Stocks Specification

Jan Veen
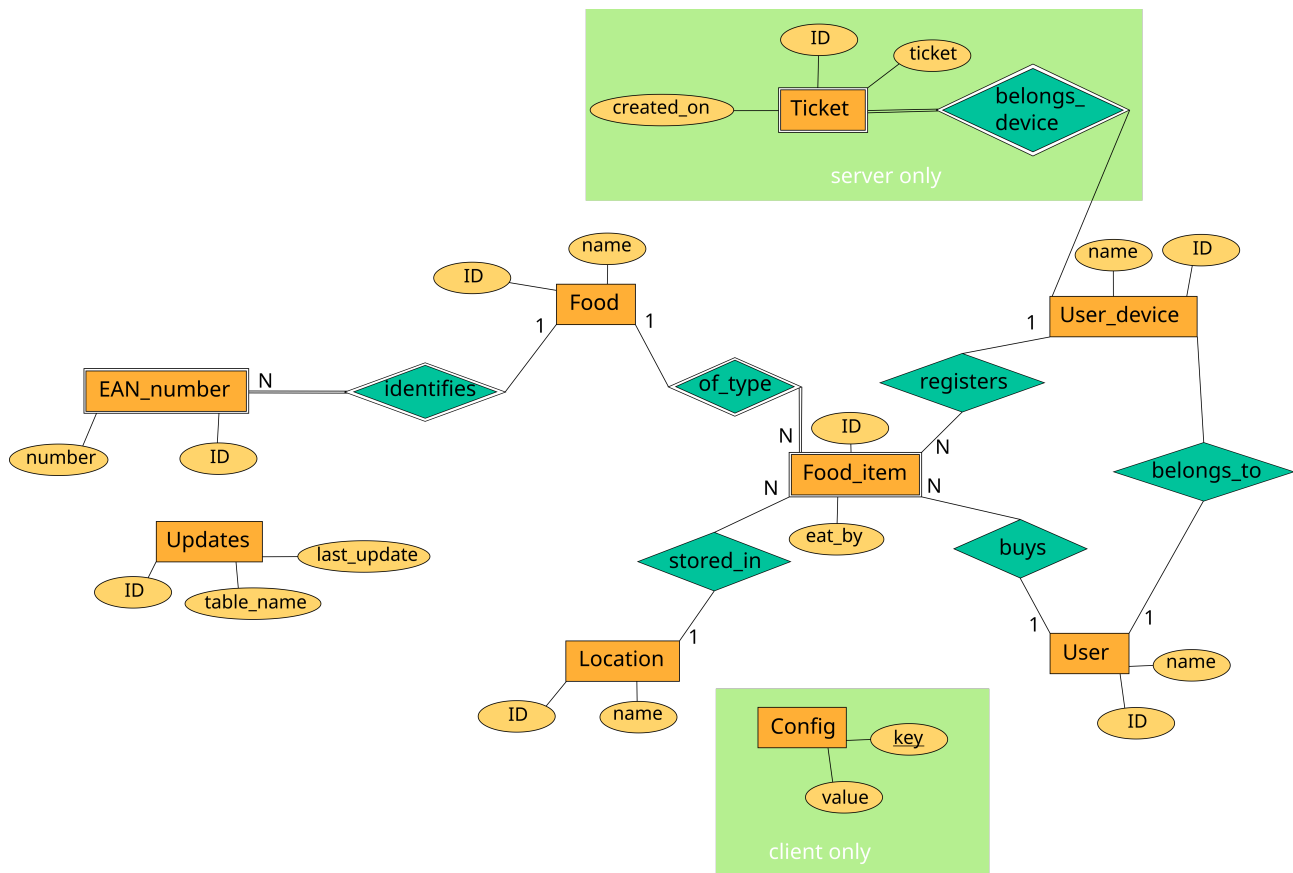
September 25, 2017

Contents

Chapter 1

Data Model

1.1 Date formats

What date format is used in which part of the system:

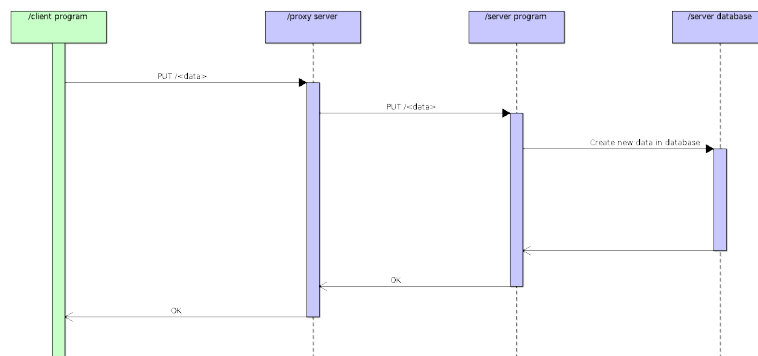| Location	Format
Client code	Localtime
Client database	Localtime
Network	UTC
Server code	UTC
Server database	UTC

Chapter 2

Architecture

2.1 Used Software
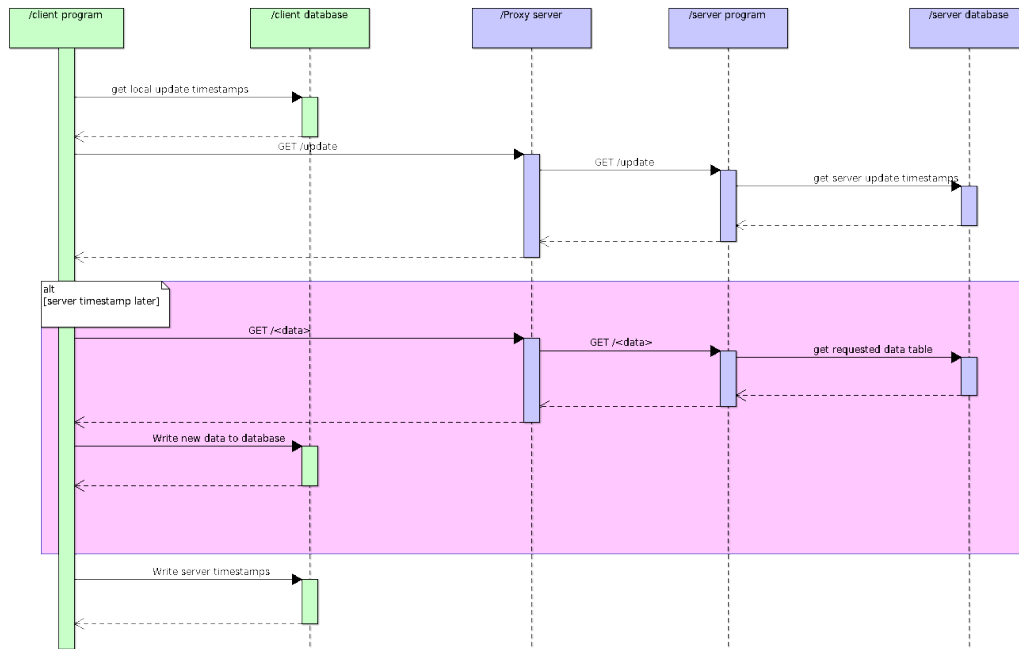
2.2 Server

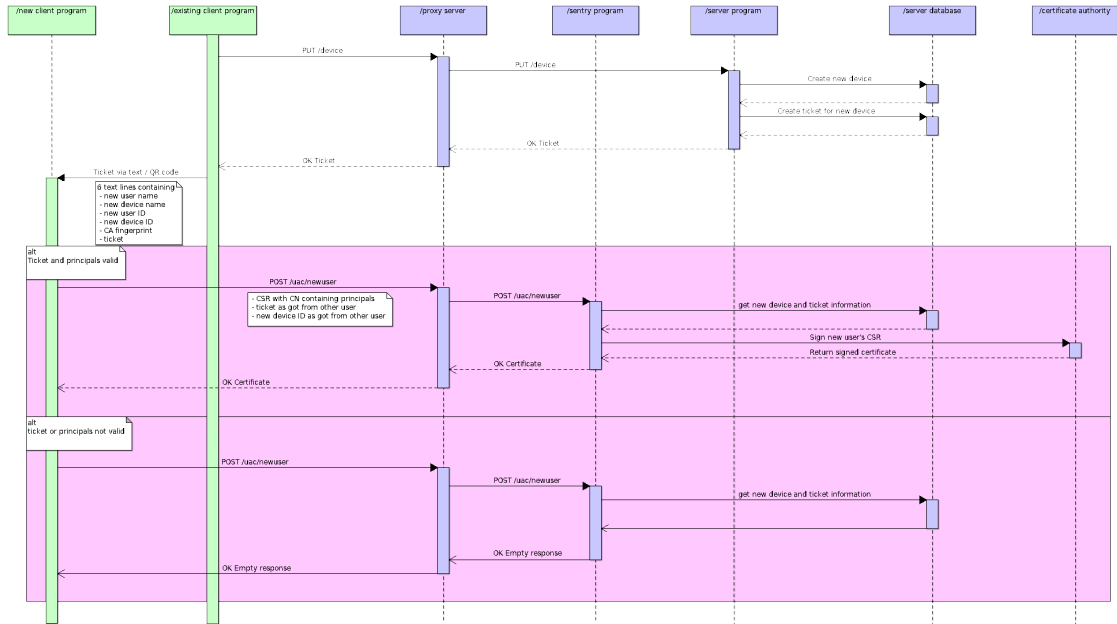## 2.3 Client

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.

Diagram participants: /new client program, /existing client program, /proxy server, /sentry program, /server program, /server database, /certificate authority

PUT /device
PUT /device
Create new device
Create ticket for new device
OK Ticket
OK Ticket
Ticket via text / QR code

6 text lines containing
- new user name
- new device name
- new user ID
- new device ID
- CA fingerprint
- ticket

alt [Ticket and principals valid]
POST /uac/newuser
- CSR with CN containing principals
- ticket as got from other user
- new device ID as got from other user
POST /uac/newuser
get new device and ticket information
Sign new user's CSR
Return signed certificate
OK Certificate
OK Certificate

alt [ticket or principals not valid]
POST /uac/newuser
POST /uac/newuser
get new device and ticket information
OK Empty response
OK Empty response

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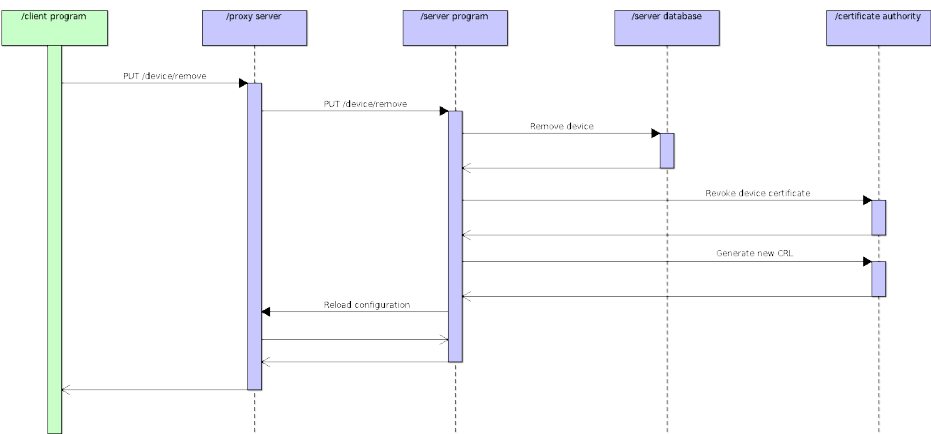
Client Verification Upon receiving a new device registration request, the sentry performs the following checks in order:

- 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