKING

#	Datum in	Issue	Verantwoordelijk	😶	Datum	Beschrijving
U1	25-04-2018	Nog nooit met GitHub gewerkt.	Mirthe	:)	15-05-2018	Uitleg gezocht.
U2	25-04-2018	Opdracht eigen deel is onduidelijk	Project	:|	N.v.t.	Zoeken naar verduidelijking

BRONNEN

- http://www.datashieldcorp.com/2013/06/04/3-different-data-encryption-methods/
- https://nl.wikipedia.org/wiki/Transport_Layer_Security
- https://www.senet.nl/blog/wat-is-encryptie/
- SSL Workshop.pdf