Stocks Specification

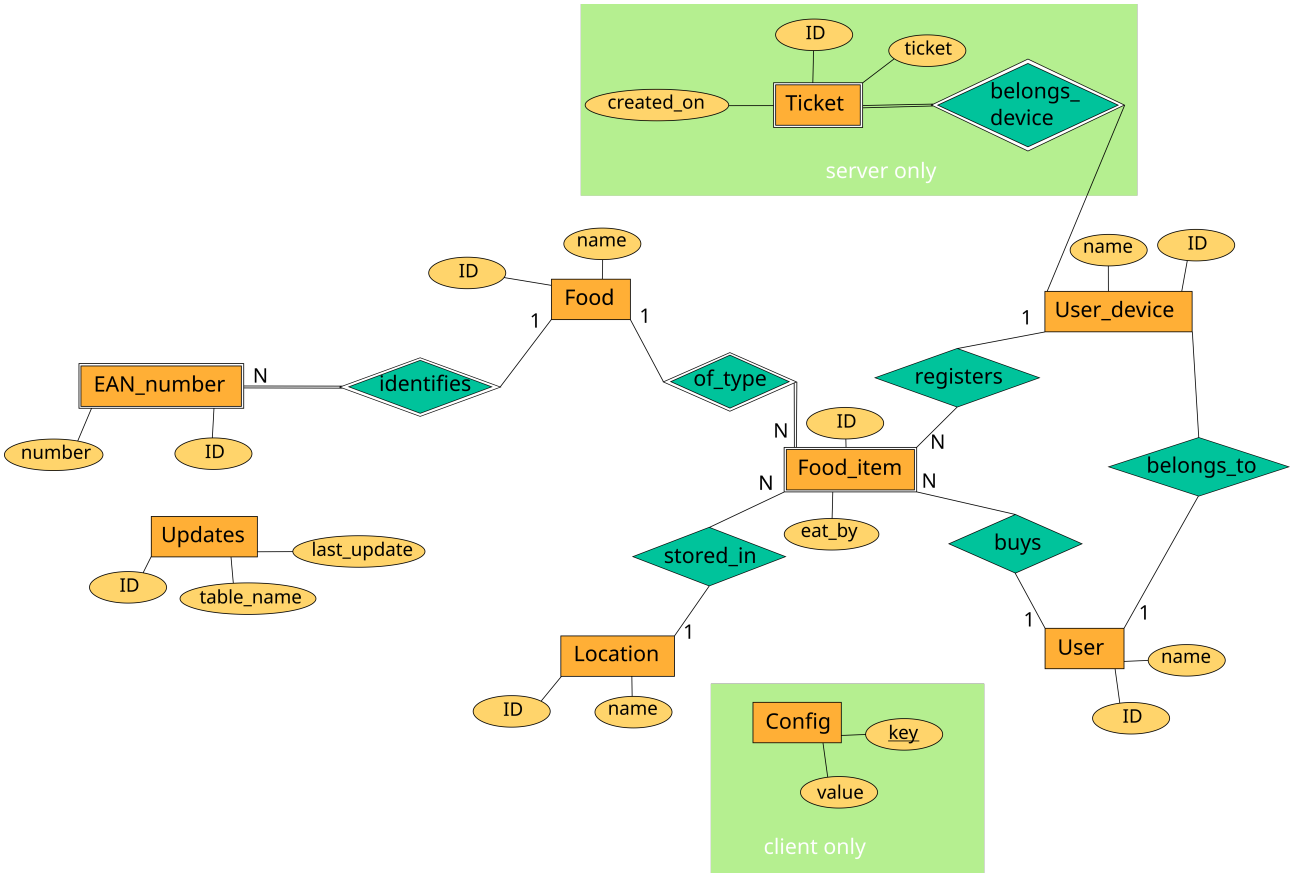
Jan Veen

July 21, 2017

Contents

Chapter 1

Data Model



Chapter 2

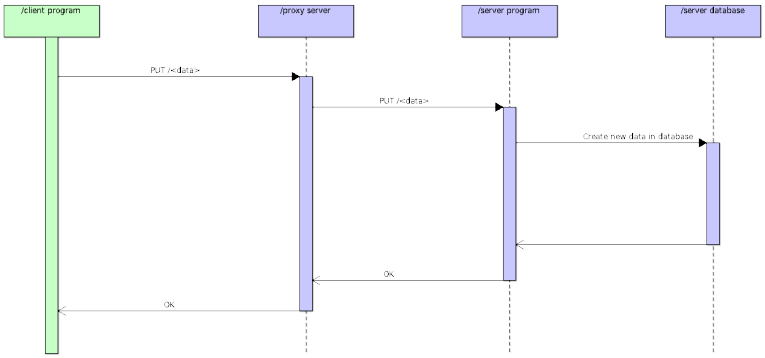
Architecture

2.1 Used Software

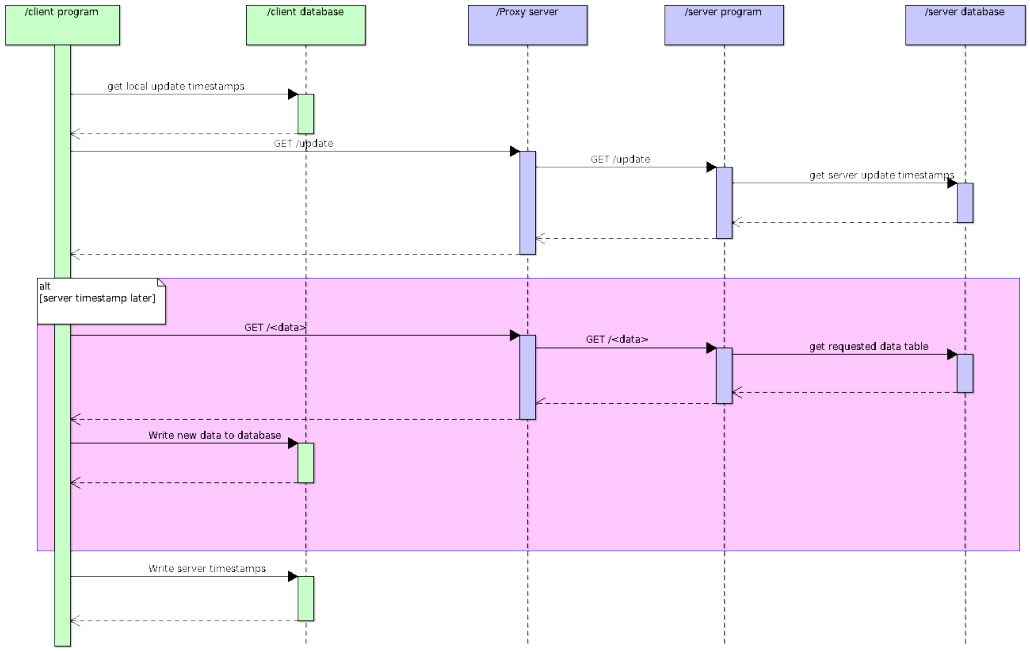
2.2 Server

2.3 Client

2.3.1 Register New Data

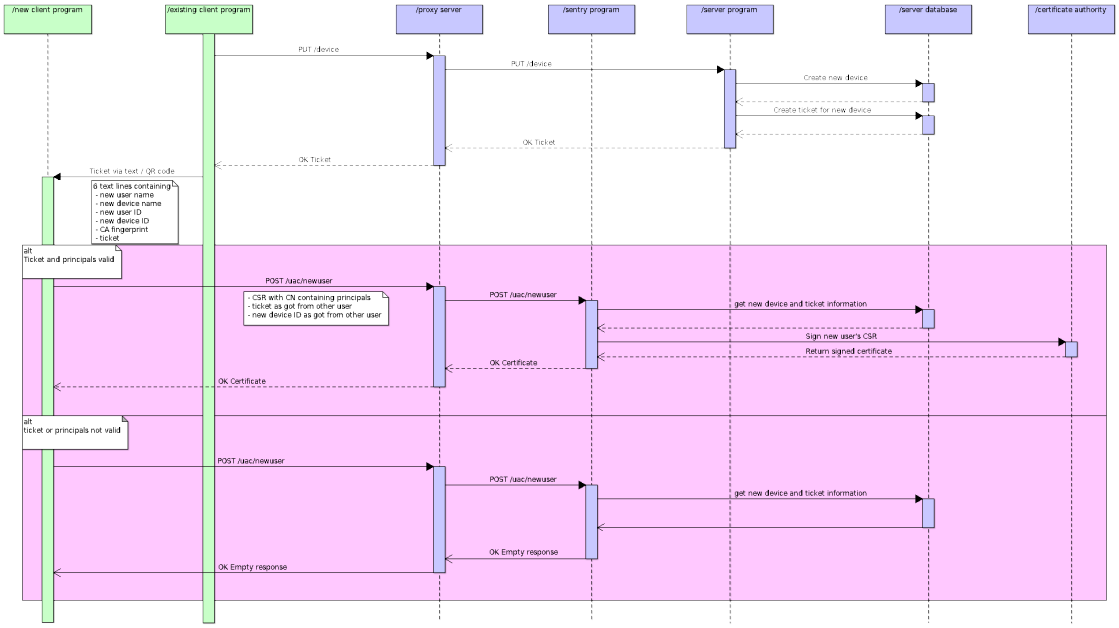


2.3.2 Refresh client database



2.3.3 New user registration

New users are always added by giving a ticket from an existing user. The details are outlined in the diagram.



Principal Names In the CSR the user stores the principals of his device. The values are formatted inside the Common Name attribute of the CSR. The pattern is `username$user_id$devicename$device_id`. So for the default test user this resolves to `John$1$Device$1`. The principals are checked in the sentry part of the server before the certificate is signed.

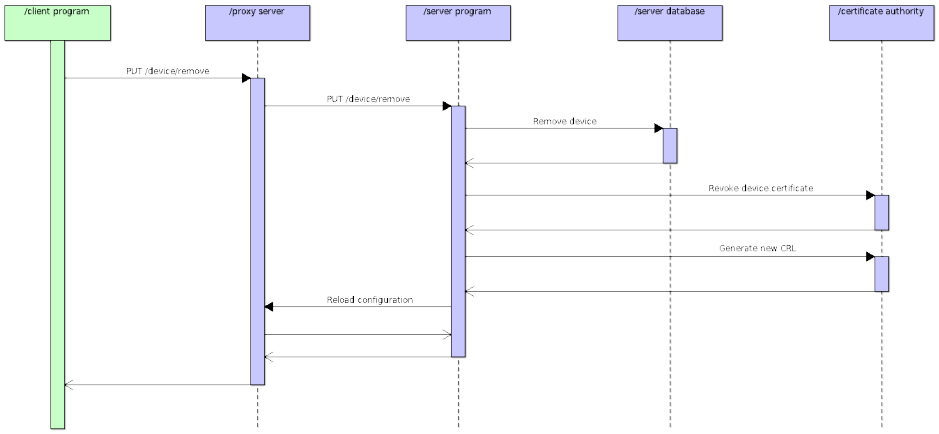
Client Verification Upon receiving a new device registration request, the sentry performs the following checks in order:

- Check if the ticket value presented by the client is found in the database
- Check the device id associated with the ticket from the database with the device id from the CSR
- Check if the remaining principals of the device match the CSR
- Check if the ticket has expired

If all the checks succeed the sentry has the CSR signed by the CA and returns it to the client.

QR Code Tickets For mobile clients it is more convenient to pass the ticket as QR code. To generate this QR code the content of the ticket has to be entered text into the QR code. The order of the values is the same as in the diagram description.

2.3.4 Device removal



2.4 Security