**SoS**​**iT**

Helpdesk Systeem

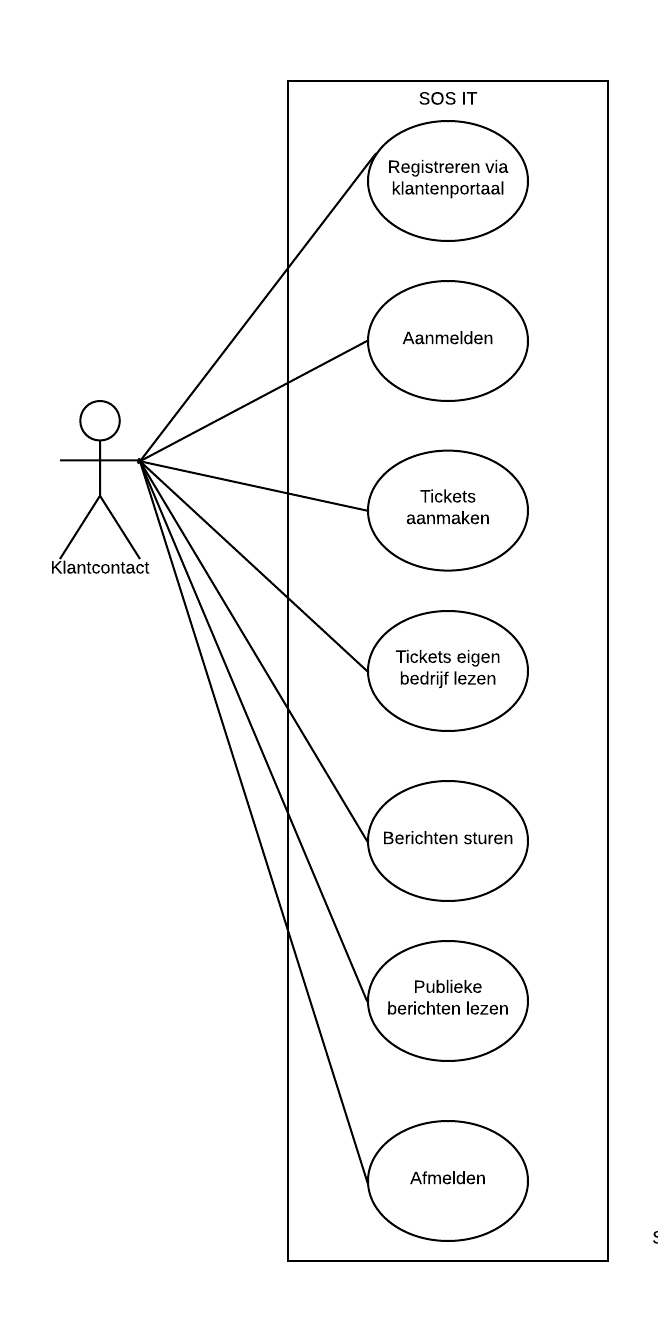
Projectwerk analyse

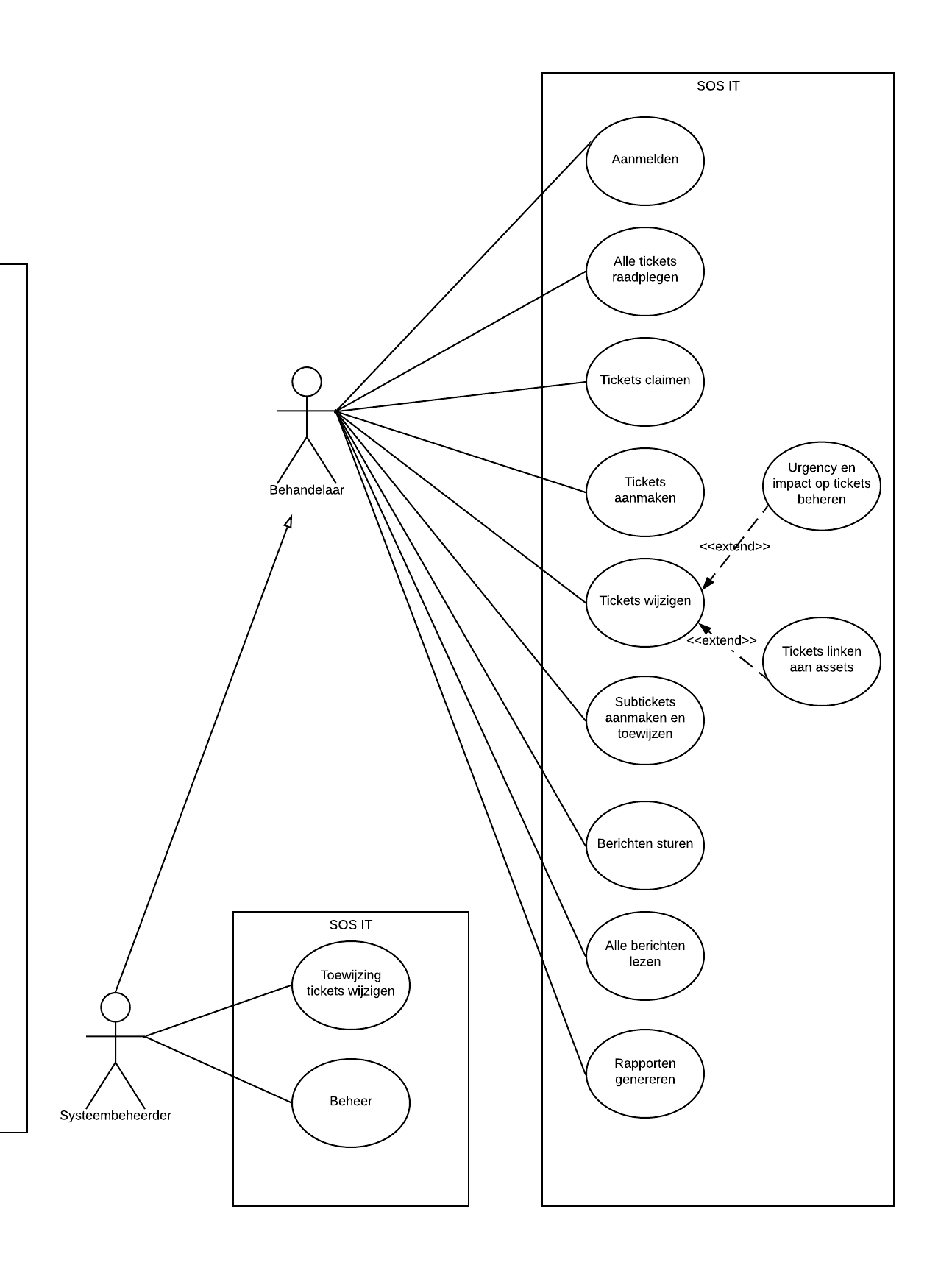
Jeroen Leyssen   
Goedele Reynders  
Maxim Ruysch   
Tom Scheyltjens   
Koen Van Looy

# Verklarende woordenlijst

# Mindmap

# Use case diagram





# Use cases

Systeem = SOS IT, helpdesksysteem

1. Klantcontact
   1. Registratie via klantenportaal
   2. Aanmelden
   3. Tickets aanmaken
   4. Tickets van het eigen bedrijf lezen
   5. Berichten sturen
   6. Publieke berichten lezen
   7. Afmelden
2. Helpdeskmedewerker/behandelaar
   1. Aanmelden
   2. Tickets aanmaken
   3. Tickets claimen
   4. Alle tickets raadplegen
   5. Tickets wijzigen
   6. Urgency/impact beheren
   7. Tickets linken aan assets
   8. Subtickets aanmaken en toewijzen
   9. Berichten sturen
   10. Alle berichten lezen
   11. Rapporten genereren
3. Systeembeheerder
   1. Toewijzing ticket wijzigen
   2. Beheer

# Activity diagram

# Klassendiagram

# ERD

# Extra optionele functionaliteiten

## Bewaren van paswoorden

Paswoorden worden gehashed opgeslagen. Met hashing wordt er een berekening uitgevoerd op de input. Deze berekening geeft een bepaalde uitkomst die wordt opgeslagen in de databank. Vanuit deze uitkomst kan je nooit terug naar de originele input.

Als een gebruiker later opnieuw inlogt, wordt de input opnieuw berekend. De hashcode die uit deze berekening komt, moet overeenkomen met de hashcode in de databank. Indien dit niet het geval is, dan is het ingevoerde wachtwoord niet correct.

Jammer genoeg bestaan er tegenwoordig manieren om hashes terug te rekenen. Hiervoor wordt er gebruikt van Rainbow Tables. Dit is een grote databank met woorden en de bijhorende hashes. Als een databank gelekt wordt en een gebruiker heeft een makkelijk woord als wachtwoord, is het voor een hacker makkelijk om de combinatie wachtwoord en gebruikersnaam te achterhalen.

Om dit op te vangen kan er gebruik gemaakt worden van salting. Niet enkel het wachtwoord, maar ook andere gegevens van de gebruiker worden gebruikt om een hash te berekenen.

Je zou paswoord kunnen hashen samen met geboortedatum (= salting). Op het resultaat van de salting kan je opnieuw hashing toepassen.

Het is belangrijk om lange (complexe) wachtwoorden te gebruiken om een betere hashing te bekomen.