

Personalized Shopping Assistant

Team 4

Thomas Ripp

Joseph Mirabile

Jose Cruz

Stevens Institute of Technology

April 16, 2021

Contents

1	Terms, definitions and abbreviated terms	2
1.1	Terms and Definitions	2
1.2	Abbreviated Terms	3
1.3	Assumptions and Dependencies	4
1.4	Operating Environment	6
2	System Requirements	7
2.1	Personal Shopper	7
2.2	Personal Shopper Merchant	9
2.3	Personal Shopper Driver	10
3	Security Requirement	12
4	Quality Attributes	14
4.1	Availability	14
4.2	Installability	14
4.3	Interoperability	14
4.4	Performance	15
4.5	Reliability	15
4.6	Robustness	15
4.7	Usability	16
4.8	Efficiency	18
4.9	Modifiability	18
4.10	Portability	19
4.11	Reusability	20
4.12	Scalability	20
4.13	Verifiability	20
4.14	Constraints	21

1 Terms, definitions and abbreviated terms

1.1 Terms and Definitions

- **OAuth:** Authentication protocol that allows one application to interact with another one on behalf of the first one.
- **Firebase Cloud Messaging:** Cross-platform message and notification solution developed by Google.
- **Customer:** Type of user who is going to search and create order by purchasing products from merchants
- **Merchant:** Store that uploads products to the platform, from which the customers are going to purchase
- **Driver:** User that fulfills the order generated by the customer
- **Order:** A list of items that was paid by the customer and fulfilled by the driver.
- **Cart:** Container that temporarily holds a group of products that are going to be purchased.
- **Estimated time of Arrival:** The amount of time that an order is going to take before arriving to the customer.
- **Interaction:** Amount of touches required by the user to perform an action, if the device has a touch screen, or the amount of clicks a user performs, if the device has a non-touch screen.
- **2FA:** Authentication methods in which a particular device is used to grant access to a website or application, if two or more pieces of evidence confirm the user identity.

1.2 Abbreviated Terms

Abbreviation	Term
PSS	Personal Shopper System
PSMS	Personal Shopper Merchant System
PSDS	Personal Shopper Driver System
PSSS	Personal Shopper Server System
FCM	Firebase Cloud Messaging
ETA	Estimated time of Arrival
2FA	2-Factor Authentication

1.3 Assumptions and Dependencies

- AS-1 The drivers are already sign up in the system when they send their driver application to the company
- AS-2 The merchants are added into to the system outside of the application scope
- AS-3 The merchants are going to submit products that are appropriate for all ages. *They are not going to upload drugs, guns, medical devices*
- AS-4 The merchants are already sign a contract that specify the types of products they can add in the platform
- AS-5 Customers do not have support for 2FA
- AS-6 Merchants required 2FA
- AS-7 Drivers have 2FA as an option
- AS-8 A driver session can only run on one device at a time
- AS-9 PSS, PSMS, PSDS only talk with PSSS, using a request-response approach.

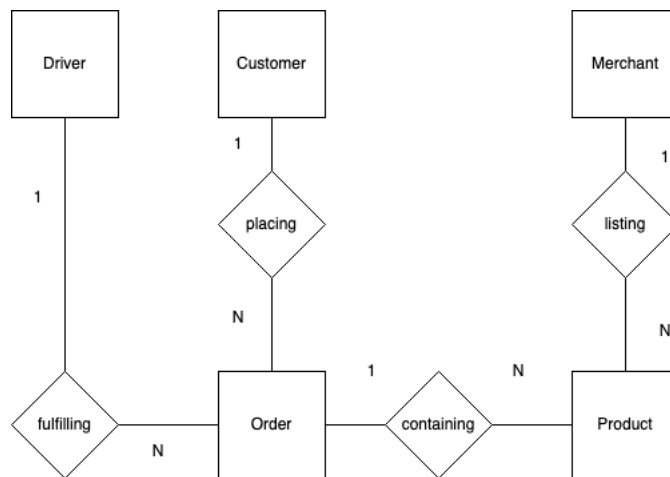


Figure 1: Logical Data Model

AS-10 Merchants have no more than 5 employees

AS-11 All the merchants, costumers and drivers operate inside the Hoboken area

AS-12 PSS have two versions mobile which is Android and a Web version

AS-13 PSMS has only a web version

AS-14 PSDS has only an Android version

AS-15 PSSS is an API server only

AS-16 Notifications in PSS (Mobile/Web) and PSDS are going to use FCM

1.4 Operating Environment

OE-1 The PSSS is going to run on AWS infrastructure

OE-2 Image assets are going to be stored in AWS S3

OE-3 New servers are going to be spin up on demand using EC2 VMS

OE-4 The PSSS can only be accessed by PSS, PSMS, PSDS

OE-5 Network requests coming from outside of US are going to be ignored

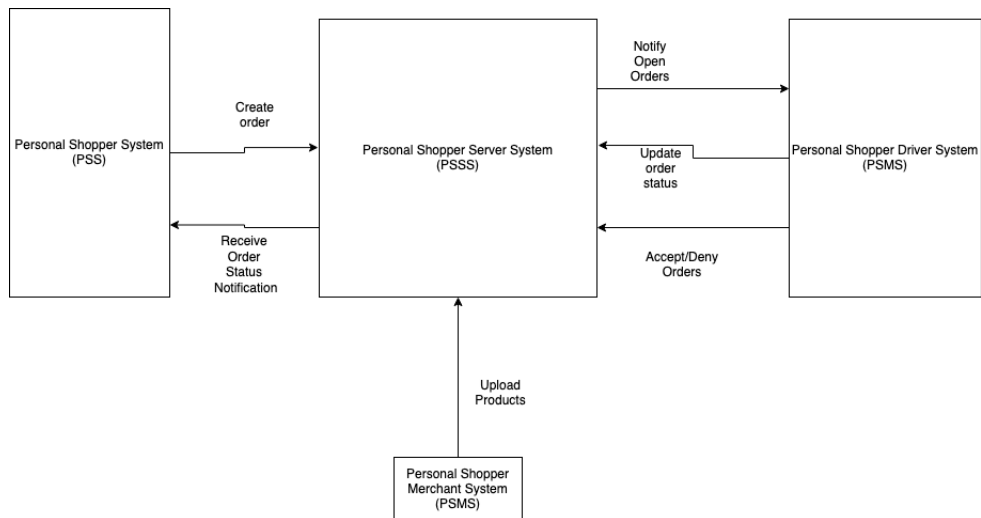


Figure 2: Context Diagram

2 System Requirements

2.1 Personal Shopper

SY-1 PSS shall enable a customers to register by requesting the following fields:

- Name
- Last name
- Phone number
- Email
- Password

SY-2 PSS shall enable customers to signup into the platform by using authorized public OAuth implementation:

- Google
- Apple

SY-3 PSS shall enable customers to login into the platform by using email and password

SY-4 The PSS shall enable customers to login into the platform by using authorized public OAuth implementation:

- Google
- Apple

SY-5 PSS shall enable customers to close an existing session

SY-6 PSS shall display a list of all the available merchants

SY-7 PSS shall display what is the customer current location inside a map

SY-8 When the customer is inside a merchant page, PSS shall enable the customer to search a product

- PSS shall display a list of products that show the name, image and short description that matches a search

- SY-9 PSS shall enable customers to add a product to the cart
- SY-10 PSS shall enable customers to add their payment information into the platform
- SY-11 When the cart has one or more items, PSS shall permit the user to create an order
- SY-12 PSS shall permit customer to cancel an order
- SY-13 PSS shall permit customer to confirm that they received an order
- SY-14 If the customer forgets its password, PSS shall request to user to enter its email address and shall an email with a temporary password
- SY-15 If there is an issue with an order, PSS shall enable customers to open an ticket about the order
- SY-16 PSS shall enable user to send a message to the driver
- SY-17 PSS shall display drivers information:
- Phone Number
 - Name
 - Profile Picture
- SY-18 PSS shall display the ETA from a pending order
- PSS shall display the ETA in terms of minutes
- SY-19 PSS shall display merchants information
- Name
 - Phone
 - Email
 - Address

2.2 Personal Shopper Merchant

SY-20 PSMS shall enable merchants to login into the platform by using email and password

SY-21 PSMS shall enable merchants to close an existing session

SY-22 PSMS shall enable merchants to add a product, by requesting the following required fields.

- Name
- Description
- Picture
- Weight

SY-23 PSMS shall enable merchants to update a selected product

SY-24 PSMS shall enable merchants to delete a selected product

- PSMS shall display a message dialog that request a confirmation from the merchant

SY-25 PSMS shall enable merchants to disable a product

SY-26 PSMS shall enable merchant to enable products that were previously disabled

SY-27 If the merchant forgets its password, PSMS shall request to user to enter its email address and shall an email with a temporary password

2.3 Personal Shopper Driver

- SY-28 The PSDS shall enable merchants to login into the platform by using email and password
- SY-29 The PSDS shall enable merchants to close an existing session
- SY-30 If the driver forgets its password, PSMS shall request to user to enter its email address and shall an email with a temporary password
- SY-31 If the driver receives an order requests, PSDS shall request to press a button with the title "Accept" to accept an order
- SY-32 If the driver receives an order requests, PSDS shall request to press a button with the title "Decline" to accept an order
- SY-33 If the driver already accept an order, PSDS shall enabled the user to decline the order
- SY-34 PSDS shall enable the driver to mark an order as delivered
- SY-35 If the driver mark an order as delivered, PSDS shall request the user to take a picture of the delivery.
- SY-36 PSDS shall enable the driver to press a button that sends a signal to PSSS that notifies to the customer that the driver it's on its way to the merchant
- SY-37 PSDS shall enable the driver to press a button that sends a signal to PSSS that notifies to the customer that the driver it's at the merchant and it's working in the order
- SY-38 PSDS shall enable the driver to press a button that sends a signal to PSSS that notifies the customer that the driver it's on its way to the deliver the order to the customer
- SY-39 If the driver requires to reach out to the driver, PSDS shall display the phone number of the customer

SY-40 PSDS shall display a list of all the orders that the drivers performer in the last 30 days

SY-41 PSDS shall display what is the driver current location inside a map

SY-42 If the driver requires technical support, PSDS shall display a technical support phone number

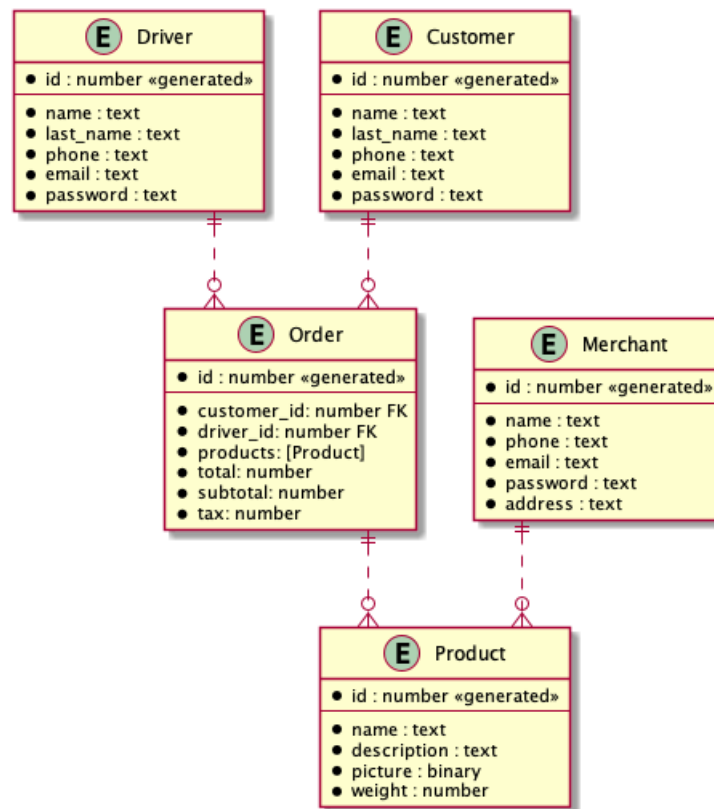


Figure 3: Data Model Diagram

3 Security Requirement

- SEC-1 The PSS shall require an email and password access to log in
- SEC-2 PSS password must no less than 8 characters, 1 special character, and 2 numbers.
- SEC-3 The PSS shall not store passwords in plain text, it shall salt the passwords and encrypt using SHA-2 algorithm
- SEC-4 The PSS shall display an error message in the case of a failure in a transaction in order to protect customer data
- SEC-5 The PSS shall allow customers to file any reports with their orders by sending an email to the support email address with the order number and issue details.
- SEC-6 The PSS shall ask the customer whether or not their order has arrived if it is 1 hour after they create the order
- SEC-7 The PSS shall allow users to delete their own account, this is also shared with the PSMS and the PSDS
- SEC-8 The PSS shall allow users to disable their own accounts for a certain period of time up to 1 year
- SEC-9 The PSS shall not store any credit card information, it will use an authorized, PCI Compliant, provider. (PayPal).
- SEC-10 The PSS shall ignore all network request that comes outside of US.
- SEC-11 The PSSS shall log all information regarding the server status into a log file.
 - SEC-11.1 PSSS shall log the utilized RAM every 5 minutes
 - SEC-11.2 PSSS shall log the utilized CPU every 5 minutes
 - SEC-11.3 PSSS shall log all search queries

SEC-12 PSSS shall consider that a request is coming from a secure environment if the communication protocol is HTTPS and a valid JWT is sent in 'Authorization' header

SEC-13 A security audit shall be performed in all the dependencies that are added to the project

SEC-14 A system security audit should be performed each year

SEC-15 The PSD shall have a 2 factor authentication procedure as an option

SEC-16 PSMS requires 2FA procedure for authentication

SEC-17 The PSD shall only allow the driver to log in from one device at a time

4 Quality Attributes

4.1 Availability

- AVL-1 The PSSS shall be available at least 99.9% during holidays, from 01:00 AM to 23:59 PM
- AVL-2 The PSSS shall be available at least 99% during the day on regular days (days that are not holidays), from 9:00 AM to 7:00 PM.
- AVL-3 The PSSS shall be available at least 90% during the night on regular days (days that are not holidays), from 01:00AM to 8:59 AM and from 7:01 PM to 11:59 PM.

4.2 Installability

- INS-1 The PSS (Mobile) should be installed from Google Play Store
- INS-2 The PSDS (Mobile) should be installed from Google Play Store
- INS-3 Installing PSSS requires that a trained operator perform the installation

4.3 Interoperability

- IOP-1 The PSS shall be able to exchange data with PSSS via HTTPS
- IOP-2 The PSDS shall be able to exchange data with PSSS via HTTPS
- IOP-3 The PSMS shall be able to exchange data with PSSS via HTTPS

4.4 Performance

PER-1 The PSSS (Web) shall take no longer than 2s when loading a page.

PER-2 The PSSS (Mobile) shall take no longer than 3s when loading a view.

PER-3 The PSSS shall take no longer than 2 seconds when searching for products.

PER-4 The PSSS shall take no longer than 5 seconds when the customer pay for the order.

PER-5 The PSSS shall take no longer than 5 seconds when the customer log in.

PER-6 The PSSS shall take no longer than 3 seconds to logout.

PER-7 The PSDS shall take no longer than 3 seconds to accept an order.

PER-8 The PSDS shall take no longer than 3 seconds to reject an order.

4.5 Reliability

REL-1 No more than 5 orders out of 1,000 can be lost due to software errors.

REL-2 The PSSS shall not be down for more than 3600 consecutive seconds.

4.6 Robustness

Offline means the software is running but it lose internet connections with the application server.

ROB-1 If PSDS goes offline, it will try to reconnect to PSMS in intervals of 10 seconds.

ROB-2 If a message is sent from PSDS to PSSS and PSDS is offline, PSDS is going to store the message in a queue and send the message when it reconnects.

- ROB-3 If a message is sent from PSS to PSSS and PSS is offline, PSS is going to store the message in a queue and send the message when it reconnects.
- ROB-4 PSDS, PSS, PSMS shall have empty input fields by default and display an error message in case a required input field is empty.

4.7 Usability

Supported OAuth accounts: Google, Facebook, Apple.

For the context of usability a workflow is going to be any combination of views, buttons, actions and inputs that helps a user to achieve a goal.

- USE-1 A first time user of PSS shall be able to create an order, with a cart already filled, in no longer than 3 seconds
- USE-2 A first time user of PSS shall be able to sign up in no longer than 2 minutes
- USE-3 A first time user of PSS shall be able to sign up in no longer than 20 seconds, if the user have a supported OAuth account
- USE-4 A first time user of PSS shall be able to sign in no longer than 5 seconds
- USE-5 A first time user of PSS shall be able to sign in no longer than 3 seconds, if the user have a supported OAuth account
- USE-6 A first time user of PSS shall be able to search for an item and add it to the cart in no longer than 20 seconds
- USE-7 A first time user of PSDS shall be able to sign in no longer than 5 seconds
- USE-8 A first time user of PSDS shall be able to accept an order in no longer than 10 seconds

- USE-9 A first time user of PSDS shall be able to deny an order in no longer than 10 seconds
- USE-10 A first time user of PSDS shall be able to logout in no longer than 5 seconds
- USE-11 A first time user of PSDS shall be able to mark that it's on its way to the merchant store, in no longer than 3 seconds
- USE-12 A first time user of PSDS shall be able to mark that it's on its way to the costumer, in no longer than 3 seconds
- USE-13 A first time user of PSMS shall be able to add a new product in no longer than 2 minutes.
- USE-14 A first time user of PSMS shall be able to remove a product in no longer than 15 seconds.
- USE-15 A first time user of PSMS shall be able to update a product in no longer than 1 minute
- USE-16 A first time user of PSMS shall be able to login in no longer than 5 seconds
- USE-17 A first time user of PSMS shall be able to logout in no longer than 5 seconds
- USE-18 A single workflow would be consider user-friendly as long as the user makes 4 mistakes or less out of 100 times repeating the same workflow. *A mistake is any action that the user performs that he didn't intent to (E.g. Button miss clicks, invalid characters on input fields, wrong text format)*
- USE-19 For the systems PSMS, PSS, PSDS, 98% of first time users should be able to use the applications without needing any help.
- USE-20 A user of PSS should be able to create an order from an already filled car in no more than 4 interactions
- USE-21 A user of PSS should be able to create an order from an empty cart in no more than 8 interactions. For an order of a single item.

- USE-22 A user of PSDS should be able to complete a delivery in no more than 2 interactions
- USE-23 A user of PSDS should be able to signal a customer that it's on its way to the store in no more than 2 interactions
- USE-24 A user of PSDS should be able to signal a customer that it's on its way to the complete the order in no more than 2 interactions
- USE-25 A user of PSMS should be able to add a product in no more than 2 interactions
- USE-26 A user of PSMS should be able to update a product in no more than 2 interactions
- USE-27 A user of PSS should be able to edit their own profile in no more than 2 interactions

4.8 Efficiency

- EFF-1 The PSSS should have at least 30% of processor capacity and memory available to the application shall be un-used at the planned peak load conditions

4.9 Modifiability

- MOD-1 Classes must follow the SOLID principles
- MOD-2 Functions calls required at least 80% of testing code coverage
- MOD-3 Public functions must be above protected functions
- MOD-4 Protected functions must be above private functions
- MOD-5 All merges to master must come from the CI server
- MOD-6 All test must pass before pushing changes to the remote repository
- MOD-7 All changes push to a release branch must be peer-reviewed.
- MOD-8 Public and protected functions must include a comment that explains the functionality

- MOD-9 Variable must be descriptive in nature, abbreviations must be avoided
- MOD-10 Constants must be all uppercase, if the constant have more than one word they would be separated by an underscore
- MOD-11 Functions and variables must begin with a lower case
- MOD-12 Classes will be capitalize
- MOD-13 Variables and functions must be written in camel case
- MOD-14 Composition must be preferred over inheritance
- MOD-15 Lines would not exceed more than 80 characters, including white spaces
- MOD-16 Code format should be applied before committing

4.10 Portability

- POR-1 Modifying the Android version to the latest version shall require changing no more than 5% of the source code
- POR-2 PSMS, PSS (Web) shall support:
- Chrome 89, 88, 87
 - Latest version of Safari
 - Firefox 87, 86, 85
 - Microsoft Edge 89, 88, 87
- POR-3 PSDS, PSS (Mobile)
- Android 12, 11, 10

4.11 Reusability

- REU-1 Web components must be reused between PSS (Web) and PSMS.
- REU-2 Authentication mechanism must be shared between PSS (Mobile) and PSDS
- REU-3 At least 45% of application architecture shall be reused between PSS (Mobile) and PSDS.
- REU-4 2FA (2-Factor Authentication) mechanism shall be shared across all the systems
- REU-5 JWT token signing and token rotation mechanism shall be shared across all the systems

4.12 Scalability

- SCA-1 The system should scale up the system horizontally, if the system gets 95% of CPU or RAM utilized, which ever comes first. The system will spin up 2 servers with the same operating system and environment but with 80% less memory than the original server.
- SCA-2 The system will scale down to 1 (original server) if the one of the previous spin up server, has less than 95% of CPU usage during 3600 consecutive seconds.

4.13 Verifiability

- VER-1 The staging environment configuration shall be identical to the production configuration environment to avoid irreproducible testing failures.
- VER-2 A tester shall be able to configure if the application is running in testing, develop or production mode

4.14 Constraints

- CON-1 Developers can only use open source libraries or tools that are either Apache or MIT license.
- CON-2 Google Pay and Apple Pay are the only supported payment providers
- CON-3 The data interchange format must be JSON
- CON-4 The authentication/authorization mechanism between applications is going to be JWT
- CON-5 JWT tokens are going to expired after 24 hours
- CON-6 The database that is going to be used in the project must be MySQL

