CLOUD4RETAIL OmniPOS SAP Endorsed Certified

Self Scanning Add-On

Version: 5.23.0

COPYRIGHT

INHALT

- Product Description – Self Scanning Client

- Product Description – Self Scanning Backend

- Product Description - Employee App

- Product Description – Wall Device Manager

- Release Notes – Self Scanning Client (Industrial Device & SDK)

- Release Notes – Self Scanning Backend

- Release Notes – Employee Hub

- Release Notes – Wall Device Manager

- User Guide - Employee App

- User Guide – Self Scanning Client (Industrial Device)

- User Guide – Wall Device Manager

1 Product Description – Self Scanning Client (Industry scanning device)

1.1 Introduction ("Big Picture")

This document describes the Self Scanning product of the GK/Retail Business Suite.

The Self Scanning Client enables a customer to scan and enter items unaided by a cashier while wandering through the store and finish their shopping trip on their own. The customers always know the value of their current virtual shopping basket, which saves time during checkout, and they can access images/pictures of the products. The Self Scanning Client from GK Software helps employees in retail businesses to cater for customer needs more extensively. The Self Scanning Client increases customer throughput.

The Self Scanning Client has a simple interface, where the customer has access to a well-structured virtual shopping basket, which lists all the items (with a picture) from the real shopping basket in an easy to grasp way and calculates the final price at all times. As a final step, the customers have the option to pay for their shopping basket by transferring the virtual shopping basket to the POS in the store, where the payments can be handled.

1.2 Scope and Functions

The key features of the Self Scanning product are summarized in the following paragraphs.

1.2.1 Industry Scanning Device

The current solution supports item entry using an industry scanning device (handheld) running the Android operating system. Currently, the PS20 Personal Shopper and the Symbol MC18 Personal Shopper, both from the retail mobile computer manufacturer Zebra, are supported as Self Scanning devices. The device includes an "intelligent cradle". It is possible to define a unique number for each cradle, a cradle zone and maintain further data centrally. The handheld device communicates with the cradle via a USB connection. For more technical information about the supported industry scanning devices, visit the Zebra product websites: www.zebra.com/ps20 and www.zebra.com/mc18.

1.2.2 Offline Capability

The Self Scanning Client is fully offline compatible (except for the display of item images; these are not available offline). If the network connection fails during the shopping trip in the store, the Self Scanning Client falls back on the internal offline database. The internal offline database gets downloaded and updated

each time that the customer connects the Self Scanning Client to the store network to make sure that the internal offline database is always as up-to-date as technically possible. Images/pictures of the items are not available offline.

2 Product Description – Self Scanning Backend

2.1 Introduction

GK Software is a leading provider of retail applications for real-time omni-channel business.

One of these is the Self Scanning module. By using the Self Scanning module, customers can use their own mobile device to scan item barcodes in the shop, create and maintain a virtual basket, and perform a fast checkout at the end of the trip. Additional scanning at a Point of Sale (POS) is no longer necessary.

It is possible to perform the checkout in multiple ways: At a POS, Pay Tower or Paystation, or also using a mobile phone in combination with a frictionless checkout. To do so, a payment service provider can be connected in order to pay for the transaction with tender types that the user registered and defined in advance.

The Self Scanning itself can be performed in two ways:

- Using an industrial device, which is provided to the customer in the shop
- Using the customer's own device (BYOD - Bring Your Own Device)

The Self Scanning solution provided by GK combines a set of powerful capabilities:

- Cloud backend
- Offline functionality

Self Scanning client applications will download all of the necessary information during the start of trip to the local storage. During the shopping trip, the client does not need to have an internet connection. Customers are able to scan item barcodes and will get all of the item information directly from the offline master data. The virtual basket is saved locally.

Once the customer finalizes the shopping trip, the client will perform a so-called "end of trip". Within this step, the offline basket will be uploaded to the backend server applications. The backend system (called the Self Scanning Service) will validate all of the scanned items, check for price modifications and check for possible fraud. The customer is informed about the result of this registration step and can continue with the payment process, either via a checkout terminal (POS) or via the in-app payment option. Once the transaction is finally paid, an exit gate can guide the customer to leave the store.

To keep the customer up-to-date with item prices during the shopping trip, the latest prices are always fetched from the backend. This is performed in the background or skipped if there is a poor internet connection in the store. The customer will not be blocked by this.

2.1.1 BYOD
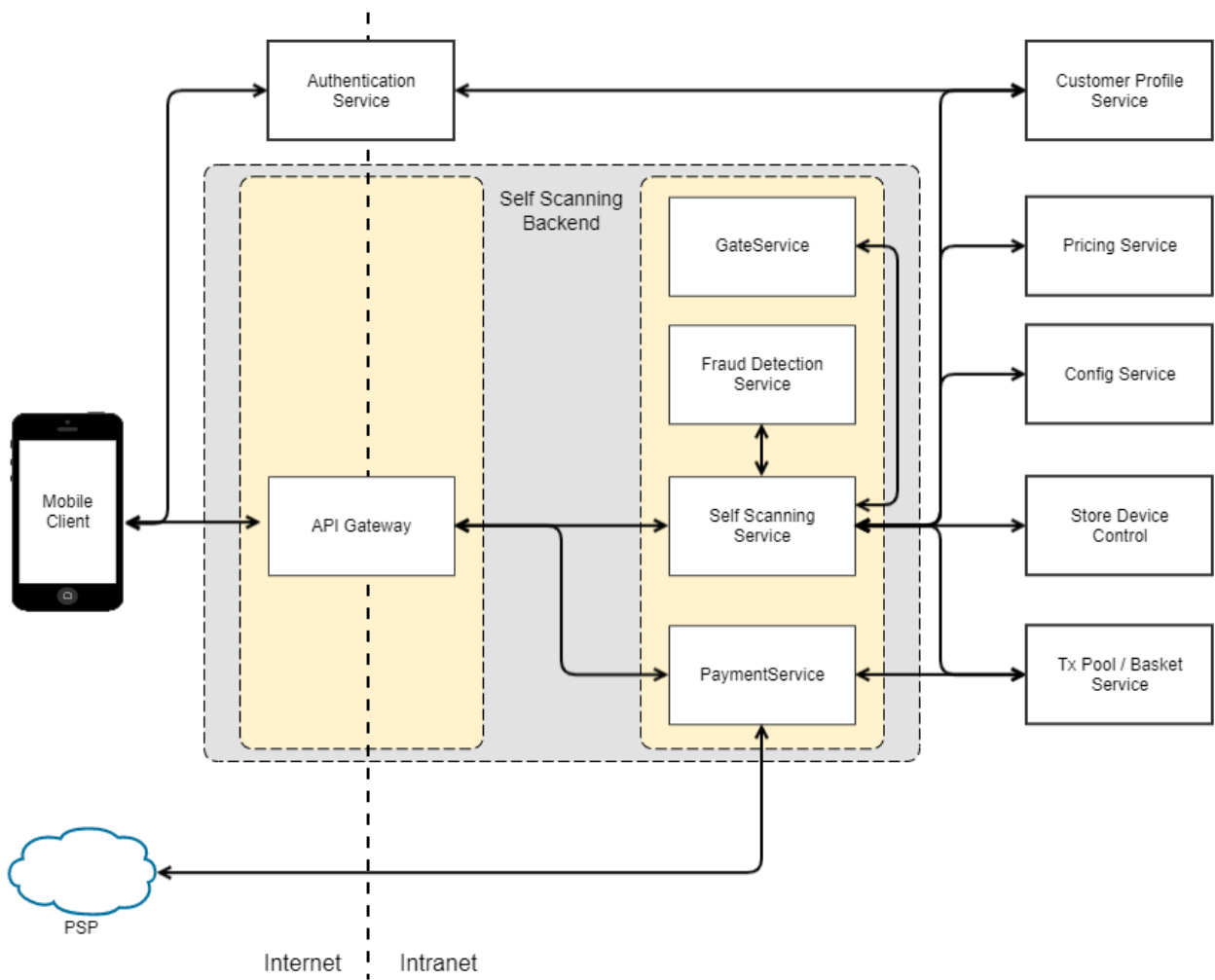
2.1.2 Industry Device
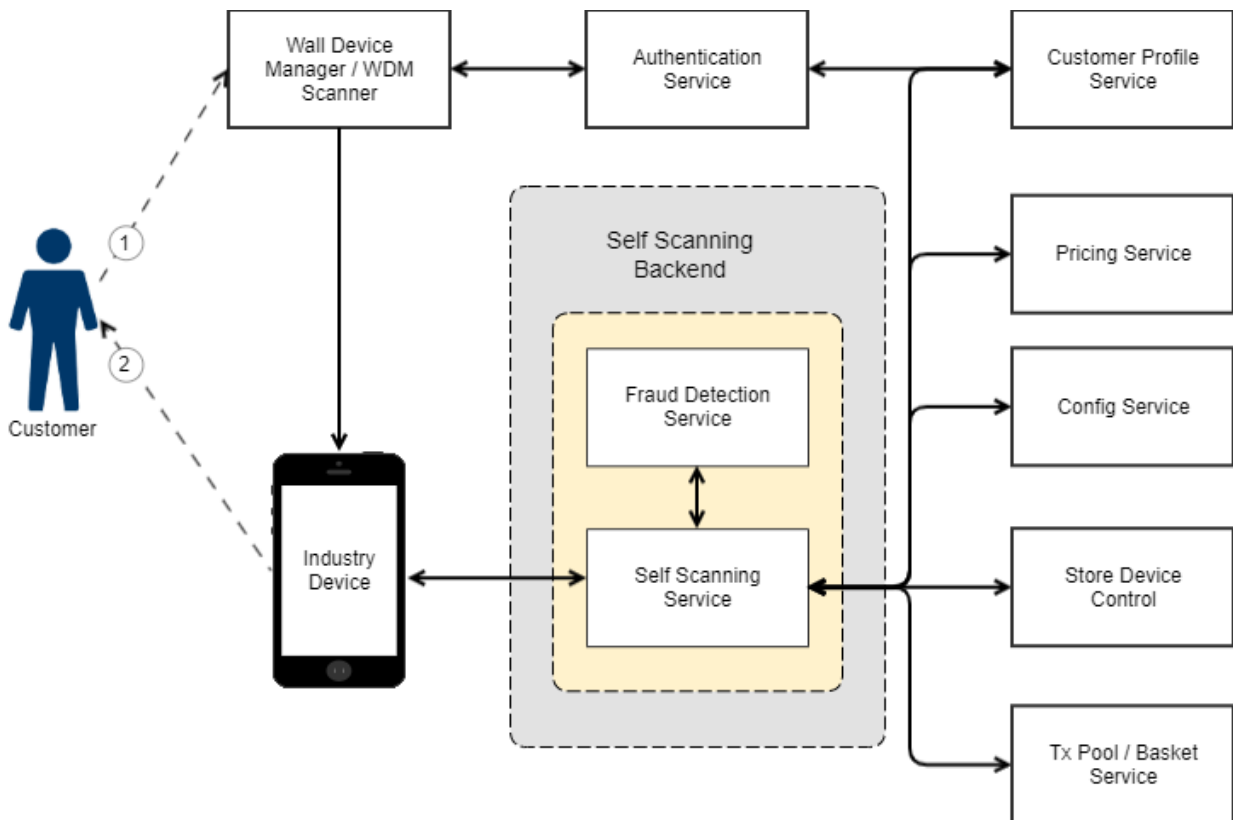
2.2 Product Bundle

The backend services provide the endpoints and functionality for the clients delivered within Self Scanning Clients bundle as well as other management applications, such as Employee App or Wall Device Manager, delivered in separate bundles. The Self Scanning Backend bundle contains the following services:

- **API Gateway** - this service is the central endpoint for any communication from the internet to the other GK services. It validates the incoming requests and forwards them to servers hosting the correlated service.

- **Self Scanning Service** - this service is the primary communication partner for self-scanning devices, such as the Industry Device or Bring-Your-Own-Device application. It manages and orchestrates the login as well as the final end-of-trip procedure and prepares the transaction for payment.

- **Fraud Detection Service** - this service assesses a transaction with regards to possible fraud and evaluates the risk. The customer might be asked for a rescan before payment if this risk exceeds a certain limit.

- **Payment Service** - this service provides endpoints for a self-scanning client to handle and process payments with a Payment Service Provider. Payment with loyalty points or gift cards is provided for and possible as well. Additionally, it can also process payments performed on a third-party system to finalize a transaction.

- **Gate Service** - this service manages the checkout codes generated during the transaction finalization. Customers can scan the code presented at the client's UI when they wish to leave the store. Gate Service verifies the code and calls the appropriate gate to open.

2.3 API Gateway

A central component for communication with the backend is the API Gateway (API GW). It exposes the APIs of the main backend components (e.g. Self Scanning Service, see below) to the public internet. By using these APIs, client applications (e.g. iOS and Android BYOD applications) can use the Self Scanning functionality. The API Gateway is not just a transparent proxy. It also validates the requests and prevents

fraud. Each request sent to the API Gateway needs to include authentication headers. Only authenticated devices get access to internal components.

The API Gateway is also used to cache frequently used data, which increases the performance of the Self Scanning applications.

Use of the API Gateway is only required once the client applications are accessing the Self Scanning functionality via the public internet. When using industrial devices (e.g. MC18/PS running Android OS), it is typical that these devices are running as an in-store solution with access to a local Wi-Fi network and without direct customer authentication. This means that the API Gateway is not necessary for this use case as the industrial devices can communicate directly with the backend components.

2.4   Self Scanning Service

The Self Scanning Service provides the backend for communication with the Self Scanning Clients. This service acts as the connecting point between the Self Scanning Clients and the GK OmniPOS system of the retailer.
The Self Scanning Service enables easy integration of Self Scanning devices into the GK system landscape. Transactions created on the client can also be changed, processed and paid for on other points of service within the GK system.

The Self Scanning Service uses the GK Logging Service, which provides an endpoint for Self Scanning and other mobile clients to send activity logs to it. The logs can then be searched, visualized and analyzed by established tools such as Elasticsearch.
This monitoring enables the support to get a timely overview of the connected clients and their condition. Problems can be detected quickly, and appropriate measures can be taken.

By using the Self Scanning module, customers can use their own mobile device to scan item barcodes in the shop, create and maintain a virtual basket and do a fast checkout at the end of the trip. Additional scanning at a Point of Sale (POS) is no longer necessary.

It is possible to perform the checkout in multiple ways: At a POS, Pay Tower or Paystation, or also using a mobile phone in combination with a frictionless checkout. To do so, a payment service provider can be connected in order to pay for the transaction with tender types that the user registered and defined in advance.

The Self Scanning itself can be performed in two ways:

- Using an industrial device, which is provided to the customer in the shop

- Using the customer's own device (BYOD - Bring Your Own Device)

2.4.1   Architecture
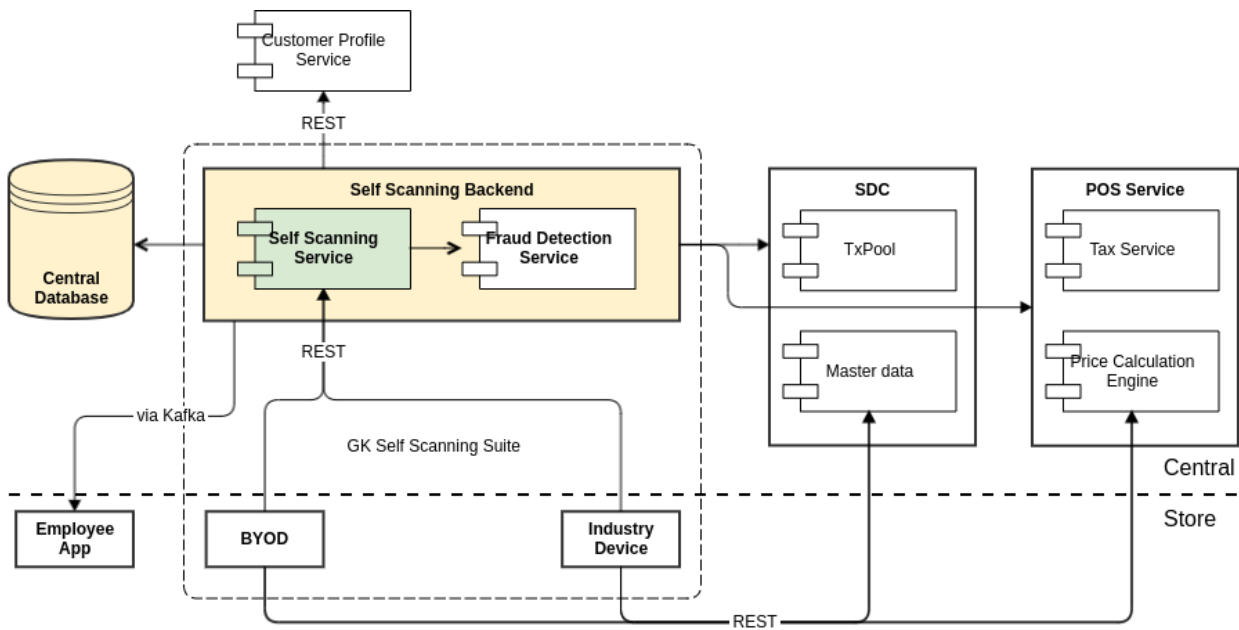
The Self Scanning solution provided by GK combines a set of powerful capabilities:

- Cloud backend

- Offline functionality

Self Scanning client applications will download all necessary information during a start of trip to the local storage. During the shopping trip, the client does not need to have an internet connection. Customers are able to scan item barcodes and will get all of the item information directly from the offline master data. The virtual basket is saved locally.

Once the customer finalizes the shopping trip, the client will perform a so called end of trip. Within this step, the offline basket will be uploaded to the backend server applications. Recalculation and validation will also be done within this step.

To keep the customer up to date about item prices, promotions etc, a recalculation of the basket is possible anytime. This can be performed in background (customer will not be blocked by this) and can be skipped in case of poor internet connection in the store.

2.4.2   Scope & Use Cases

2.4.2.1 Start-of-Trip
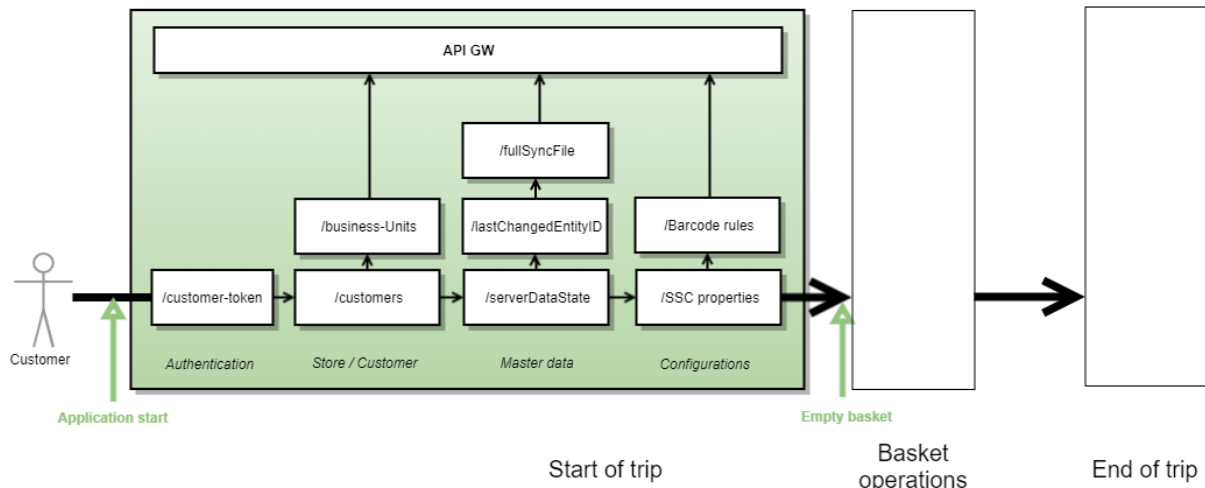
SSC_StartOfTrip

The start of trip defines all steps and requests against API Gateway, that are performed to start with the creation of a virtual (offline) basket. From a customer perspective, it summarizes everything that is happening between opening a Self Scanning client application and displaying an empty basket, where the customer can start scanning item barcodes.

The start of trip can be divided into four steps:

Steps	Description
Configurations	As one step during the start of trip, the SSC client application can download specific configurations. This can contain basket rules (e.g. item limitations) but also rules how to interpret item barcodes. Whether both steps are necessary depends on the client and requirements. It is recommend to download at least the normal SSC properties to get the latest configurations for the basket handling. GK provides a dedicated module, Barcode Processor, which can be used to interpret item barcodes. Once this module is used, it's recommended to download the barcode processor rules additionally during the start of trip. Additional config downloads are possible as well and they depend on the requirements and configuration. Details about the configuration download can be found in APIs chapter.
Download store & customer information	During the start of trip, it is necessary and useful to get all details about the selected businessUnit (shop) and the customer performing the Self Scanning trip. Downloading the businessUnit details contain properties, which are necessary for the registration process (i.e. used currency and currency symbol) as well as for the end of trip step (esp. the businessUnitGroupId). Thus, it's recommended to implement this step. The downloaded customer information contains also the flag, if the customer is applicable for in-app payment as used in end of trip. Beside that, additional customer data, such as names, can be used to improve the customer experience in the Self Scanning client application, but is optional. Details about the download of store and customer information can be found in the APIs chapter.
Master data download	This required step will download all item master data for the specific shop from the backend server. By using the serverDataState API, the client can check if a new full master data download (fullSyncFile), or just an incremental update shall be done (lastChangedEntityID). A full download could also be done on each start of trip, but it consumes more data and time than an incremental update. Details about the master data download can be found in the APIs chapter.
Authentication	This step authorizes the Self Scanning clients against the backend applications. This step is necessary for all BYOD clients, that access the API Gateway via public internet. Details about the authentication can be found in the APIs chapter.

2.4.2.2 Basket recalculation

Once a customer performsany basket operation (e.g. adding items, changing quantity of items, removing items), it is recommend to perform a basket recalculation. This will send the transaction via POS Service interface to PCE and update all prices, apply promotions etc.

The request can be processed in the background and should not block the user interface. Once a customer is offline, the request can easily be skipped. The fallback is always to display the prices which are within the offline master data.

For best practice, the requests should be queued:

- All requests shall be added to a serial queue

- The serial queue will send one request after another

- Once a recalculate response is returned, the queue needs to be cleaned up except for the latest request

- Once a recalculate response is returned and an offline basket operation happened between the request being sent and the response, the response shall be ignored (since it would overwrite the latest offline operations)

- Once a recalculate response is returned and no offline basket operation occurred, the PCE response can be used to update the offline basket
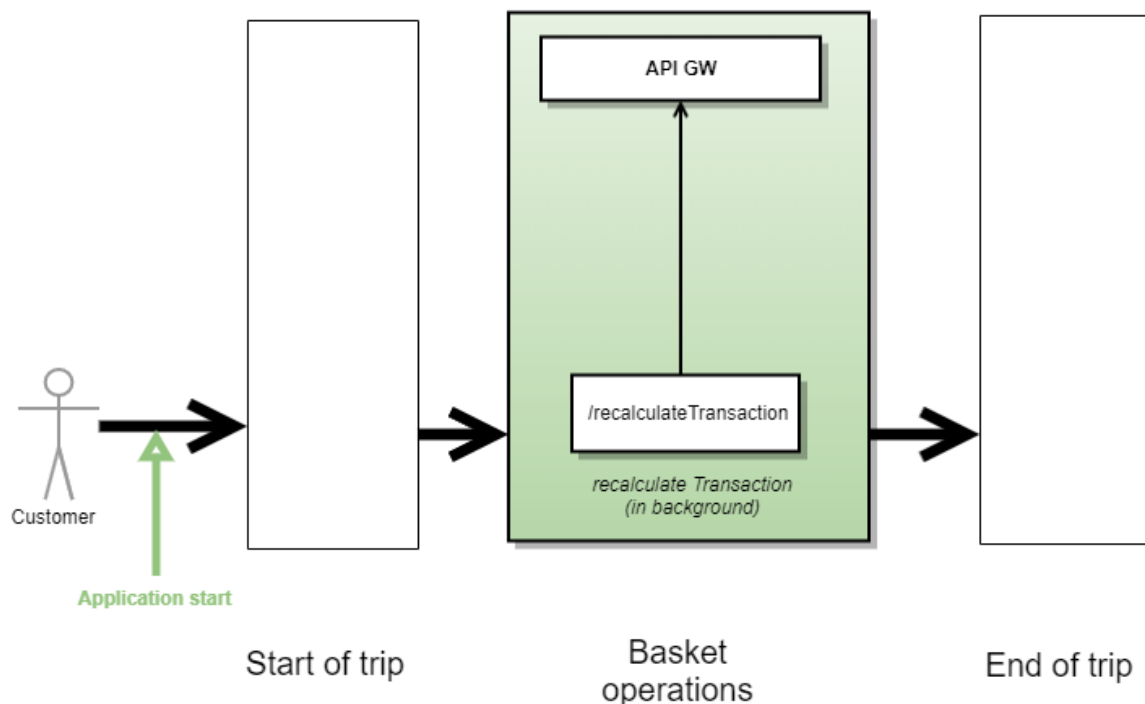
2.4.2.3 End of Trip

The end of trip is defining the step where the client application is uploading the offline basket to the Self Scanning Service. The Self Scanning Service will do several internal steps to process the transaction afterwards:

- Reload all master data and create a complete transaction

- Load the businessUnit and customer information again

- Recalculate the transaction (by calling PCE)

- Call Fraud Detection Service to check if fraud check is necessary or not

- Saving the transaction into GK transaction pool

Once the end of trip is done the Self Scanning Service will return the updated transaction information to the clients. In addition, a suspension number, if returned, which later can be used on the checkout station, to retrieve the transaction from the transaction pool.

If something fails during the end of trip or the Fraud Detection Service requests additional checks (e.g. partial or full rescan), the Self Scanning Service will return an operatorNecessary=true state. This means the

customer cannot proceed with mobile payment at this moment and needs to get in touch with a store employee.
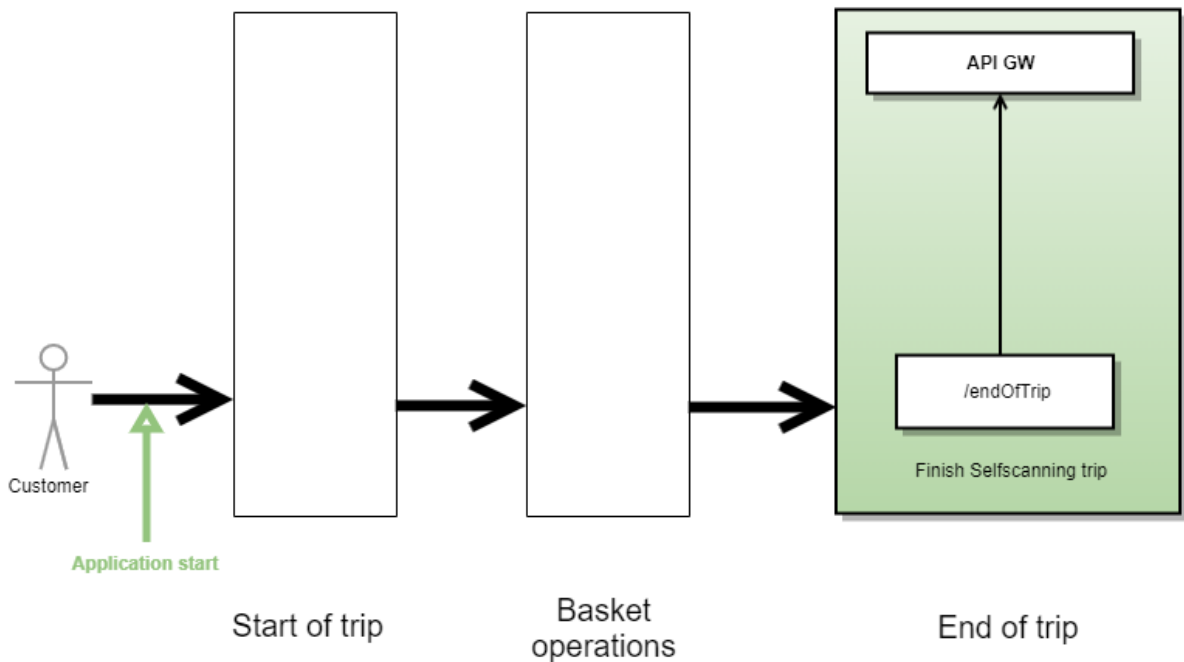
2.4.2.4 Self Scanning Special Cases

The main special cases are displayed below

Special case	Description
Void line items	It might be necessary to keep cancelled positions in a receipt for audit or process purposes. For example, the Self Scanning Service will cancel the position with the collective item after having added the merged weighted items of a scale receipt. The collective item position is kept in the response for process purposes, but will not appear on clients UI since it is marked as cancelled.
Items with sales restrictions	It might be necessary to restrict the sale of certain items, i.e. to customers of certain age. This has to be approved by a store assistant. It might also be necessary to keep items in the store master data but block them from sale completely because they are discontinued but still viable for returns. Or it might be of use for a retailer to display a message to its customers every time they register a certain item. The restrictions are checked on the client side. If a store assistant app is used, the client can send requests for manual authorization to it via Self Scanning Service. The approval is then given via this app and the result is provided back to Self Scanning Service and subsequently to the client app.
Items with deposits	Prices of some items, such as bottled beverages include some deposits which the customer can get back when they return the empty bottles. These deposits must be registered separately to be shown on the resulting receipt. Those specific deposit positions must also be linked to the correlated items.
Weight encoding / Price encoding barcodes	It is possible to encode the weight or the price of a pre-packed (weight) item into a barcode printed on the packaging of the item. This barcode can be scanned and parsed by a client app, and a corresponding item position can be created.
Items with standard promotions (CPD)	It might be necessary to restrict the sale of certain items, i.e. to customers of certain age. This has to be approved by a store assistant. It might also be necessary to keep items in the store master data but block them from sale completely because they are discontinued but still viable for returns. Or it might be of use for a retailer to display a message to its customers every time they register a certain item. The restrictions are checked on the client side. If a store assistant app is used, the client can send requests for manual authorization to it via Self Scanning Service. The approval is then given via this app and the result is provided back to Self Scanning Service and subsequently to the client app.
Promotion Recommendations	Consumers can be informed about promotions which could be applied to their baskets during a Self Scanning trip. This is especially good to know if not all conditions for the promotions are fulfilled - e.g. some items are missing from the basket. To do so, the PCE provides an option to return eventual promotions and information about the missing trigger items (items the customers must put in the basket to have the promotion applied), and about discounted items.

2.5 Fraud Detection Service

To protect the retailer from shoplifting, the Self Scanning suite offers a fraud detection function. Based on the statistical information, retailers can decide whether a customer should be subject to a partial or full rescan. The used statistics are based on item operations (e.g. removing items from the basket) or item restrictions This lowers the risk of losses due to fraud in Self Scanning processes for the retailer.

There are two variants of the fraud detection:

- Rule-Based fraud detection using a fixed rule set to assess a transaction
- Artificial intelligence fraud detection using machine learning algorithms for evaluation

A separate step to check rescan preconditions adds a possibility to react in a flexible manner to the current load and performance situation. The subsequent feedback process allows also to learn from the rescan results obtained on other GK systems.

2.5.1 Architecture
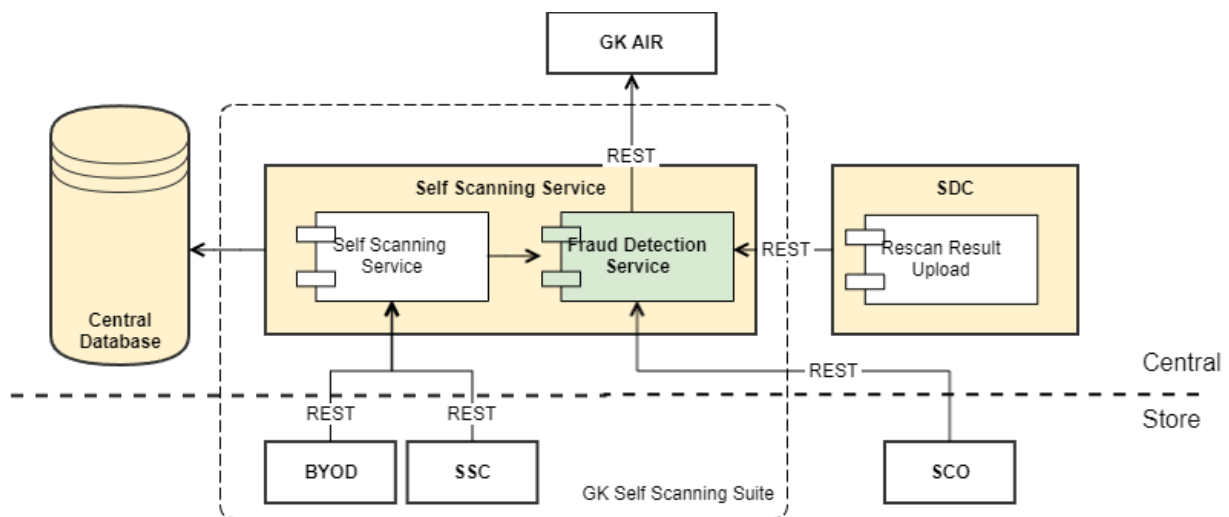
Fraud Detection Service is delivered as a service within the Self Scanning Service bundle. The integration as a service keeps the system flexible to allow enhancements to the service or even allow the used algorithms to be replaced completely.

2.5.2 Scope & Use Cases

2.5.2.1 Fraud Detection

Fraud detection takes place in self-scanning use cases during the end-of-trip procedure and thus immediately before a payment is made. The transaction is checked for fraud risk. If risk is detected, the transaction is flagged for recheck. In this case, the purchase cannot be paid until a part or the entire shopping basket is checked by a store employee.

Fraud Detection Service can be also called by self-checkout stations to assess purchases scanned there.

The fraud detection process is divided into several steps:
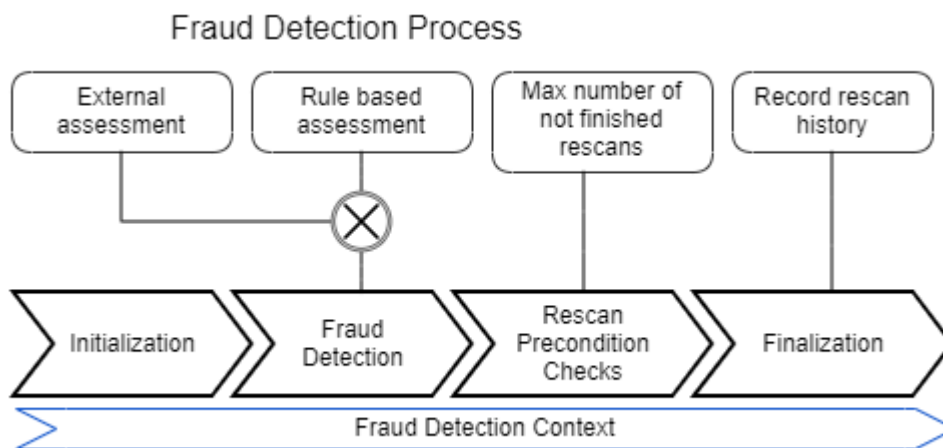
- Initialization - the first phase after a fraud detection request is received. This step prepares the context for the following fraud detection in the service

- Fraud detection - fraud detection first analyzes the probability of a fraud (rule-based fraud detection) and decides whether no rescan, partial rescan, full rescan, or critical full rescan should be performed. This assessment can be also forwarded to an external system for i.e. artificial intelligence fraud detection.

- Rescan precondition checks - if a partial or full rescan has been recommended by the assessment, a check is made to see if the rescan can be performed. This depends on the number of open rescan requests, the number of rescans within the last hour or the current working day. Critical full rescan means that full rescan is done anyway - rescan precondition checks are skipped in that case.

- Finalization - the last phase before the response is sent back. If a rescan was recommended, this data is stored to DB (rescan history)

The transactions are assessed either by applying an internal rule set or by forwarding the transaction data to GK AIR for external assessment.

Rule-Based Fraud Detection

The rule-based fraud detection uses strict rules, which can be individually configured by the retailer. A purchase of specific items or unusual usage of the Self Scanning Client, for example, can automatically trigger a shopping basket check by the shop assistant.

Artificial Intelligence Fraud Detection (Add-on)

The artificial intelligence fraud detection is an optional add-on, which unlocks additional functionality of the fraud detection. Artificial intelligence fraud detection is based on the GK AIR technology, which enables a more complex rule set and is connected to the databases and application programming interfaces (APIs) from GK AIR. An artificial intelligence enhanced rule set is a rule set that may include more external variables, such as the previous online purchase history of a customer, to trigger a shopping basket check by the shop assistant. Please check also the appropriate GK AIR documentation.

2.5.2.2 Rescan Result Processing

Fraud Detection Service provides a feedback interface to retrieve information about rescan results. This feedback information updates the internal rescan history. The results are also provided to the GK AIR system for learning and model improvement if the assessment was performed by this external system.
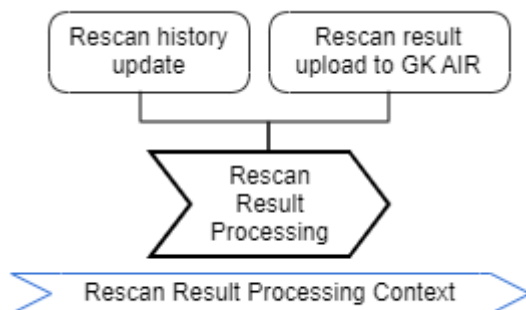
2.6   Payment Service

When using Self Scanning Clients on customer devices (BYOD), the shopper can also pay directly in this client application using their favored payment method. The client application contacts the Payment Service, which will initiate communication with an external payment provider (Adyen). In addition, this service handles communication and the transactions within the correlated GK OmniPOS environment and will inform the Gate Service about the finalization of the transaction. The Gate Service will then open the exit gate when the shopper shows the generated exit code.

Together with the Self Scanning Client, this provides a frictionless shopping experience to customers on-site in a store without involving a POS. The personnel capacities that are freed up can be used to provide customers with more advice and better service. Stationary checkout points are still available since they are integrated into the GK landscape.

Additionally to card payments, Payment Service also offers a possibility to pay by loyalty points, based on the customer's current points balance. Gift card payment is supported as well.

2.6.1   Architecture

Payment Service can be called directly by BYOD clients or indirectly via Scanless Frontend Service. To process each payment, the service communicates with the appropriate backend services. The payment service retrieves or stores the transactions either from a TxPool or from the basket service.
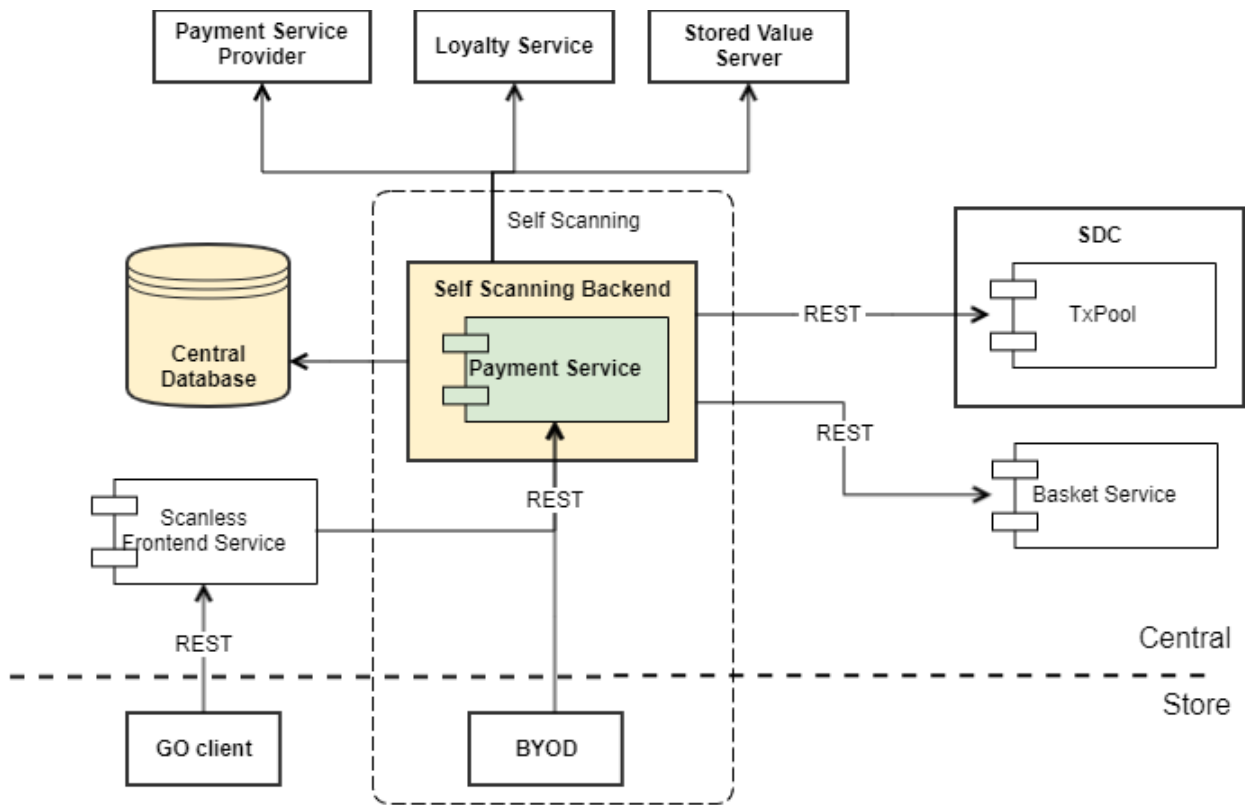
Payment Service is deployed within the Self Scanning bundle, specifically the Self Scanning backend.

2.6.2 Scope & Use Cases

2.6.2.1 In-App Payment

In-app payments are payments performed within the Bring Your Own Device client application. The PSP validates the amount to be paid and orchestrates the calls to the appropriate back-end systems for the specific payment method. In the case of credit card payments, there is a dop-in on the client side, which also uses direct communication with the PSP.
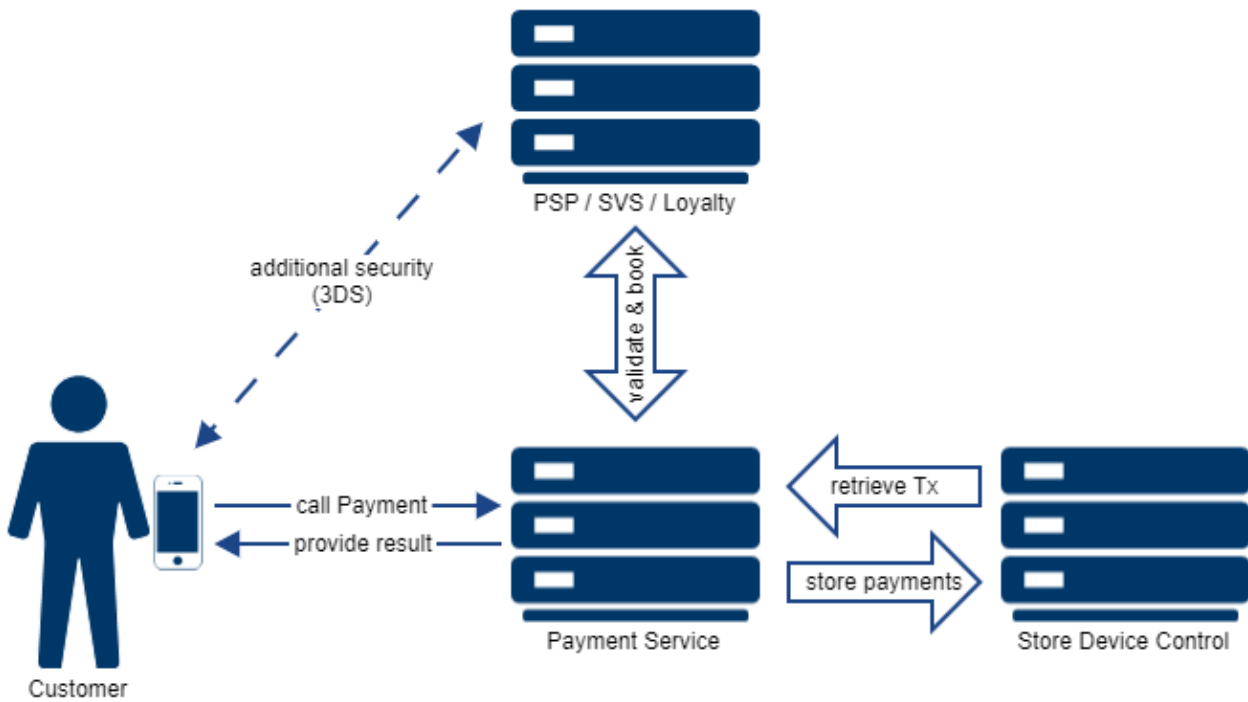
In-app payments take place in self-scanning use cases after the end-of-trip procedure is completed. The suspended transaction is retrieved from SDC and payment context is initialized. The further payment is negotiated between Payment Service and the respective payment backend. In the case of credit card payment with PSP this also includes communication between the client app and PSP backend to collect the credit card details. After retrieving a success message, the PS creates the payment position and stores it to the transaction.

Payment processes can be repeated until the transaction is fully paid.

In-app Payment Process
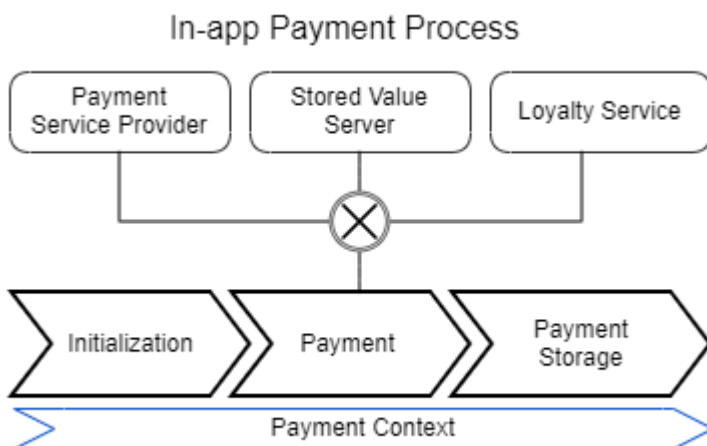
2.6.2.2 Pre-Authorized Payments

Pre-authorization is used by GK GO clients. The payment is validated/authorized before the customer starts the shopping trip. The check-out will then use this information to process a payment without further involvement of the shopper.

Pre-authorization is limited to credit card payments and requires a token, which is created in advance by storing the card details at the PSP.
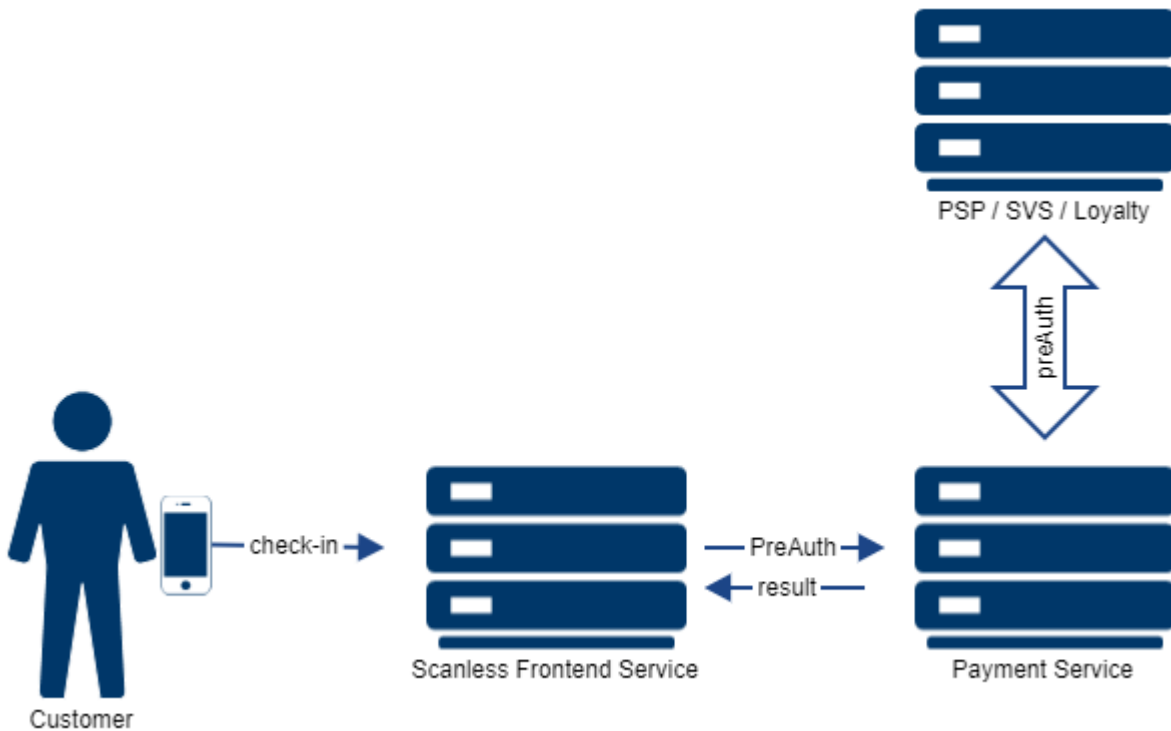
Payment pre-authorization is called by the Scanless Frontend Service during the check-in process. Payment Service retrieves the payment token for the given customer from the PSP. This token information is stored in the payment context and used in the checkout process to settle the pre-authorized payment.

Pre-Authorization Process
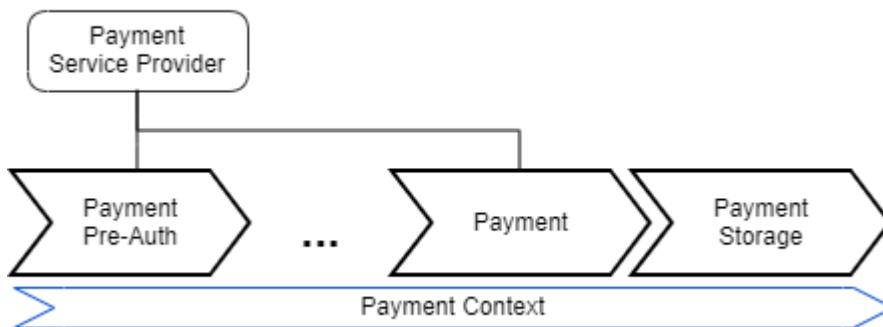
2.6.2.3 External Payment

The external payment function can be used by third party payment systems to register an already processed payment to a GK transaction. After calling the correlated endpoint, the Payment Service will create a tender position for each payment record provided in the call and save it to the transaction.

The payment is expected to fully cover the amount outstanding for this transaction.

3rd party provider   Payment Service   Store Device Control

2.6.2.4 Transaction Finalization

When TxPool is used as the transaction backend, the payment service will perform the finalization steps. This includes the generation of a digital receipt and the country specific fiscalization signatures and procedures. If the basket service is used, the transaction is finalized by this service.

2.7 Gate Service

After using the Self Scanning Clients on customer devices (BYOD), at the end of the shopping trip, the shopper can also exit the store directly by using the Gate Service.

The Gate Service will receive the command to either open or stay closed from the Gate Adapter.

The command can be sent by either the Event Service or a client (SCO POS, Mobile Assistant), depending on the consumer journey.

The client application contacts the Payment Service, which will initiate communication with an external payment provider (Adyen). In addition, this service handles communication and the transactions within the correlated GK OmniPOS environment and will inform the Gate Service about the finalization of the transaction. The Gate Service will then open the exit gate when the shopper shows the generated exit code.

Together with the Self Scanning Client, this provides a frictionless shopping experience to customers on-site in a store without involving a POS. The personnel capacities that are freed up can be used to provide customers with more advice and better service. Stationary checkout points are still available since they are integrated into the GK landscape.

In addition to automatic check-out, the Gate Service offers options for manual checkout in the case of an error.

2.7.1 Architecture
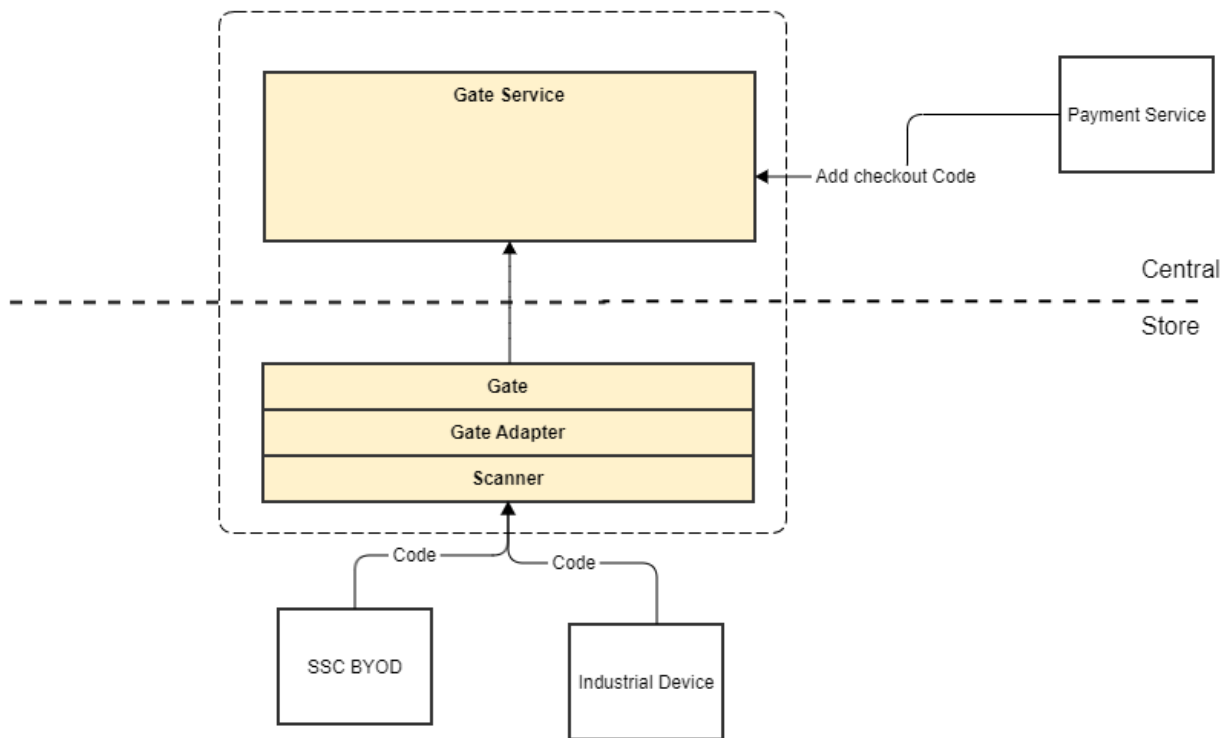
2.7.2   Scope & Use Cases

2.7.2.1 Register Check-out Code

Once the self scanning trip has successfully been completed and payment was successful, the Payment Service will return a checkout code, which can be used to open the exit gate. The Gate Service should check the code presented by the customer against the code the Self Scanning Service generated.

2.7.2.2 Validate Checkout Code

Once the shopping tip is successfully completed, the consumer moves to the checkout area where the gates are located.

If no intervention is necessary: the self scanning service will generate a checkout code that will be shared with the SSC application. This code will be scanned by the scanner at the gate and passed to the Gate Service who will check it against the code created by the Self Scanning Service.

If no error occurs, the scanning of the QR-code will open the gates and the customer can leave the store. If an error does occur, employee intervention will be required.

Diagram labels: Self Scanning Service / Payment Service, Validate end-of-trip, Code verification, Customer, Show code, response, Scanner, Gate Adapter/Service, Response, Action, Gate
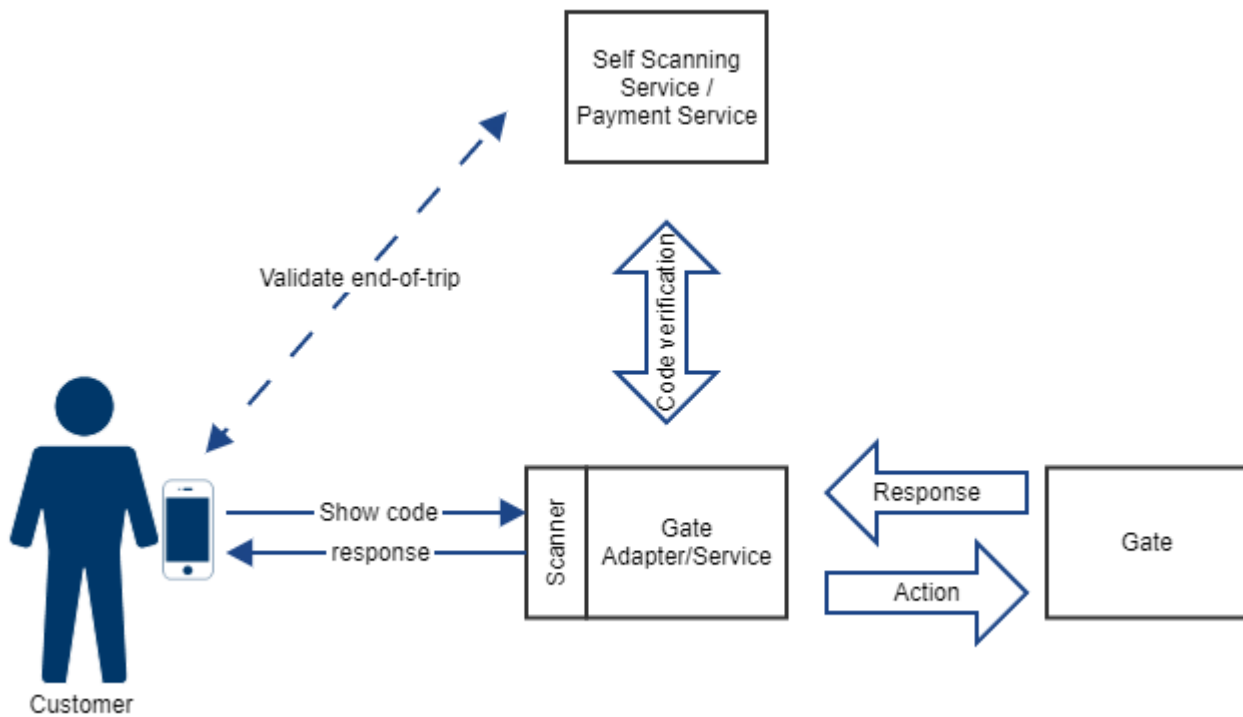
3 Product Description – Employee App

3.1 Introduction

The Employee App assists employees in the store with their daily work in customer service and with administrative tasks. The application is designed as a platform that can be easily extended with additional functionalities. The Employee App does not have a dedicated backend system but uses established services and their interfaces.

3.1.1 Event Driven Communication
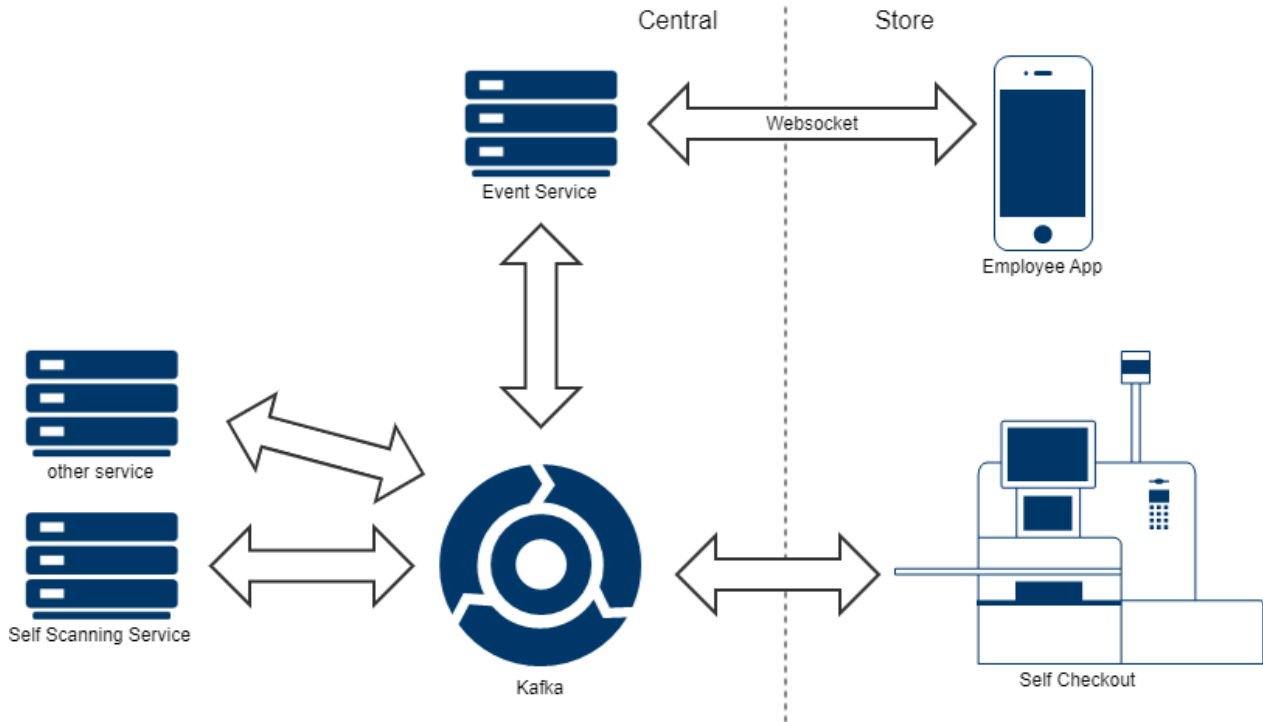
- The GK internal event communication architecture uses Kafka as the central event broker.

- Employee App clients connect via webservice to Event Service to subscribe and retrieve events. This service acts as a proxy to limit consumed resources on the event broker.

- Beside that, the Employee App can also connect to services by REST interfaces if this is required by the use case (see below)

3.1.2 Modular Architecture

Employee App
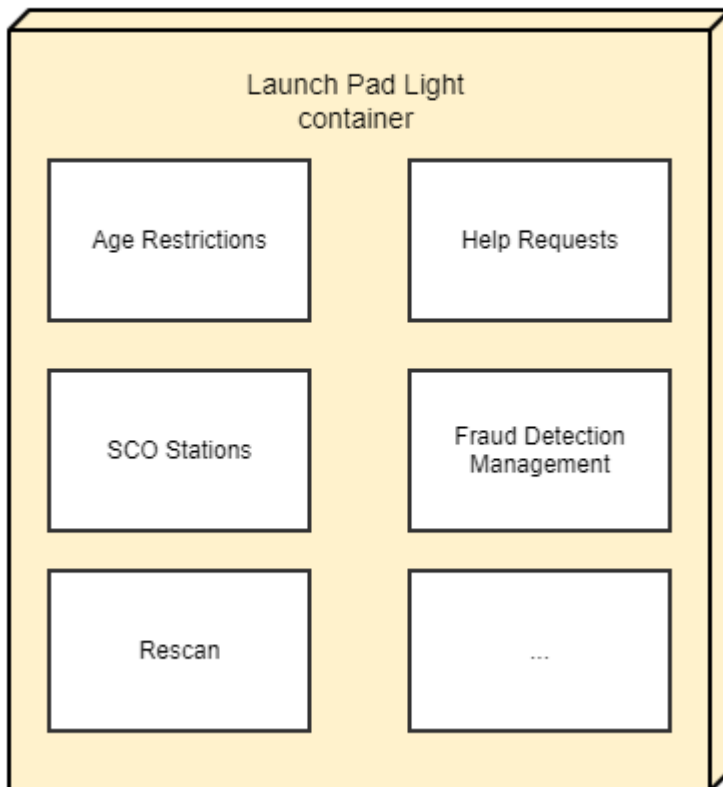
- The Employee App is a Launchpad Light container with a set of Javascript/Vue.js applets bundled into a package
- Fast and easily extendable; additional apps can be developed by projects or partners by using the AppEnablement framework
- It has to be tailored and customized for the customers use case

3.2   Scope & Use Cases

3.2.1   Age Verification

In some cases, customers may want to purchase items that require manual approval by a store assistant. For example, these may be items that can only be sold to people of a certain minimum age. With the help of the Employee App, an employee can confirm this minimum age on the sales floor, meaning that the customer can complete their purchase using the client app. The Employee App utilizes the Self Scanning Service interfaces for this purpose.

Initial Situation: A self-scanning user scans an item that needs age approval by an employee. This is shown to the user as an info message. The user can then decide if they want to resolve this at a stationary POS during checkout or to contact an employee. The user can also decide to continue scanning and resolve this issue anytime before the payment. As a result, any payment (POS or in-app) will be blocked until the required age is confirmed.

request to approve age / provide result

forward request / provide result

Infopoint

meet at infopoint for approval

meet at infopoint for approval

Selfscanning customer
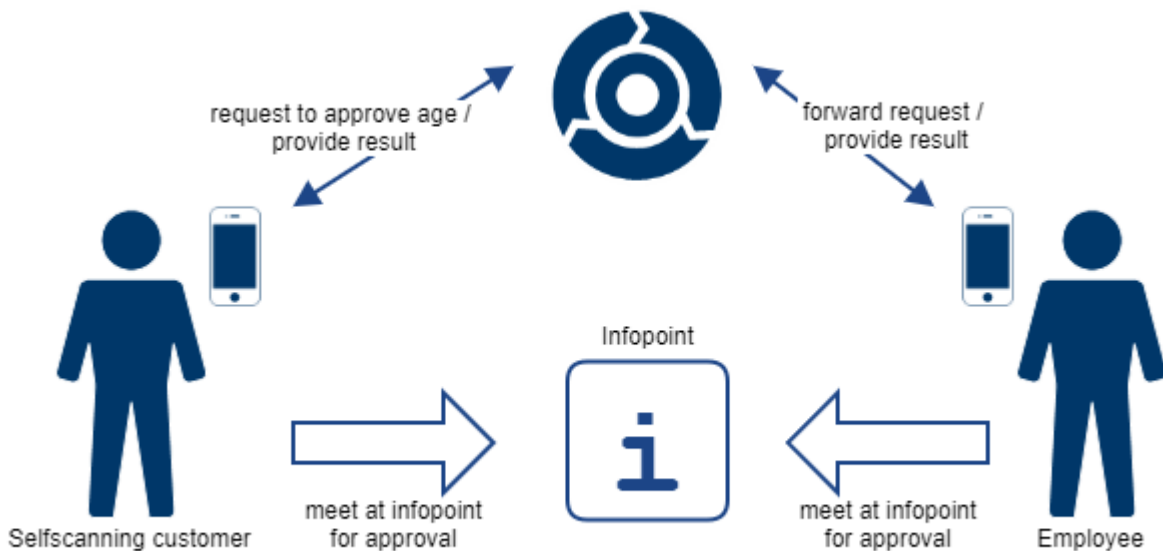
Employee

- After starting the correlated function on the SSC, the user scans a QR code at an info point, containing location information

- The app forwards the request to SSS, that creates a Kafka event

- The employee is informed about this request on their Employee App and meet the customer at the info point

- The employee checks the age and approves the request

- The approval is forwarded via Kafka event broker to the self-scanning client, that re-enables the in-app payment

Alternative Process:

- After the correlated function is started on SSC, it shows an QR code with the transaction information with the request to contact an employee at an info point

- The customer approaches an employee directly in the store

- The employee scans the displayed QR code

- The Employee App downloads the correlated transaction information and sales restrictions

- The employee checks the age and approves the request

- The approval is forwarded via Kafka event broker to the self-scanning client that re-enables the in-app payment

3.2.2   Help Request

Self Checkout stations (SCO) are self-service checkouts located in the exit area of a store where customers can scan the items and pay for their purchases on their own. In addition, customers can ask for help. The Employee App offers the possibility to receive and display messages generated by the SCO. The store employee can then go to the displayed SCO and assist the customer.

Initial Situation: A self-scanning user needs help at a Self Checkout station. The SCO offers a button to call for employee assistance.
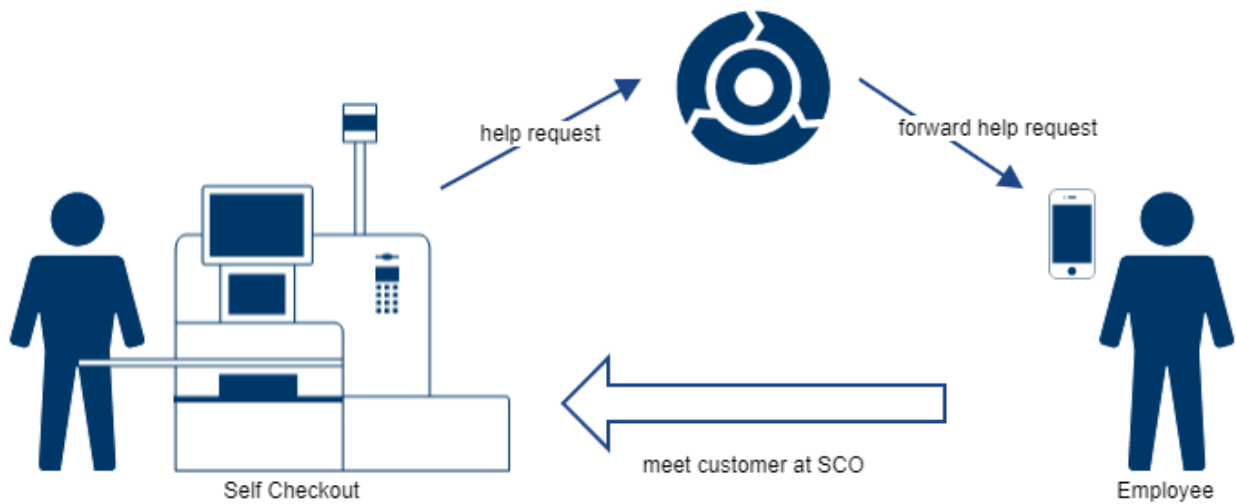
- After starting the correlated function on SCO, it creates a help request event and stores it to Kafka

- The Employee App retrieves those requests and shows them in the correlated tile

- An employee approves the event and contacts the customer at the correlated SCO

3.2.3 Rescan

Initial Situation: Fraud Detection can assign fraud risk to a given purchase transaction according to a set of rules or by constant learning. If this risk exceeds a certain threshold the transaction or parts of it must be scanned with the assistance of a store employee. Any payment is blocked until the rescan is performed.

Rescan with Self Scanning Client
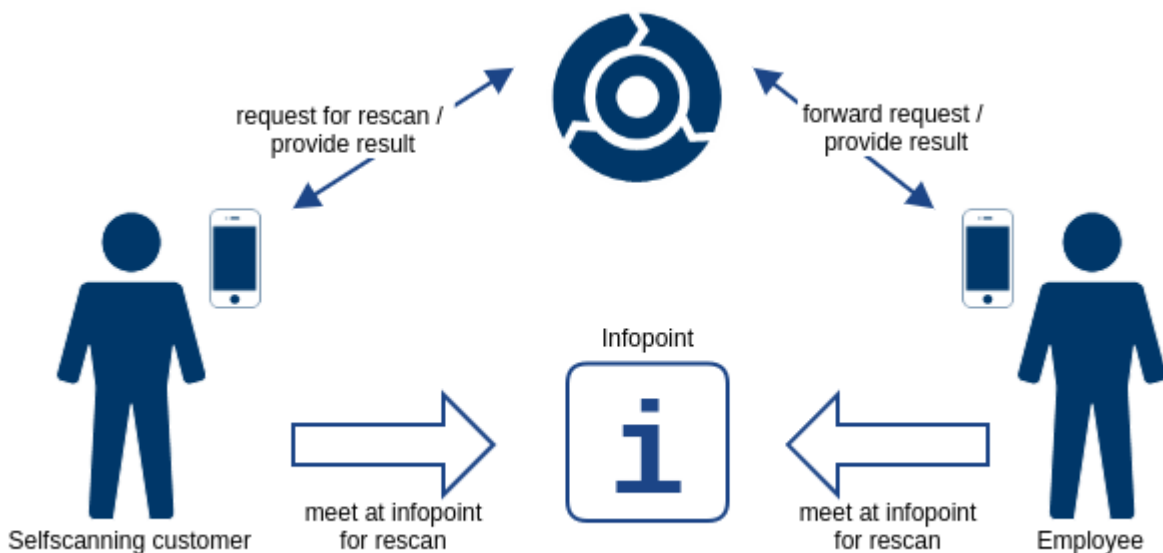
- If the rescan is triggered by Fraud Detection, the SSC shows a QR code with the transaction information and the request to contact an employee at an info point

- The employee scans the displayed QR code

- The Employee App downloads the correlated transaction information

- The employee scans the required number of items with the Employee App
- The result is forwarded via Kafka event broker to the SSC that re-enables the in-app payment

Rescan on SCO
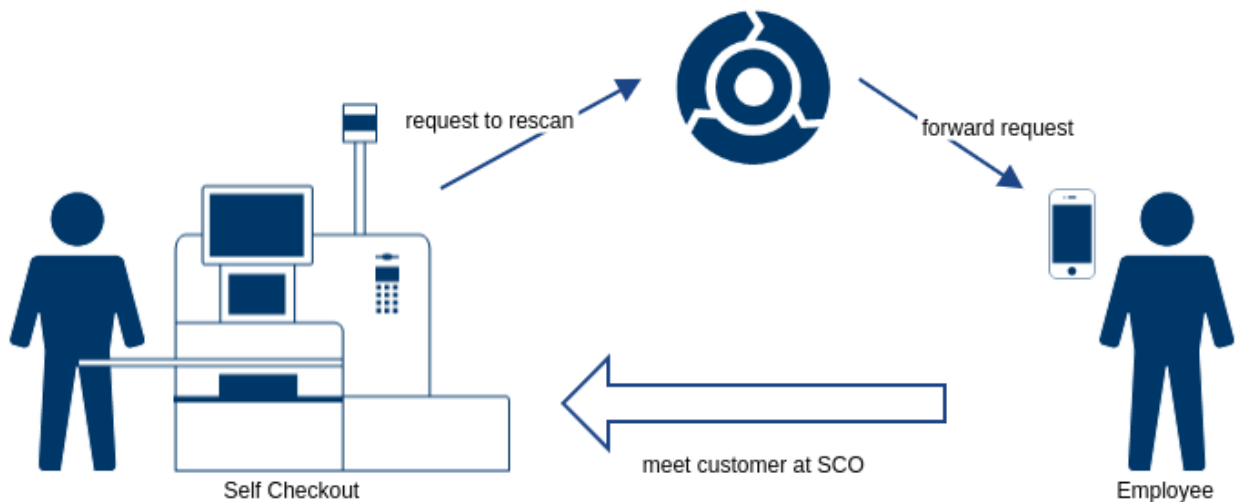
- after Fraud Detection rates the transaction accordingly, the SCO creates a rescan event and stores it to Kafka
- The Employee App retrieves those requests and shows them in the correlated tile
- The employee can now meet the customer to perform the rescan directly at the correlated SCO station

3.2.4   SCO Error

Error situations can occur during this process. These can be hardware errors or business process errors. The Employee App offers the possibility to receive and display messages generated by the SCO. The store employee can then go to the displayed SCO and solve the problem. Special situations, such as transaction timeouts or age verifications, can be resolved directly in the Employee App. The result is returned to the SCO station and processed there.

Initial Situation: A SCO station encounters an error, such as running out of paper or similar, that hinders the finalization of a self-scanning customer receipt.

Self Checkout — Employee
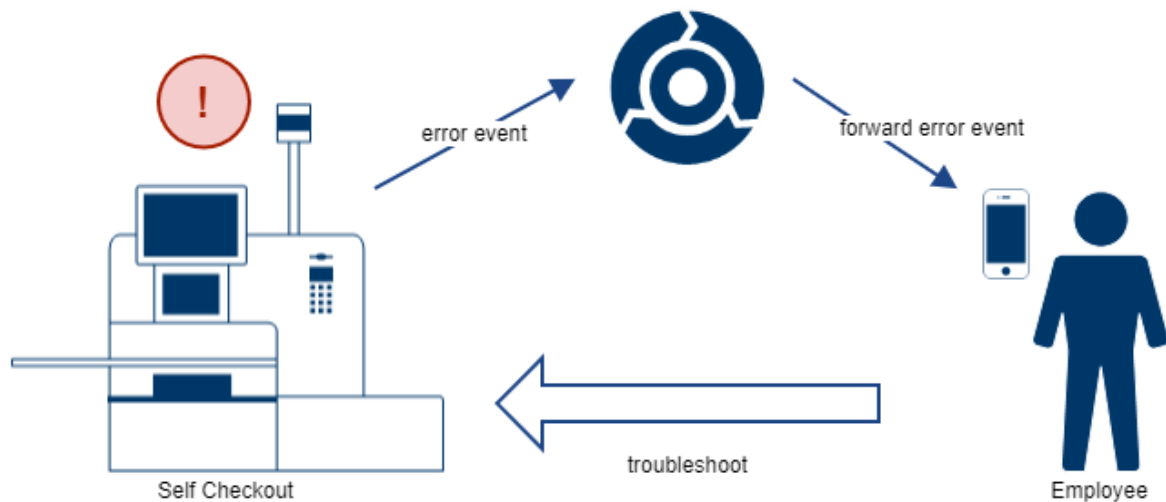
Process:

- If SCO encounters an error such as a receipt printer error, it creates an error event and stores it to Kafka
- The Employee App retrieves those evens and shows them in the correlated tile
- The employee can now correct the error at the correlated SCO

3.2.5 Fraud Detection Configuration

The Fraud Detection Service is normally configured via the Storemanager Server. However, it may also be necessary to completely override the service configuration for short periods of time to reduce or prevent queues at the stationary POSes and Self Checkout stations. The Employee App provides a feature that allows the employee to disable Fraud Detection for a specified time. The application utilizes the Fraud Detection Service interfaces for this purpose.

The function on the Employee App changes the configured behavior of the Fraud Detection Service for a certain time by using a specific predefined profile or by disabling fraud detection completely. After the configured time has passed, FDS returns to the default configuration.

Unlike the others, this specific use case doesn't facilitate any event communication. Loading and storing configuration is done by direct REST calls to the Config Service API.

Fraud Detection Service — Configuration Service — Employee
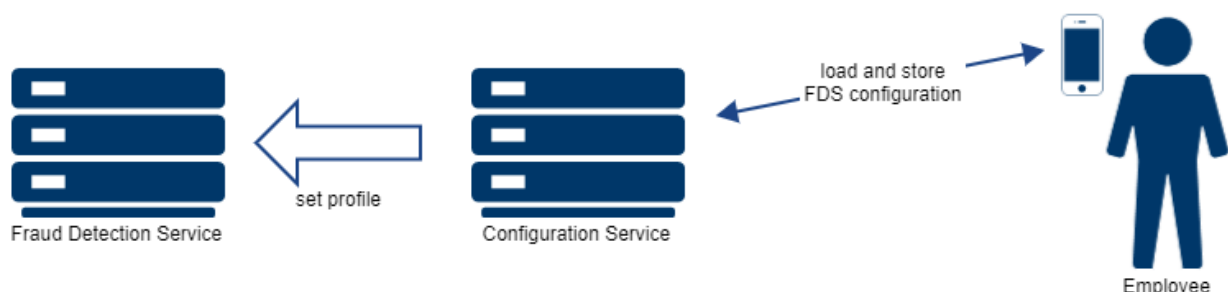
Process:

- When starting the correlated function on the Employee App, the currently active FDS configuration is downloaded from the Configuration Service.
- The employee can now select the profile and the duration of the temporary configuration change.

- After saving and activating it, the Configuration Service sends the changed config to FDS, which will reload and apply it.
- After the defined time, the configuration will be reset to the original profile.

3.3 Product Bundle

The predefined Employee App bundle includes a set of already implemented applets for the work. Those apps are displayed on the main screen in separate tiles. The selection of functions can be defined on build time.
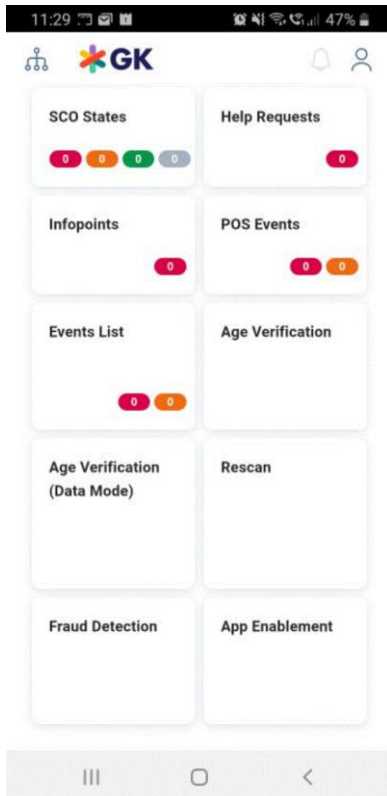
3.3.1 Predefined Applets

3.3.1.1 SCO States

This function shows the state of the SCOs in the store. It lists the configured stations with a short description summary. The state details are displayed when selecting an entry. This state is read out from the events sent by this station.

The representing tile on the main screen also shows the count of SCO stations in the correlated state.

3.3.1.2 Help Requests

This help requests function lists all open help requests. Help request information includes the SCO station it was sent from. An Employee App user can select single requests to mark them as done.

The tile itself shows the total number of open help requests.

3.3.1.3 Info Points

This function provides an overview of all events that are assigned to a specific info point. This applies in particular to age restrictions and rescan events. The name of the info point is a free text that was scanned from a QR code by the SSC and is used as a filter criterion. Each entry contains the type and identifier of the

respective transaction. The function assigned to the respective event can be started directly from the list view.

The tile itself shows the total number of open requests for all info points.
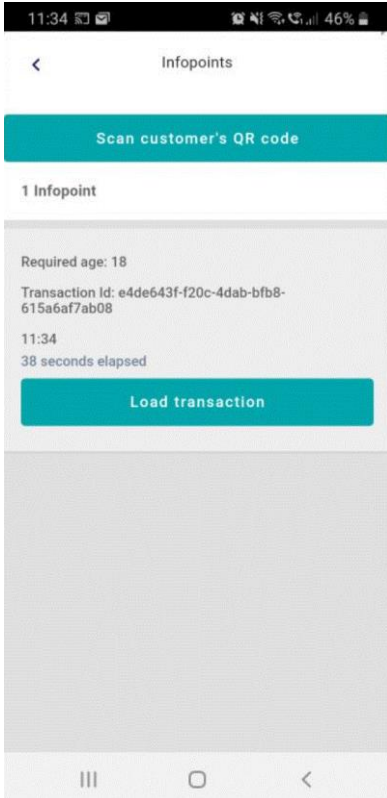
3.3.1.4 POS Events

This function displays all events assigned to a specific cash register. The list view of the functions shows the events by workstation id, grouped by the creating station.

The tile itself shows the total number of open error and info events.

3.3.1.5 Event List

All error and info events are shown within this function. This list shows them unfiltered, sorted by creation date. If a function is assigned to a particular event type, it can also be started from this view.

The tile itself shows the total number of open error and info events.
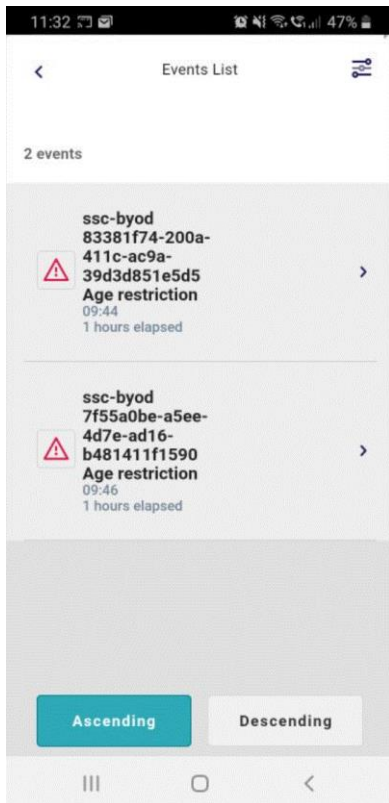
3.3.1.6 Age Verification

Within this function, an employee can approve the age of a customer if the purchase contains some items restricted to a minimum age. The employee can scan a QR code containing the transaction information to download it and approve or decline the customer's age.

3.3.1.7 Age Verification (Data Mode)

This function works the same way as the Age verification function, except that in this case the employee must enter the customer's birthday.

3.3.1.8 Rescan

This feature allows an employee to perform a partial rescan for a self-scanning transaction without involving a POS or SCO station. The employee scans a number of random items from the customer's shopping cart. If any of these items are not found in the transaction, a full rescan must then be performed at a stationary checkout or SCO. If this is not the case, the SSC is informed, and the customer can pay for their purchase in the app.

3.3.1.9 Fraud Detection

This function can be used by the employee to override the FDS configuration settings by a different profile, i.e., to decrease the number of rescans temporarily. The user can select a certain FDS profile and define the time it should be active for. Approval will activate the selected configuration profile.

3.3.1.10   App Enablement

This is an example app using the AppEnablement framework. It doesn't implement any particular use case or function, but just shows an overview.

4 Product Description – Wall Device Manager

4.1 Introduction Wall Device Manager

The Wall Device Manager manages the scanners and the cradles. It checks the availability of scanners in terms of zone, battery status, and handicap flag. It communicates with the customer database and, if available, the validation engine in order to check the customer number and to fetch the appropriate validation flag. It is also used for communication during the customer's first use of the scanner.

In the device management of the Wall Device Manager, the self scanning devices and cradles are managed and divided into the corresponding zones. The management of the walls and zones is carried out using an editor in Storemanager. The cradle location information needs to be stored in the cradles with the built-in 'Cradle Tool' of the Zebra MC18.

The integrated client in the terminal with an HTML5 GUI manages the entry and authorization of customers and the dispensing of devices. The Wall Device Manager is built into the dispensing wall and is therefore the interface to the customers using self scanning. It reads customer cards or 2D barcodes of mobile phones and processes the information accordingly.

This service may run on several instances in the store, i.e. in the dispensing walls: One Wall Device Manager is installed per wall. The Wall Device Manager replicates and ensures permanent availability of devices.

Tasks

- Read customer card or 2D barcode
- Transfer the customer card number to the POS Service
- Handicap process (store and hand over handicap flag)
- Language process (store and hand over language setting to MC18 device and payment kiosk)
- Interface to customer
- Customer handling (entry process)
- If necessary, communication of T&Cs
- Check the customer number in use at the store
- Communication with the customer database (check the card barcode on customer database)
- Check if MC18 is available on the wall (battery status – unlock only possible from a defined threshold/handicap)
- Retrieve and process status info from all MC18s
- Update tables after status changes
- Bulk-unlock MC18s
- Delivery of data for the administration client

4.2 Wall Device Manager Administration Client

The Wall Device Manager Administration Client is a tool to manage the cradles, zones and scanners. It can be used on tablets or on workstations (recommended) in the store.
It is possible to define the cradle and zones using an editor in Storemanager. In addition, it retrieves the status output of the Wall Device Manager. The target group is store employees.
The Wall Device Manager Administration Client is used to display the status of all self scanning devices in a table.
The following data of the self scanning devices is to be displayed in a list:

- Device ID
- Device status
- Battery status

- Cradle ID

- Software version

- Version master data import

- Last message

Any of the values can be used to sort the list.

The individual statuses are described in the Release Notes of the Wall Device Manager. Further information can be found in the appropriate chapters of this document. Wall Device Manager Dispensing / Disposal.

The Wall Device Manager Administration Client (Wall Device Manager Client) is integrated with the scanner service, a separate application that is not part of the Wall Device Manager Client (WDM Client). When a barcode is scanned, then the scanner service provides the type and the value of the barcode for the WDM Client.

Special barcodes (e.g. Aztec barcode) need an additional interpretation because more than the type and the value of the barcode is needed.

4.3 Device Dispensing

4.3.1 General

The device dispensing area can consist of any number of device dispensing zones. One zone consists of one Wall Device Manager and the appropriate cradles and scanners in a wall. The cradles in the lower rows are defined as a handicap zone.

The Wall Device Manager is a touchscreen client that is placed on the dispensing wall and allows customers to collect a scanner.
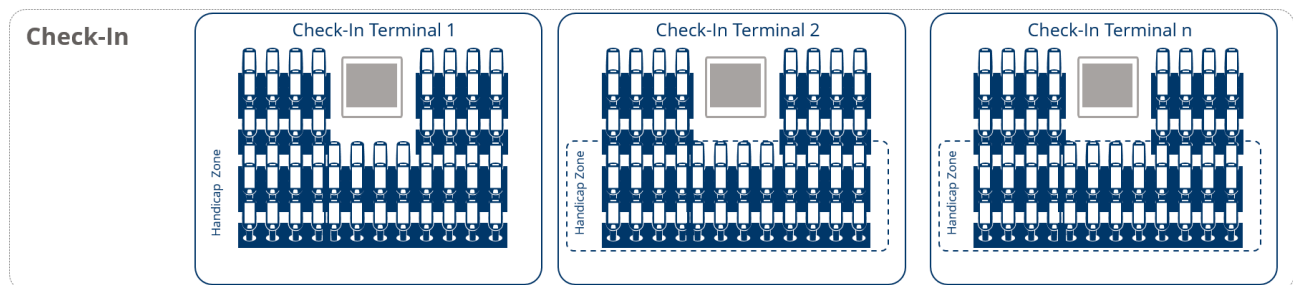
Abbildung 1 Device dispending area [1]

4.3.2 Device Overview

This function is used by a service person to get a status overview of all self scanning devices within a store. The service person may check the status, the location (if the device is located on the wall) and some more information of the device.

The 'Device Overview' mask shows an overview of all self scanning devices within the store. The table is sorted by 'Wall' in ascending order and within the 'Wall' by 'Row' and 'Column' in ascending order. The user is able to change the sorting and to sort the table by table header in ascending/descending order. Additionally, filtering in each column (except the 'Last Message' column) is possible by pressing the table header and editing the filter criteria in the input field. For example, it is possible to filter in the 'Device Status' column for all 'Available' devices or in the 'Battery Status in %' column for all devices with a battery status '<40'.

4.3.3 Device Dispensing Inactive

It should be possible to set the Wall Device Manager and the handheld dispenser to the status "Inactive", for example by scanning the "Set Inactive" barcode and activate the Wall Device Manager and the handheld dispenser by scanning the "Activate" barcode.

Welcome Screen

The welcome screen of the device dispensing terminal is set to the default store language and guides the customer through the dispensing process of a scanner.

4.3.4 Language Selection
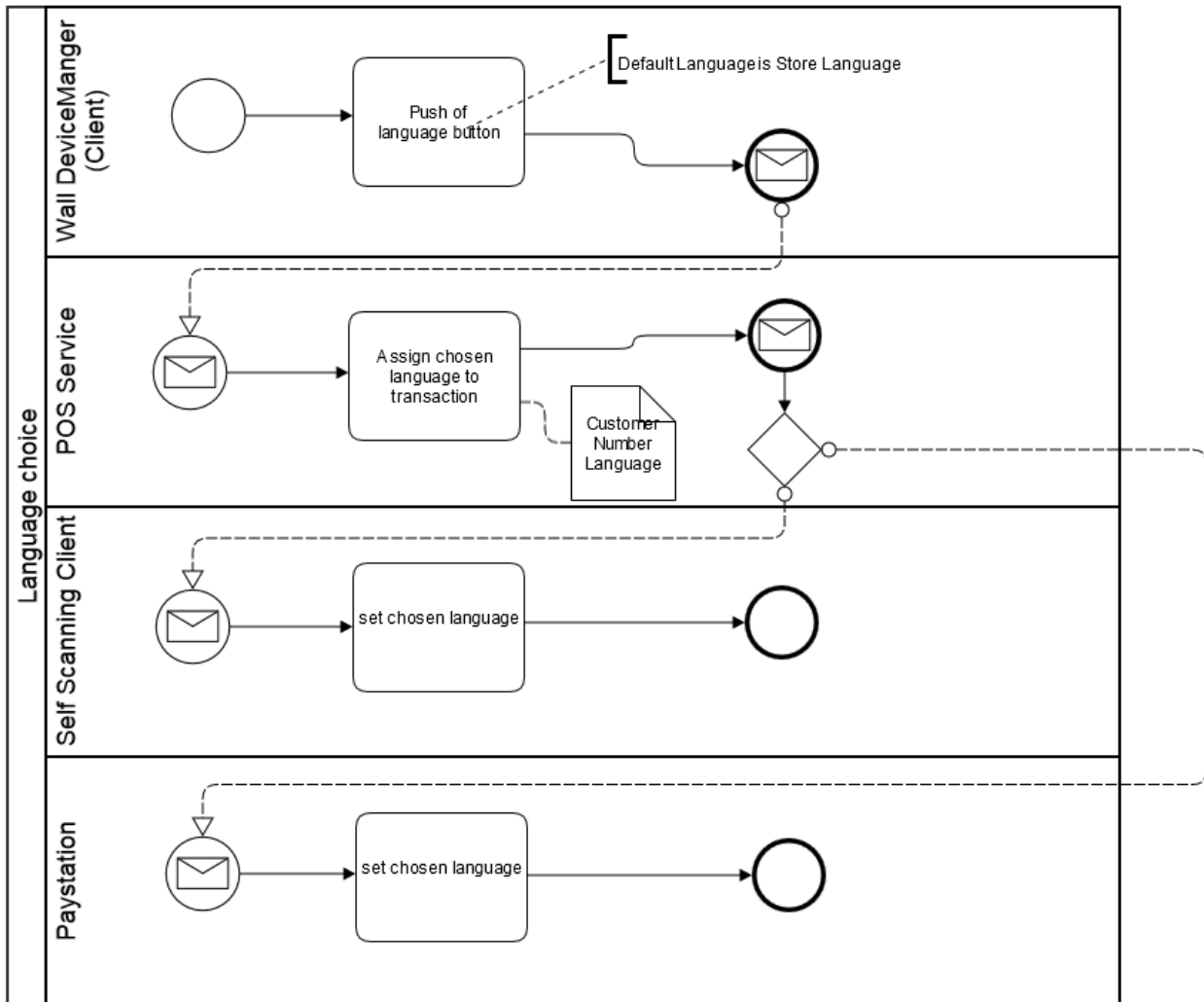
Abbildung 2 Language choice [2]

By touching the language button, the customer can select from the available languages for the Wall Device Manager, the scanner and the payment kiosk. If the customer does not touch a language button, the default store language is set.

4.3.5 Use of the 'Handicap' Button to Select a Handheld Device in the Lower Area of the Device Dispenser

Touching the handicap button (e.g. a symbol with a wheelchair) overwrites the default dispensing of a scanner from one of the upper rows. In this case, a scanner from one of the lower rows (predefined handicap zone) can be taken out.

4.3.6 Standard Device Dispensing Process for Industry Solution

The customer scans a valid customer card or the 2D barcode on their smartphone on the Wall Device Manager. The customer number is transferred by the Wall Device Manager with the selected language and the handicap option.

For the customer card, the customer number is read and transferred. For the Aztec 2D code, the customer number is read but other data in the code remains unconsidered.

The Wall Device Manager checks whether a self scanning device is available in the dispensing wall according to the battery status and handicap zone criteria. If there is no self scanning device with a sufficient battery level in the default area, a device from the handicap area will be unlocked and vice versa. The devices are to be dispensed according to the principle of highest battery level, i.e. the device with the highest battery level in its zone (default or handicap) will be unlocked. If there are no devices with a sufficient battery level in either of the two zones, unlocking is prevented and the following message is displayed: "No device dispensable." The availability of the self scanning devices depends on the following parameters:

- Battery status (configurable threshold) - only devices with a sufficient battery level are dispensed.

- Cradle zone

- Handicap zone

- Self scanning device is in the status 'available'

The Wall Device Manager checks whether there is already an open or interrupted self scanning transaction for this customer number in the store. If so, the terminal displays the following message: "Self scanning is currently not possible as the customer number is already in use". In this case too, no device is dispensed.

The Wall Device Manager then checks on the customer database via the POS Service whether the customer is locked and fetches the validation flag for the customer.

If the customer card is locked, then the following message will be displayed on the terminal screen in the appropriate language: "Self scanning device cannot currently be dispensed. Please contact a service person".

After a successful check of the customer number, the self scanning device dispensing process is triggered. The cradle of the unlocked mobile self scanning device will light up and the self scanning device can be taken out.

When taking out the self scanning device, POS Service login is performed. The cradle and the LED of the self scanning device stop flashing.

During login, a virtual shopping basket is opened and the validation flag (if enabled) and the language are transferred.

If the self scanning device is not taken out of the cradle after a certain amount of time (configurable), the cradle is locked again. The customer card must then be scanned again. The data previously read is discarded. The customer is reported back to the customer database as 'validated' if they have received a validation flag.

If a self scanning device is placed back in the dispensing wall, the transaction is automatically canceled. If the self scanning device is in the offline state, the transaction is canceled and the display returns to the start screen.

After the self scanning device has been taken out, the status changes from 'available' to 'shopping'.

Parallel to this process, the validation code is returned by the customer database. This validation code specifies whether or not the customer is validated after disposing the self scanning device. The validation code is also assigned to the open receipt.

4.4   Validation

Scanning the 'end-of-trip barcode' executes the validation process. According to the parameter which was set during device dispensing, the following use cases apply.

4.4.1   Validation Parameters

4.4.1.1 No Validation

The customer may proceed to the payment kiosk. The deferred receipt is unlocked for payment.

4.4.1.2 Full Inspection

The message "Please contact the service staff for a full inspection" appears on the screen of the handheld device.

The deferred receipt is locked for payment until the service personnel unlocks it at the end of the validation routine.

4.4.1.3 Random Inspection

The message "Please contact the service staff for a random inspection" appears on the screen of the handheld device.

The deferred receipt is locked for payment until the service personnel unlocks it at the end of the validation routine.

Special Case - Customer Ignores Message

Use case: The customer ignores the message, puts the handheld device back into the cradle (or just puts the handheld device away) without contacting the service personnel and scans their payment code at the payment terminal.

In the case of a full inspection, the following message will appear on the screen of the payment terminal: "Please contact the service staff for a full inspection." No other functions will be available to the customer.

In the case of a random inspection, the following message will appear on the screen of the payment terminal: "Please contact the service staff for a random inspection". No other functions will be available to the customer.

Only the service personnel have the right to clear the message by scanning a special barcode card.

4.5   Checkout / Disposal

The self scanning device can be disposed of in the checkout area, at a self checkout station, service station or at a normal cash register.

As soon as the customer wants to finish shopping, they scan an end-of-trip barcode in the checkout area and a full screen with the following message will appear "Did you scan all items?". It is only possible to answer the question by touching a YES or NO button.

If the customer touches the **YES** button, the appropriate validation function is executed.

If the customer touches the **NO** button, the screen of the handheld device jumps back to the scanning menu.

As soon as validation has been executed successfully, the following message pops up: 'Please proceed to the payment kiosk and scan the barcode at the payment tower".

Upon scanning the payment barcode, the receipt is transferred to the payment kiosk where the customer is located and the following message pops up on the screen of the handheld device: "Please dispose of the handheld in the disposal zone".

In addition, the status message on the handheld device will change to 'Not available'.

The customer can pay with the accepted payment methods on the POS Client in the self scan pay mode.

4.5.1   Device Disposal Areas

In the standard solution, the self scanning devices are disposed of in the disposal areas and the payment is made at the payment kiosk.
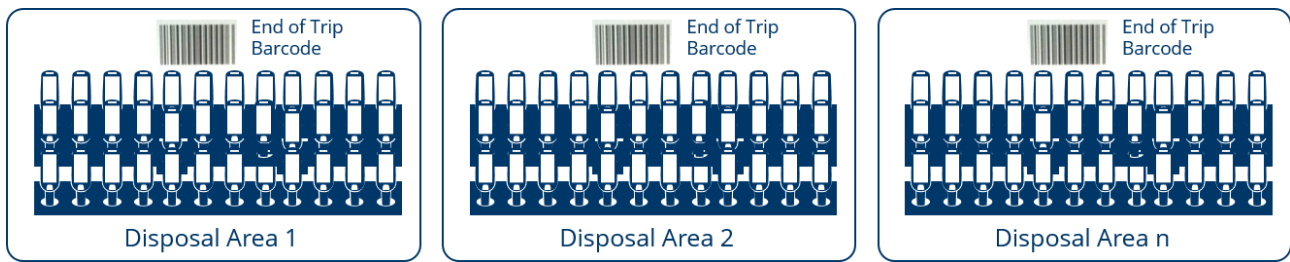
Abbildung 3 Device disposal area [3]

Check-Out
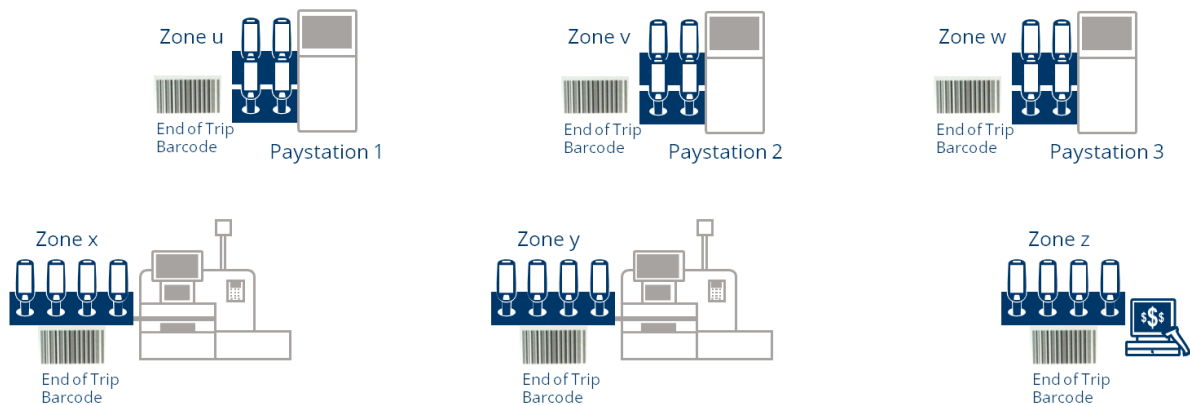
Abbildung 4 Checkout [4]

4.5.2   Disposal Process

At the end of trip, the following process takes place:

There are basically two ways to finish the shopping and to transfer the transaction to the payment kiosk:

- Scan the "end-of-trip" barcode (EAN 13 with prefix 146)
- Place the scanner in the device disposal area

With scan of the end-of-trip barcode

When scanning the end-of-trip barcode, it is checked whether line items are included in the virtual shopping basket.

If not, the virtual shopping basket is automatically canceled. This is performed independently of a validation flag. A message with the following text is displayed: "Thanks for your visit. Please put the scanner back". In this case, no validation result (logoff request) would be sent to the customer DB; the customer is automatically selected for validation again at the next purchase.

If line items are included, the message with the question "Have you scanned all items?" is displayed.

Input window: The message "Have you scanned all items?" appears on the screen including buttons to confirm or reject (yes/no).

Input = yes (without validation): If the customer answers the question with 'yes', the following message is displayed: "Please put the scanner back and pay for the purchase at a payment kiosk!". An interruption is created (END OF TRIP ready for payment).

Input = yes (with validation): If the customer has been selected for shopping cart validation and answers the question with "yes", the following message is displayed: "Please contact a service person to perform a random check". An interruption is created: reason code (END OF TRIP ready for payment).

Input = no: If the customer answers the question with 'no', the Self Scanning Client returns to the list view. No interruption is created.

As soon as the self scanning device is put back into the cradle, the display changes to the start screen and the device status changes to "Not available".

Without scan of the end-of-trip barcode

When putting the self scanning device back into a cradle, it is checked whether it is a dispensing or disposal area.

Dispensing area: The transaction is canceled and the display returns to the start screen.

Disposal area:

If the virtual shopping basket contains no line items, the transaction is automatically canceled. A message with the following text is displayed: "Thanks for your visit". In this case, no validation result (logoff request) would be sent to the customer DB; the customer is automatically selected for validation again at the next purchase.

If there are line items in the virtual shopping basket, a message with the following text is displayed: "Please scan the end-of-trip barcode" and the cradle starts flashing. The self scanning device is not locked.

If the self scanning device is taken out before defined timeout, the system returns to the list view or the item entry mode and the customer can scan the end-of-trip barcode or enter more items.

After the timeout, the device is automatically locked and the cradle stops flashing, even if the question has not yet been answered. The transaction is set to "interruption" (ReasonCode: confirmation required). Consequently, the customer has to answer the question at the payment kiosk. The display changes to the start screen and the device status changes to "Not available".

4.5.3 Out of Service

The check-in area can be taken out of operation manually for various reasons. For this purpose, the service barcode (EAN-13 with prefix 146) is scanned. The message "Out of Service" appears on the screen of the check-in area in the store language. Furthermore, a type 10 message with the corresponding text ("Out of Service") is displayed on the Self Scanning Client.

In the status 'Check-in closed', it is not possible to remove a self scanning device.

To put the check-in area into operation again, the "Service Code" barcode is scanned again.

4.6 Service

4.6.1 Self Scanning Device Pickup

The service person can, for example, take devices from the checkout zone and take them to the check-in zone. By scanning the 'service barcode', the self scanning device is unlocked and can be removed.

The self scanning devices are addressed by the Device Manager.

4.6.2 Self Scanning Device Swapping

The service person can defer the shopping cart (e.g. if the battery is dead) by scanning a special barcode and transfer it to a new device. To do so, it is necessary to unblock the customer number because the customer number is blocked in the store by default as soon as the customer number has opened a self scanning transaction. It should be possible to fetch the transaction from the POS Service by scanning the customer card with the new device. The original self scanning device loses control over the transaction.

Standard Case (Manual Deferral):

If the battery level falls below a defined threshold, the following warning message is displayed: "Warning: low battery", "Please contact the service person". The customer seeks out a service person. The service person scans the service barcode and defers the transaction (e.g. by a function button on the self scanning device user interface). The shopping cart including the customer number is deferred and is no longer available on the self scanning device. The service person takes another self scanning device by scanning the service

barcode and then the customer card. The shopping cart including the customer number is transferred to the new Self Scanning Client which automatically switches to registration mode. The old self scanning device can be moved to a disposal area and the customer can continue shopping. Both self scanning devices send their status updates.

Special Case 1 (Automatic Deferral):

If the battery level falls below a defined threshold, the following warning message is displayed: "Warning: low battery. Please contact the service person". The customer ignores this message. If the battery level falls below the next defined threshold, the following warning message is displayed: "Warning: battery is empty. The self scanning device will shut down. Please contact the service person". After that, the shopping cart including the customer number is automatically deferred by the self scanning device and the device turns off. After the shopping cart has been deferred, it is no longer available on the self scanning device. The customer seeks out a service person. The service person takes another self scanning device by scanning the service barcode and then the customer card. The shopping cart including the customer number is transferred to the new Self Scanning Client which automatically switches to registration mode. The customer can continue shopping. The old self scanning device is moved to a disposal area to charge the battery. Both self scanning devices send their status updates.

Special Case 2 (No Deferral):

If a device is no longer able to defer the shopping cart (e.g. because the battery level goes down to zero too quickly, the device is offline at the moment or the process is prevented by a device fault), then the customer must contact a service person again. The service person takes another self scanning device by scanning the service barcode. The customer card is then scanned and a deferred or open shopping cart is searched for. If a shopping cart with the status "open" is found, the service person must confirm that the shopping cart (including the customer number) should really be transferred to the new device. The new self scanning device then switches to registration mode. The customer can continue shopping. As soon as the old self scanning device can resume its operations, it must find out that another self scanning device (or a POS) now has control over "its" transaction and that it is not allowed to process it anymore. It does not accept any further changes for this transaction and discards it from the internal memory. The same behavior applies if the use case "Fetch an open transaction at the payment kiosk" is performed at a payment kiosk.

In any case, it must be possible to read the customer number from both the EAN-13 barcode of a physical customer card and a 2D Aztec code of the application.
In the case of a 2D Aztec code, only the customer number is used.

4.6.3   Bulk Device Pickup

It is possible to unlock the self scanning devices of an entire zone. The device pickup should be controlled for each self scanning device.

Here, voltage fluctuations must be avoided, i.e. it must be ensured that only a certain number of self scanning devices are unlocked simultaneously upon a command.

Only a certain, configurable number of self scanning devices in a zone are unlocked upon a command. Only after the self scanning devices have been taken can the next zone be unlocked. Gaps are skipped. In principle, the bulk device pickup is performed from top left to bottom right.

Device pickup is to be triggered automatically. The trigger is the status message of the device that was taken first. The number of devices to be removed (=x) is configurable. The devices to be removed are unlocked and flash. If the first device is taken, the device x +1 starts to flash, i.e. x devices are always flashing. The process ends with the removal of the last device on the wall.

It is still possible to take the devices individually, i.e. there are the buttons "bulk device pickup" and "individual device pickup".

If a customer puts the device back in the disposal area during the bulk device pickup, then the device taking is not taken into account.

4.7   Administration of Cradles

4.7.1   Configuration

To ensure that both the device and the Wall Device Manager know which self scanning device is in which cradle, each cradle can be programmed with an ID.
The cradle ID consists of 3 values:

- Wall ID

- Column ID

- Row ID

To ensure that the Wall Device Manager and the self scanning device recognize the dispensing areas and the disposal areas, cradles are divided into zones (walls).
The dispensing or disposal function must be assigned to each Wall ID because the devices must react differently depending on the type of action (e.g. the device is put into a cradle).
In addition, a Wall Device Manager must be assigned to each wall with a dispensing function because the Wall Device Manager must know from which wall the devices should be released.

For each device wall, there is also a handicap zone that must be considered by the Wall Device Manager depending on the customer (selection).

This results in the following configuration table that must be administered:

- Wall ID: defines the wall

- Col ID from: column number from

- Col ID to: column number to

- Row ID from: row number from

- Row ID to: row number to

- Type: dispensing or disposal

- Handicap: handicap zone Yes or No. Only relevant to dispensing.

- Responsible Wall Device Manager: Wall Device Manager ID. Only relevant to dispensing.

Example of a list

Wall ID	Col ID from	Col ID to	Row ID from	Row ID to	Type	Handicap	Responsible WDM
1	1	10	1	10	Dispensing	No	1
1	1	10	11	12	Dispensing	Yes	1
2	1	10	1	10	Dispensing	No	2
2	1	10	11	12	Dispensing	Yes	2
3	1	10	1	10	Dispensing	No	3
3	1	10	11	12	Dispensing	Yes	3
....							
12	1	15	1	8	Disposal	-	-
13	1	15	1	8	Disposal	-	-

This data can be maintained in Storemanager. The data is required by the self scanning devices (type is relevant) and by the Wall Device Manager (dispensing and handicap are relevant).

4.7.2   Staging

The cradle zones are administered according to the Configuration chapter described above. The programming of the cradle IDs is done by placing a self scanning device into a cradle. The communication is carried out by the internal BUS of the system.

Using the software provided by Zebra, the cradle ID can be programmed.

5 Release Notes – Self Scanning Client (Industry scanning device and SDK)

This document describes the functional and technical news and improvements relating to the following applications and services in the latest version:

- **Self Scanning Client (Industry Device)**
- **Self Scanning SDK iOS**
- **Self Scanning SDK Android**

Additional information can be found in the following documents:

- Installation Guide: installation
- Operation Guide: operation, monitoring
- Upgrade and Update Guide: update process
- Security Guide: encryption, password handling, user management
- Product Description: product information
- Customizing Guide: configuration information
- Customizing Reference: parameter description for configuration needs
- User Guide: instructions for use

Use the table of contents to jump directly to the appropriate version:

5.1 5.23 Versions (SAP 7.6)

Version 7.6 (5.23.0) is released based on feature drop FD-2305 and will also include the issues fixed in any previous feature drop.

🖥 **Release date** ➜ 02 Jun 2023

5.1.1 Key Features

5.1.1.1 Loyalty Management

- *Loyalty rewards* - Members of a loyalty program can now redeem tier-specific rewards.

5.1.2 Feature Drop FD-2305

🖥 **Release date** ➜ 31 Mar 2023

What's New

/

Fixed Issues

/

5.1.3 Feature Drop FD-2304

🖥 **Release date** ➜ 31 Mar 2023

What's New

/

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-6248	Android, Industry Device	Bug	[Industrial device] Failed to load item images
POSS-6256	Android, Industry Device	Bug	[Industrial device] Crashed when client is onboarded outside the cradle
POSS-6256	Android, Industry Device	Bug	[AGW] Content cannot be downloaded from DSG (PDF/videos)
POSS-6280	Android, Industry Device	Bug	[Android] PCE not called
POSS-6279	iOS, Industry Device	Bug	[iOS] PCE not called
POSS-6298	Android, Industry Device	Bug	[Industrial device] Returns 401 with fiscal certification - workaround
POSS-6249	Android, Industry Device	Bug	[Industrial device] Returns 401 with fiscal certification
POSS-6279	Industry Device, iOS	Bug	[iOS] PCE not called

5.1.4   Feature Drop FD-2303

🗔 **Release date ➜** 31 Mar 2023

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-6040	Industry Device	Story	[Android] Test and last steps for client onboarding on industrial device
POSS-5088	Industry Device	Story	[Android] Rich content displayed

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-6035	Industry Device	Bug	[Android] Wrong total amount in basket with basket promotions

5.1.5   Feature Drop FD-2302

🗔 **Release date ➜** 03 Mar 2023

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-5594	Android, CPS_SDK, GkGo App, SSC, Vision App	Story	[Android] Verify methods protected with reCAPTCHA
POSS-5591	CPS_SDK, GkGo App, iOS, SSC, Vision App	Story	[iOS] Verify methods protected with reCAPTCHA
POSS-5511	SSC	Story	[Demo Cloud] Promotion recommendation not displayed in SSC BYOD
POSS-5089	Android, GkGo App, SSC, Vision App	Story	[Android] Create proper name for output files from build
POSS-4782	Android, GkGo App, SSC, Vision App	Story	[Android] Unification of SharedPreferences
POSS-5431	Android, GkGo App, SSC, Vision App	Story	[Android] Create proper name for output files from build
POSS-5784	iOS, SSC	Story	[iOS] Send loyalty information in recalculate request to PCE
POSS-5783	Android, SSC	Story	[Android] Send loyalty information in recalculate request to PCE

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-5575	Android, Industry Device	Bug	[Android] Industrial App does not run on Zebra PS20
POSS-3438	Android, SSC	Bug	[Android] getJWT called too often
POSS-5674	BYOD-iOS, GkGo App, SSC, Vision App	Bug	[iOS] Update icons of standard apps to new branding

5.1.6   Feature Drop FD-2301

🗔 **Release date ➜** 03 Feb 2023

What's New

/

Fixed Issues

/

5.1.7 Feature Drop FD-2212

📇 **Release date** ➜ 06 Jan 2023

What's New

No changes in this version.

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-4806	BYOD-Android	Bug	[Android] Error during EOT for existing shopping basket
POSS-5256	BYOD-iOS	Bug	[iOS] Points payment is failing

5.1.8 Feature Drop FD-2211

📇 **Release date** ➜ 02 Dec 2022

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-4331	BYOD-iOS, SSC_SDK	Story	[iOS SSC SDK] Update of AFNetworking and use of XCFramework

Fixed Issues

No fixes in this version.

5.1.9 Feature Drop FD-2210

📇 **Release date** ➜ 04 Nov 2022

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-4759	BYOD-iOS	Story	[iOS] Update the versions of the applications and the SDKs
POSS-4758	BYOD-Android	Story	[Android] Update the versions of the applications and the SDKs

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-3607	BYOD-Android	Story	[Android] Age verification via Infopoint

No fixes in this version.

5.2 5.22 Versions

Version 5.22.0 is an intermediate release and not intended for Premium Qualification. It is based on a feature drop to be defined and will also include the issues fixed in any previous feature drop.

📇 **Release date** ➜ 06 Oct 2022

5.2.1 Key Features

5.2.1.1 Privacy

- Customers can now use the device without an account as anonymous customers

5.2.1.2 Payment

- Update to the library so that the client ID can be used in the new version of the Adyen Drop-in control.

- To avoid deploying multiple binaries with several Adyen settings, the setting will be read from the config QR code which can be scanned in the app.

- Payment with points is now possible with the SSC BYOD iOS and Android

5.2.1.3 Registration/Login

- Customers can now use the Self Scanning Service from their devices without having to register or create an account, i.e. as anonymous customers.

- The client (iOS/Android) can now perform a login against Keycloak with the relevant tenant information (tenant in multitenancy or global mode).

- When onboarding against the CPS, a consumer can also sign-up for a loyalty program. Their loyalty and CPS ID will be the same in order to link both accounts.

5.2.1.4 Multitenancy

- The multitenancy support for the clients is a follow-up implementation of the recent "Customer Profile Service Multitenancy Support". The check-in QR code that is used at the entrance area of the store was extended to contain an optional tenant ID. The tenant ID is then used in the requests to backend services.

5.2.1.5 Security

- Basic Auth has been replaced by OAuth 2.0. Clients use JWT access tokens for authentication at central and edge services and get a JWT refresh token that is used to get new JWT access tokens before expiration and also a new JWT refresh token.

- Secure Client Onboarding: This new onboarding process uses a pre-registration process for clients and therefore no longer relies on pre-shared keys.

- New frequency of scans of applications/services on Fortify. As the reaction time to security incidents is limited by the SLAs, it is necessary to know about potential security issues in the apps as soon as possible.

5.2.2 5.22.0-FD-2209 (Feature Drop)

Release date ➔ 06 Oct 2022

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-4718	BYOD-Android, SSC_SDK, LS_SDK	Story	[Android] SSC Standalone - Loyalty onboarding
POSS-4716	BYOD-iOS, SSC_SDK, LS_SDK	Story	[iOS] SSC Standalone - Loyalty onboarding
POSS-3963	BYOD-Android, SSC_SDK, LS_SDK	Story	[Android] Implement points payment
POSS-4749	BYOD-Android, SSC_SDK	Story	[Android] Extend endOfTrip v2 by customerCardId - Points collection process
POSS-4748	BYOD-iOS, SSC_SDK	Story	[iOS] Extend endOfTrip v2 by customerCardId - Points collection process
POSS-3964	BYOD-iOS, SSC_SDK, LS_SDK	Story	[iOS] Implement points payment

Fixed Issues

No fixes in this version.

5.2.3 5.22.0-FD-2208 (Feature Drop)

Release date ➔ 02 Sep 2022

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-3797	Industry Device	Story	[Android] Industry Device - Secure Client Onboarding
POSS-3993	Industry Device	Story	[Android] SSC industry device - Replace logo on main screen with new logo

Fixed Issues

No fixes in this version.

5.2.4 5.22.0-FD-2207 (Feature Drop)

Release date → 29 Jul 2022

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-3797	Industry Device	Story	[Android] Industry Device - Secure Client Onboarding

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-3866	Industry Device, SSC_SDK	Bug	[Android] SSC - Image download API exposes complete DSG to the Internet
POSS-3992	Industry Device	Bug	[Android] SSC industry device does not read selfscan-config-native.json completely
POSS-3993	Industry Device	Bug	[Android] SSC industry device - Replace logo on main screen with new logo
POSS-4269	Industry Device	Bug	[Industry Device] Device should switch back to standby mode when the device is plugged in again

5.2.5 5.22.0-FD-2206 (Feature Drop)

Release date → 01 Jul 2022

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-4223	Industry Device	Story	Whitelabel App (SSC & GK GO) - Pass Fortify tests
POSS-3946	Industry Device	Story	Customers can now use the device without an account as anonymous customers
POSS-4224	BYOD-iOS	Story	[iOS] Whitelabel App (SSC & GK GO) - Pass Fortify tests

Fixed Issues

No changes in this version.

5.2.6 5.22.0-FD-2205 (Feature Drop)

Release date → 03 Jun 2022

What's New

No changes in this version.

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-3866	Industry Device	Bug	[Android] SSC - Image download API exposes complete DSG to the Internet
POSS-4027	BYOD-Android	Bug	[Android] Analyze why barcodes cannot be scanned
POSS-4072	BYOD-Android	Bug	[Android] SSC BYOD App crashes during payment
POSS-3867	BYOD-iOS, SSC_SDK	Bug	[iOS] SSC - Image download API exposes complete DSG to the Internet

6 Release Notes – Self Scanning Backend

This document describes the functional and technical news and improvements relating to the following applications and services in the latest version:

- **API Gateway**

- **Self Scanning Service** (incl. Fraud Detection Service, Payment Service, Fraud Detection Service, Gate Service)

- **Shopping List Service**

Additional information can be found in the following documents:

- Installation Guide: installation

- Operation Guide: operation, monitoring

- Upgrade and Update Guide: update process

- Security Guide: encryption, password handling, user management

- Product Description: product information

- Customizing Guide: configuration information

- Customizing Reference: parameter description for configuration needs

- User Guide: instructions for use

- Sizing Guide: deployment, technical data relating to CPU, hard disc, etc.

Use the table of contents to jump directly to the appropriate version:

6.1   5.23 Versions (SAP 7.6)

Version 7.6 (5.23.0) is released based on feature drop FD-2305 and will also include the issues fixed in any previous feature drop.

🖼 **Release date →** 02 Jun 2023

6.1.1   Key Features

6.1.1.1 Payment Service

- *More payment types for external payments* - Payment Service now also supports EFT or cash payments as a tender type in external payments.

- *Fiscalization ES/AT* - Payment Service is now prepared to fulfil the fiscal rules in Spain and Austria by integrating the appropriate Fiscal Service and processes. Please note that this change enables only Self Scanning to be used in those countries. Please also check the GK GO Release Notes for the status of implementation in those applications.

- *Deployment reorganization* - Payment Service is now reorganized into a separately deployed microservice. This type of organization is used only in cloud environments, while on-prem installations still deploy this service within the Self Scanning Service package.

- *Use of Basket Service in payment* - The Payment Service will now save each processed payment as a tender position to the Basket Service, replacing direct TxPool access. This eliminates the need to suspend a transaction prior to payment. In addition, any finalization step such as receipt fiscalization and printing is handed off to the Basket Finalization Service.

6.1.1.2 API Gateway

- *Notification Interfaces* - API Gateway forwards interface calls to the Push Notification Service & Basket Notification Service. Clients are now able to subscribe to those services to be notified about new offers or item recommendations even if the client application is suspended.

- *SPOT Interfaces* - API Gateway integrates SPOT & Engagement Service APIs. Those endpoints can now be called by clients to retrieve and send information to the SPOT cloud, such as item recommendations and activity events.

6.1.1.3 Platform

- *NetWeaver deprecated* - Support for NetWeaver is deprecated and removed from the installer packages.

6.1.2 Feature Drop FD-2305

🖥 **Release date** ➜ 02 Jun 2023

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-6259	API Gateway, GkGo App	Story	[PS] Adapt /transaction/drop also for BASKET txType
POSS-4753	API Gateway	Story	[AGW] Add {keycloak-realm} placeholder option to certificatesUrlPattern
POSS-6181	API Gateway	Story	[AGW] Add {keycloak-realm} placeholder option to certificatesUrlPattern

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-6506	API Gateway	Bug	[AGW] Does not start on-prem test systems
POSS-6448	API Gateway	Bug	[AGW] App log is at wrong path
POSS-6204	API Gateway	Bug	[AGW] Did not work with environment from ENV vars
POSS-6597	Self Scanning Service	Bug	[SSS] Single occurrence of Payment Service HTTP 500 in "prod"
POSS-6552	API Gateway	Bug	[AGW] Secrets should be hidden in case of extendedRestLoggingEnabled

6.1.3 Feature Drop FD-2304

🖥 **Release date** ➜ 05 May 2023

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-6179	API Gateway	Story	[AGW] Add Edge Notification Service registration API (HTTP)
POSS-5764	API Gateway	Story	[AGW] Update CPS endpoints as part of consent flag
POSS-6332	API Gateway	Story	[AGW] Add gift card/certificate status method to API endpoints (Payment Service)
POSS-6322	API Gateway	Story	[AGW] Add gift card/certificate payment method to API gift endpoints (Payment Service)

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-6283	Android, Self Scanning Service	Bug	[SSC] [Android] CPS verification default should be email when reading QR code
POSS-6387	Payment Service	Bug	[SSS] Scales and empties are causing operatorNecessary=true
POSS-6386	Payment Service	Bug	[PS] eReceipt download link not provided to consumer client
POSS-6325	Payment Service, Self Scanning Service	Bug	[PS][iOS] Digital receipt NOT available in app after successful mobile payment
POSS-6311	Payment Service	Bug	[AGW] Missing exception cause in decryption catch
POSS-6204	Payment Service	Bug	[AGW] Does not work with environment from ENV vars

6.1.4 Feature Drop FD-2303

🖥 **Release date** ➜ 31 Mar 2023

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-5356	Payment Service	Story	[PS] Mask accountNumber received in external payment
POSS-4858	Payment Service	Story	[PS] Start settle payment with BASKET_ID instead of TRANSACTION_ID - PS API
POSS-5676	API Gateway	Story	[AGW] Update PS API with basket lifecycle changes

POSS-5581	Payment Service	Story	[PS] Enforce no TX modifications when owner is BS
POSS-4854	Payment Service	Story	[PS] Cancel payment use-case
POSS-4884	Payment Service	Story	[PS] Disable basket finalization logic when BS is owner of basket
POSS-4852	Payment Service	Story	[PS] Send tenderLineItems to Basket Service
POSS-4850	Payment Service	Story	[PS] Load basket from Basket Service
POSS-5588	Payment Service	Story	[PS] Update PS API with new txPaymentFinished flag
POSS-4883	Payment Service	Story	[PS] Persist basket origin at PS database
POSS-4849	Payment Service	Story	[PS] New txIdType BASKET_ID
POSS-5577	Payment Service	Story	[PS] Drop payment use-case - Integration test
POSS-4853	Payment Service	Story	[PS] Drop payment use-case
POSS-5685	Payment Service	Story	[PS] Integration tests with BASKET_ID
POSS-5826	Payment Service	Story	[PS] Implement cancel points payment use-case (basket action)
POSS-5827	Payment Service	Story	[PS] Use MapStruct to map transaction sub-objects in basket action API calls
POSS-5880	API Gateway	Story	[AGW] Add Fiscal Service GET /certificate
POSS-5573	Payment Service	Story	[PS] Verify Basket Service notification handling
POSS-4885	Payment Service	Story	[PS] Persistency of approved tender line items
POSS-5773	API Gateway	Story	[AGW] SAP Air Key Support - Integration
POSS-5544	API Gateway	Story	[AGW] AGW Extension - GK GO age verification
POSS-5706	API Gateway	Story	[AGW] (New PS) Expose PS endpoints to AGW
POSS-6072	API Gateway	Story	[AGW] Add UC6 subscription API
POSS-5707	Self Scanning Service	Story	[SSS] Remove SAP NetWeaver deployment builds support - 5.23 master
POSS-5480	Self Scanning Service	Story	[SSS] Add GK-Passport header to the API - Adopt SSS implementation - 5.23 master
POSS-6179	API Gateway	Story	[AGW] Add Edge Notification Service registration API (HTTP)

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-6196	Self Scanning Service	Bug	[SSS] Cannot be installed on v5.23
POSS-5940	API Gateway	Bug	[AGW] AGW on C4R DEV is sending wrong JWT to digital-distribution-service on SPOT
POSS-6152	API Gateway	Bug	[AGW] AGW uses request's token to call Push Notification Service or SPOT when it could not get token from PNS/SPOT keycloak
POSS-6228	API Gateway	Bug	[AGW] customer-interaction-service API with wrong types (string vs object)

6.1.5   Feature Drop FD-2302

Release date → 03 Mar 2023

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-5524	Self Scanning Service	Story	[SSS] Extract mod-common to common repository
POSS-5258	API Gateway	Story	[CPS] Verify methods must be protected with reCAPTCHA
POSS-5379	API Gateway	Story	[AGW] Update public Shopping List Service API with use-case 6

POSS-5536	Payment Service	Story	[PS] Add TerminalTransactionReferenceNumber to external payment API and adjust mapping
POSS-6560	API Gateway	Hot fix	[AGW] Kubernetes update to 1.25
POSS-6556	Self Scanning Service	Hot fix	[SSS] Kubernetes update to 1.25

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-5613	Payment Service	Bug	[PS] Adyen Dropin payment methods missing
POSS-5775	Payment Service	Bug	[PS] Fiscalization Austria
POSS-5618	Payment Service	Bug	[PS] Finalized transactions from PS in 5.23 are no longer visible in empties reports

6.1.6   Feature Drop FD-2301

🖥 **Release date ➜** 03 Feb 2023

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-5228	API Gateway	Story	[AGW] Improve configuration of routes and decisions when to use TokenAuthFilter
POSS-4651	API Gateway	Story	[AGW] Create dedicated artifact containing only the APIs provided by AGW
POSS-5523	API Gateway	Story	[AGW] Add basket endpoints for Self Scanning Clients
POSS-3025	Self Scanning Service	Story	[SSS] Future-proof copying of external items in the end-of-trip
POSS-5512	API Gateway	Story	[AGW] Update Store Device Control endpoint to enable item-based searches in the Shopping List Service

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-5520	Self Scanning Service	Bug	[SSS] Storemanager editor fixes
POSS-5508	Payment Service	Bug	[PS] PDF binaries are missing after update to FD-2211 - 5.23
POSS-4926	API Gateway	Bug	[AGW] Integrate fixed OpenAPI definitions
POSS-5533	Payment Service	Bug	[PS] External payment should not revert an open transaction in the event of an error
POSS-3563	API Gateway	Bug	[AGW] Check and fix OpenAPI definitions
POSS-5472	Self Scanning Service	Bug	[SSS] Update restrictions/locationId when recalling PUT /transaction-authorization with same txId
POSS-5795	API Gateway	Bug	[AGW] Customer profile registration with username fails with 400

6.1.7   Feature Drop FD-2212

🖥 **Release date ➜** 06 Jan 2023

What's New

/

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-5276	Self Scanning Service	Story	[SSS] Send loyalty information in recalculate request to PCE during EOT
POSS-5272	API Gateway	Story	[AGW] Add MD API for business unit search
POSS-4698	Payment Service	Story	[PS] Fiscal Service ES integration
POSS-5100	Payment Service	Story	[PS] Finish DE fiscalization after transaction is cancelled
POSS-5270	Payment Service	Story	[PS] Payment rollback process
POSS-5230	Payment Service	Story	[PS] Implement transaction level locking
POSS-2397	Self Scanning Service	Story	[SSS] Set fixed time zone for IT
POSS-4191	API Gateway	Story	[AGW] Add integration test support
POSS-4998	Self Scanning Service	Story	[SSS] SM Configuration for LS calls

POSS-4697	Payment Service	Story	[PS] Fiscal Service AT integration
POSS-5314	Payment Service	Story	[PS] Add LoyaltyService ExtensionKey to the transaction - 5.23 master
POSS-5340	Payment Service	Story	[PS] Increase fiscal mapping library

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-5282	API Gateway	Bug	[AGW] Fix BasicAuthenticationPropagationFilter when ssc-byod-anonymous client is removed - 5.23 master
POSS-5313	Self Scanning Service, Payment Service	Bug	[SSS/PS] Transactions created by SSS/PS always have SequenceNumber '0'
POSS-4989	API Gateway	Bug	[AGW] AGW should not fill GK-Customer-Id for the anonymous customer - 5.23 master
POSS-5396	API Gateway	Bug	[AGW] Missing APIs in Confluence + bugs in the upload
POSS-5451	Shopping List Service	Bug	[SLS] Correct the Boolean checkbox editors in Storemanager
POSS-5187	Payment Service	Bug	[PS] Missing SM config for e-receipt upload URL
POSS-5347	Payment Service	Bug	[PS] Handle all errors with DE fiscalization
POSS-5339	Payment Service	Bug	[PS] Fix fiscalization process error handling
POSS-5472	Self Scanning Service	Bug	[SSS] Update restrictions/locationId when recalling PUT /transaction-authorization with same txId

6.1.8   Feature Drop FD-2211

🖥 **Release date** ➜ 02 Dec 2022

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-5159	API Gateway	Story	[AGW] New API for anonymous customer accounts
POSS-5020	API Gateway	Story	[AGW](LS) Add tierId to the GET /current/loyalty-accounts endpoint
POSS-4810	Payment Service	Story	[PS] Extend external-payment to support CASH, TERMINAL payment types - Implementation
POSS-4808	Payment Service	Story	[PS] Extend external-payment to support CASH, TERMINAL payment types - API
POSS-4772	Payment Service	Story	[PS] Remove idempotency key workaround
POSS-4901	API Gateway	Story	[AGW] Consolidate log configuration
POSS-4032	API Gateway	Story	[AGW] "GK-" headers should not be allowed from the client
POSS-5101	API Gateway	Story	[AGW] Enable token exchange for SPOT cloud communication
POSS-4949	API Gateway	Story	[AGW] Add Push Notification Service API in AGW
POSS-4951	API Gateway	Story	[AGW] Add Basket Notification Service API in AGW
POSS-5021	API Gateway	Story	[AGW](CPS) Customer registration endpoints should work without a token
POSS-4921	API Gateway	Story	[AGW] Publish Digital Distribution Service on AGW
POSS-4872	Payment Service	Story	[PS] Implement blacklist for transaction extensions during transaction retrieval
POSS-5100	Payment Service	Story	[PS] Finish DE fiscalization after transaction is cancelled
POSS-4855	Payment Service	Story	[PS] Migrate Fiscal Service DE integration to common support
POSS-4697	Payment Service	Story	[PS] Fiscal Service AT integration
POSS-4698	Payment Service	Story	[PS] Fiscal Service ES integration
POSS-4567	API Gateway	Story	[AGW] Add item search service API
POSS-4993	Self Scanning Service	Story	[SSS] Logic to call Loyalty Service to retrieve customer loyalty information
POSS-	Self Scanning	Story	[AGW] Improve calling for keycloak's token (refresh token, etc.)

5107	Service		

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-5135	Payment Service	Bug	[PS] Payment not done but store could be exited
POSS-4963	Payment Service	Bug	[PS] Fix thrown TransactionUtilsException in calculatePaymentAmount
POSS-4930	Self Scanning Service	Bug	[SSS] Fix OpenAPI definitions
POSS-2857	Payment Service	Bug	[PS] If externalPayment fails, there is still a finalized transaction (without tenders)
POSS-4931	API Gateway	Bug	[AGW] Incorrect default configuration for cloud
POSS-4446	API Gateway	Bug	[AGW] Logging of the network communication on the cloud

6.1.9   Feature Drop FD-2210

🖥 **Release date →** 04 Nov 2022

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-3851	API Gateway	Story	[AGW] Automatic update of swagger versions in Confluence

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-4819	API Gateway, CPS	Bug	[AGW][LS] GDPR records not created consistently

6.2   5.22 Versions

Version 5.22.0 is an intermediate release and not intended for Premium Qualification. It is based on feature drop 5.22.0-FD-2209 and will also include the issues fixed in any previous feature drop.

🖥 **Release date →** 06 Oct 2022

6.2.1   Key Features

6.2.1.1 API Gateway Interface Updates

Definition files for interfaces provided over API Gateway have been updated to support the new functionality of the attached backend and frontend systems:

- GK GO endpoints are now published over API Gateway.

6.2.1.2 Multitenancy

- Migration of the default tenant to 000 and the default realm to 000-customers

6.2.1.3 Self Scanning Service/Payment Service

- Users now have the option of paying with their points (points as tender). Cancellation of this type of payment is also an option.

- The same tender that was used for payment must be used for the refund.

6.2.1.4 Security

- All exception messages have been sanitized

- Clients use OAuth 2.0. to communicate with the services. They use JWT access tokens for authentication at central and edge services and get a JWT refresh token that is used to get new JWT access tokens before expiration and also a new JWT refresh token.

6.2.2 5.22.0-FD-2209 (Feature Drop)

Release date → 06 Oct 2022

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-4234	Payment Service	Story	[PS] Introduce conversion extension -> Correlation in transaction finalization
POSS-4639	API Gateway	Story	[AGW][LS] Add public endpoint for customer loyalty account creation and deletion
POSS-2556	Self Scanning Service	Story	[SSS] Require a special employee role to call status endpoint
POSS-4383	API Gateway, Shopping List Service	Story	[AGW] Add SLS item maintenance API to AGW
POSS-4380	API Gateway, Shopping List Service	Story	[AGW] Add SLS UC1 API to AGW
POSS-4666	API Gateway	Story	[AGW][LS] Add promotionPointRedemptionFactor to GET /loyalty/v1/customers/current/loyalty-accounts endpoint
POSS-4747	API Gateway	Story	[AGW] Extend endOfTrip v2 by customerCardId
POSS-4689	API Gateway	Story	[AGW][LS] Update points history on API Gateway
POSS-4545	Payment Service	Story	[PS] Create journal binary
POSS-4745	Self Scanning Service	Story	[SSS] Extend endOfTrip v2 by customerCardId - Points collection process
POSS-4557	Payment Service	Story	[PS] Implement "cancel" endpoint for points payment
POSS-4765	Payment Service	Story	[PS] Introduce new PAYMENT_STARTED basket state into payment handling
POSS-4537	API Gateway	Story	[AGW] Update passport library

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-4185	Payment Service	Bug	[PS] Fix payment init idempotency for transaction ID type SUSPEND_NO
POSS-4499	API Gateway, Payment Service	Bug	[PS][AGW] Problem when retrieving transaction on SCO
POSS-4740	Self Scanning Service	Bug	[SSS] Fiscal info wrongly encoded
POSS-4165	Payment Service	Bug	[PS] Fix payment init idempotency for other transaction ID types
POSS-1931	Self Scanning Service	Bug	[SSS] EOT fraud detection features are not compliant with FDS (and its original requirements)
POSS-4632	API Gateway, Loyalty Service	Bug	[AGW][LS] REST API upload does not work correctly
POSS-4464	API Gateway	Bug	[AGW] Calling Configuration Service should not be allowed with Basic Auth (only OAuth2 is allowed)
POSS-4704	Payment Service	Bug	[PS] GK GO use-case with one click payment does not work (NPE)
POSS-4775	Payment Service	Bug	[PS] The old amount is still present in the next payment after the option to pay with points is cancelled, so two payments are needed.
POSS-4776	Payment Service	Bug	[PS] User cannot pay with points after cancelling points payment
POSS-4791	Self Scanning Service	Bug	[SSS] Kafka topic prefix is not automatically set during deployment
POSS-4777	Payment Service	Bug	[PS] Cancelation of points payment does not check if the paymentId links to points payment
POSS-4789	API Gateway	Bug	[AGW] Calling the Configuration Service should not be allowed with Basic Auth

6.2.3 5.22.0-FD-2208 (Feature Drop)

Release date → 02 Sep 2022

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-3474	Payment Service	Story	[PS] Pre-authorized checkout - Add DB index for payment status

POSS-3906	Payment Service	Story	[PS] Define API for promotion points payment
POSS-3911	API Gateway	Story	[AGW] Publish API for promotion points payment
POSS-3944	Payment Service	Story	[PS] Implement points payment

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-3705	Payment Service	Bug	[PS] Fiscalization failing for linked scale receipts
POSS-3562	API Gateway	Bug	[AGW] Validation does not work - 5.22
POSS-3550	Payment Service	Bug	[PS] Fix calling Checkout Service
POSS-4465	API Gateway	Bug	[AGW] Clean up application-docker.yaml
POSS-4474	API Gateway	Bug	[AGW] Websocket authentication takes wrong password for anonymous customer
POSS-3664	API Gateway	Bug	[AGW] Validation of some endpoints does not work
POSS-4541	Payment Service	Bug	[PS] Time zone removed for correlated transactions
POSS-4622	Payment Service	Bug	[PS] Duplicate receipt ID after workstationId is changed for an open transaction

6.2.4   5.22.0-FD-2207 (Feature Drop)

🖥 **Release date → 29 Jul 2022**

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-4306	API Gateway	Story	[AGW] Multitenancy - Redirect to correct keycloak realm
POSS-4188	API Gateway	Story	[AGW] Secure Client Onboarding - 5.22
POSS-3893	API Gateway	Story	[AGW] Multitenancy - Send tenant ID from OAuth token as header
POSS-4238	API Gateway	Story	[AGW] Multitenancy - OAauth 2.0
POSS-4222	API Gateway	Story	[AGW] Add restrictions to Help requests REST API
POSS-3722	API Gateway	Story	[AGW] Allow websocket connection to Event Service
POSS-3945	Payment Service	Story	[PS] True Anonymous Customers - 5.22 master
POSS-3862	Payment Service	Story	[PS] Invalidate payment OTP after usage
POSS-3942	API Gateway	Story	[AGW] True Anonymous Customers - 5.22 master
POSS-3172	API Gateway	Story	[AGW] Info version value should be provided automatically
POSS-3868	Payment Service	Story	Points as tender - Refinement
POSS-3173	API Gateway	Story	[AGW] Add app-info endpoint
POSS-3774	API Gateway	Story	[AGW] API changes: oldPin (plain) and optional
POSS-3948	API Gateway	Story	[AGW] Expose APIs for help requests - Add POST request
POSS-3943	Self Scanning Service	Story	[SSS] True Anonymous Customers - 5.22 master
POSS-3691	Payment Service	Story	[PS] Update version of fiscal service API
POSS-4258	API Gateway	Story	[AGW] Support anonymous tokens in websocket forwarding
POSS-4271	Self Scanning Service	Story	[SSS] Implement Kafka authentication
POSS-3234	Payment Service, Self Scanning Service	Story	[PS] [SSS] Refactor caching on the Self Scanning Service to enable it in the Payment Service as well to obtain the business unit from SDC
POSS-3540	API Gateway	Story	[AGW] (CPS) Passport support for GDPR - 5.22 master
POSS-3910	API Gateway	Story	[API GW] Expose new Basket Service API to search for basket by externalClientId
POSS-3951	Payment Service	Story	[PS] In-App Payment - Call Basket Service with PAYMENT_FINISHED when settled
POSS-3991	Self Scanning Service	Story	[SSS] Secure Client Onboarding - Merge to 5.22
POSS-3494	Payment Service	Story	[PS] Extend payment methods by merchantAccount
POSS-	Payment Service	Story	[PS] Possibility to load non-suspended transactions

3201			
POSS-3716	API Gateway	Story	[AGW] Expose APIs for help requests

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-3170	API Gateway, Self Scanning Service, Payment Service	Bug	[SSS][PS][AGW] Empty customer ID should not be allowed in the REST API
POSS-3585	API Gateway	Bug	[AGW] (PS) 400 Bad Request when calling /payments/v1/pre-authorizations/one-time-password
POSS-3564	Payment Service	Bug	[PS] 401 when calling payment-proxy/method with JWT token (from CPS/keycloak)
POSS-3916	API Gateway	Bug	[AGW] (DSG) Cannot get images from DSG when the path contains a slash - 5.22 master
POSS-3915	API Gateway	Bug	[AGW] (DSG) Enable DSG validation
POSS-3736	Self Scanning Service	Bug	[SSS] Error creating bean with the name 'crmAdapter' - Not starting in cloud
POSS-4036	Self Scanning Service	Bug	[iOS] Amounts are overwritten after recalculate call
POSS-3865	API Gateway	Bug	[AGW] SSC - Image download API exposes complete DSG to the Internet - 5.22 master
POSS-4372	Payment Service	Bug	[PS][GK Go] Payment Service does not support SUSPEND_NO for GK GO (SCL) transactions
POSS-4037	Self Scanning Service	Bug	[Android] Amounts are overwritten after recalculate call
POSS-4443	API Gateway	Bug	[AGW] Fix Config Service authorization and clean up cloud templates

6.2.5   5.22.0-FD-2206 (Feature Drop)

🖼 **Release date → 01 Jul 2022**

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-2260	SSS	Story	[SSS] Sanitize all exception messages. Sanitization done in the common exceptions (shared components) and other exceptions.
POSS-4007	Payment Service	Story	[PS] Bottlenecks were identified and improvements were made to the Payment Service in the context of GK GO (payment preauthorization, payment settlement operations).

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-3988	Payment Service	Bug	[PS] Payment Service returns an exception when calling paymentInit for a second time (e.g. payment was canceled the first time).

6.2.6   5.22.0-FD-2205 (Feature Drop)

🖼 **Release date → 03 Jun 2022**

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-3173	API Gateway	Story	[AGW] Add app-info endpoint
POSS-3172	API Gateway	Story	[AGW] Info version value should be provided automatically
POSS-3714	API Gateway	Story	[AGW] Modify config service validation to allow GKR-gk-go
POSS-3942	API Gateway	Story	[AGW] True Anonymous Customers - 5.22 master

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-3865	API Gateway	Bug	[AGW] SSC - Image download API exposes complete DSG to the Internet - 5.22 master
POSS-3916	API Gateway	Bug	[AGW] (DSG) Cannot get images from DSG when the path contains a slash - 5.22 master

7 Release Notes – Employee App

This document describes the functional and technical news and improvements relating to the following applications and services in the latest version:

- **Employee Hub**

Additional information can be found in the following documents:

- Installation Guide: installation

- Operation Guide: operation, monitoring

- Upgrade and Update Guide: update process

- Security Guide: encryption, password handling, user management

- Product Description: product information

- Customizing Guide: configuration information

- Customizing Reference: parameter description for configuration needs

- User Guide: instructions for use

- Sizing Guide: deployment, technical data relating to CPU, hard disc, etc.

Use the table of contents to jump directly to the appropriate version:

7.1 5.23 Versions (SAP 7.6)

Version 7.6 (5.23.0) is released based on feature drop FD-2305 and will also include the issues fixed in any previous feature drop.

📷 **Release date** ➔ 02 Jun 2023

7.1.1 UI Changes

- This versions includes minor UI adjustments such as adding the possibility to sort SCO stations in the SCO widget or the removal of the welcome section in the main screen.

- The Employee App is now called the Employee Hub.

7.1.2 Feature Drop FD-2304

📷 **Release date** ➔ 05 May 2023

What's New

/

Fixed Issues

/

7.1.3 Feature Drop FD-2303

📷 **Release date** ➔ 30 Mar 2023

What's New

/

Fixed Issues

/

7.1.4   Feature Drop FD-2302

🖼 **Release date** ➜ 03 Mar 2023

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-3037	Employee App	Story	[Employee App] Sorting of SCO stations
POSS-4805	Employee App	Story	Employee App - Remove Hello/Welcome Section

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-5614	Employee App	Bug	[Employee App] Never-ending loop during confirmation of age-restricted items
POSS-5900	Employee App	Bug	[Employee App] Error loading customer transaction

7.1.5   Feature Drop FD-2301

🖼 **Release date** ➜ 03 Feb 2023

What's New

No changes in this version.

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-5448	Employee App	Bug	[Employee App] Infopoint name is not shown correctly when SSC BYOD is scanned at infopoint
POSS-5611	Employee App	Bug	[Employee App] Rescan functionality throwing "Error loading customer transaction"

7.1.6   Feature Drop FD-2212

🖼 **Release date** ➜ 06 Jan 2023

What's New

No changes in this version.

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-5447	Employee App	Bug	[Employee App] Rounding issue inside age verification

7.1.7   Feature Drop FD-2211

🖼 **Release date** ➜ 02 Dec 2022

What's New

No changes in this version.

Fixed Issues

No fixes in this version.

7.1.8   Feature Drop FD-2210

🖼 **Release date** ➜ 04 Nov 2022

What's New

No changes in this version.

Fixed Issues

No fixes in this version.

7.2   5.22 Versions

Version 5.22.0 is an intermediate release and not intended for Premium Qualification. It is based on feature drop **5.22.0-FD-2209** and will also include the issues fixed in any previous feature drop.

🖼 **Release date** ➜ 06 Oct 2022

7.2.1   Key Features

7.2.2   5.22.0-FD-2209 (Feature Drop)

🖼 **Release date** ➜ 06 Oct 2022

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-3842	Employee App	Story	[Employee App] Improve user guidance in scanner view
POSS-4577	Employee App	Story	[Employee App] Minor UI improvements

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-2936	Employee App	Bug	Rescan transaction retrieval - Line item association
POSS-4769	Employee App	Bug	Age verification and price rounding buttons missing
POSS-4768	Employee App	Bug	No option to select the age on iOS

7.2.3   5.22.0-FD-2208 (Feature Drop)

🖼 **Release date** ➜ 02 Sep 2022

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-4517	Employee App	Story	[Launchpad Lite] GK GO: Add Basket Service endpoint in commonApi
POSS-3808	Employee App	Story	[Employee App] GK GO: Age verification process
POSS-3277	Employee App	Story	[Employee App] Consolidate empty lists views
POSS-3632	Employee App	Story	[Employee App] Cloud template package (docker + helm) like ssc-byod-cloud-template

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-3230	Employee App	Bug	[Employee App][iOS] Unable to load the transaction when calling employee at Infopoint
POSS-3236	Employee App	Bug	[Employee App] Incorrect authorization for multiple restricted items
POSS-4060	Employee App	Bug	[Employee App] Notification toaster message not aligned properly
POSS-3874	Employee App	Bug	[iOS] Employee App redirects to welcome page if closed after login
POSS-3873	Employee App	Bug	[Android] Employee app redirects to welcome page if closed after login

7.2.4   5.22.0-FD-2207 (Feature Drop)

🖼 **Release date** ➜ 29 Jul 2022

What's New

No changes in this version.

Fixed Issues

No changes in this version.

7.2.5   5.22.0-FD-2206 (Feature Drop)

🖼 **Release date** ➜ 01 Jul 2022

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-4225	Employee App	Story	Employee App - Passed Fortify tests
POSS-3177	Employee App	Story	[Employee App] Consumer app help requests

Fixed Issues

No changes in this version.

7.2.6   5.22.0-FD-2206 (Feature Drop)

Release date → 01 Jul 2022

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-4225	Employee App	Story	Employee App - Passed Fortify tests

Fixed Issues

No changes in this version.

7.2.7   5.22.0-FD-2205 (Feature Drop)

Release date → 03 Jun 2022

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-3632	Employee App	Story	Employee App - Cloud template package (docker + helm) like ssc-byod-cloud-template

Fixed Issues

No changes in this version.

7.3   5.21 Versions (SAP 7.5)

Version 7.5 (5.21.0) is released based on feature drop 5.21.0-FD-2204 and will also include the issues fixed in any previous feature drop.

Release date → 03 May 2022

7.3.1   Key Features

New Employee App: This application supports store personnel when helping customers during their self scanning trips.

7.3.1.1 Fraud Detection Management

- With this functionality, the store employee can increase the flow of customers that are waiting to pay for their shopping baskets, without having to go through the centralized configuration logic that exists now. The function can change the configured behavior of the Fraud Detection Service in such a way that fraud detection can be fully disabled for a certain amount of time, or the configuration can be set to a specific predefined profile.

7.3.1.2 Age Restriction Handling

- Certain product categories can only be sold to customers after a manual age check to prevent these products from being purchased by customers under a certain age. The Employee App also offers the option of performing this age check during self-scanning trips in direct contact with the customer, allowing them to enjoy the benefits of a virtually frictionless shopping experience.

7.3.2   5.21.0-FD-2204 (Feature Drop)

Release date → 29 Apr 2022

What's New

No changes in this version.

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary

POSS-3275	Employee App	Story	[Employee App] - Fortify - Pipeline and fixes
POSS-3696	Employee App	Bug	[Employee App] - Error loading the Infopoint transactions from the Events List tile

7.3.3   5.21.0-FD-2203 (Feature Drop)

📇 **Release date** ➔ 01 Apr 2022

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-3243	Employee App	Story	[Employee App] - Update localization files on-the-fly
POSS-2790	Employee App	Story	[Employee App] - Age verification triggered by SCO via Event Service
POSS-3244	Employee App	Story	[Employee App] Logging Service connection - E2E TEST

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-3241	Employee App	Bug	[Employee App] Duplicate events for the same transaction are displayed in the Infopoint tile
POSS-3397	Employee App	Bug	[Employee App] Payment failing when rescan is successful
POSS-3362	Employee App	Bug	[Employee App] Unable to load sale restricted transactions
POSS-3346	Employee App	Bug	[Employee App] Init screen not displayed
POSS-3274	Employee App	Bug	[Employee App] Placeholder for additional COOP bugs and GKRI

7.3.4   5.21.0-FD-2202 (Feature Drop)

📇 **Release date** ➔ 28 Feb 2022

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-2474	Employee App	Story	[Employee App] Fraud Detection - Implementation of Hour selection UI
POSS-2475	Employee App	Story	[Employee App] Fraud Detection - Implementation of Timer UI
POSS-2551	Employee App	Story	[Employee App] Fraud Detection - Generation of API client for fraud-detection-config/v1 endpoint
POSS-2476	Employee App	Story	[Employee App] Fraud Detection - Implementation of Swagger files and communication to backend

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-3268	Employee App	Bug	[Employee App] UI bug SCO overview: Filtering and sorting
POSS-3266	Employee App	Bug	[Employee App] Configuration Service authentication using hardcoded Basic Authentication
POSS-3267	Employee App	Bug	[Employee App] UI bug for cash recycler events
POSS-2784	Employee App	Bug	[Employee App] Void items in transaction can be scanned from Employee App

7.3.5   5.21.0-FD-2201 (Feature Drop)

📇 **Release date** ➔ 04 Feb 2022

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-2791	Employee App	Story	[Employee App] Kafka client implementation
POSS-2792	Employee App	Story	[Employee App] SCO States List Overview
POSS-2793	Employee App	Story	[Employee App] Help request
POSS-2796	Employee App	Story	[Employee App] Support of general events
POSS-2890	Employee App	Story	[Employee App] Support widgets in Launchpad
POSS-2958	Employee App	Story	[Employee App] SCO State Detail Overview
POSS-2997	Employee App	Story	[Employee App] Display event notifications according to event severity

POSS-3036	Employee App	Story	[Employee App] Filter by SCO station
POSS-3003	Employee App	Story	[Employee App] Load configurations
POSS-3047	Employee App	Story	[Employee App] Extract strings into properties files
POSS-3109	Employee App	Story	[SM] Update template for Employee App configs
POSS-3101	Employee App	Story	[Employee App] Infopoints tile in Launchpad Lite
POSS-3180	Employee App	Story	[Employee App] Events List Tile
POSS-3044	Employee App	Story	[Employee App] Logging Service connection

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-3208	Employee App	Bug	[Employee App] Login button UI change
POSS-3178	Employee App	Bug	[Employee App] Event counts displayed in the main screen are incorrect
POSS-3217	Employee App	Bug	[Employee App] Infopoint event is not appearing in the Employee App for a second time
POSS-3233	Employee App	Bug	[Employee App] Age verification missing exception handling
POSS-3215	Employee App	Bug	SCO states are only updating when logging in to the Employee App again
POSS-3214	Employee App	Bug	[Employee App] Rescan functionality should use basic authentication
POSS-3209	Employee App	Bug	[Employee App] Event counts displayed in the main screen are incorrect (go into Settings and then back to main screen)

7.3.6   5.21.0-FD-2110 (Feature Drop)

🖥 **Release date → 29 Oct 2021**

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-2655	Employee App	Story	[Employee App] Age verification/data mode - Jump to next field and removal of red info

Fixed Issues

No changes in this version.

8   Release Notes – Wall Device Manager

This document describes the functional and technical news and improvements relating to the following applications and services in the latest version:

- **Wall Device Manager**

- **Wall Device Manager Scanner**

Additional information can be found in the following documents:

- Installation Guide: installation

- Operation Guide: operation, monitoring

- Upgrade and Update Guide: update process

- Security Guide: encryption, password handling, user management

- Product Description: product information

- Customizing Guide: configuration information

- Customizing Reference: parameter description for configuration needs

- User Guide: instructions for use

- Sizing Guide: deployment, technical data relating to CPU, hard disc, etc.

Use the table of contents to jump directly to the appropriate version:

8.1   5.23 Versions (SAP 7.6)

Version 7.6 (5.23.0) is released based on feature drop FD-2305 and will also include the issues fixed in any previous feature drop.

🖥 **Release date** ➔ 02 Jun 2023

8.1.1   Key Features

8.1.1.1 New Branding

- New branding for the WDM as part of the overall company-wide rebranding.

8.1.1.2 Security

- Client security when communicating with the backend is now ensured with OAuth 2.0.

8.1.2   Feature Drop FD-2305

🖥 **Release date** ➔ 02 Jun 2023

What's New

No changes in this version.

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-6462	WDM	Bug	[WDM] Cannot scroll to the end in Device Overview

No fixes in this version.

8.1.3   Feature Drop FD-2304

🖥 **Release date** ➔ 05 May 2023

What's New

No changes in this version.

Fixed Issues

No fixes in this version.

8.1.4   Feature Drop FD-2303

🖥 **Release date** ➔ 31 Mar 2023

Hot Fixes

Issue Key	Component(s)	Issue Type	Summary
PBLM-6819	WDM, WDM Scanner	HF	Wall Device Manager fails to start due to an error during the onboarding operation.

What's New

No changes in this version.

Fixed Issues

No fixes in this version.

8.1.5   Feature Drop FD-2302

🖥 **Release date** ➜ 03 Mar 2023

What's New

No changes in this version.

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-5574	WDM	Bug	[WDM] Logo background does not match screen background

8.1.6   Feature Drop FD-2301

🖥 **Release date** ➜ 03 Feb 2023

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-5373	WDM	Story	[WDM] Secure Client Onboarding implemented on the Wall Device Manager
POSS-5494	WDM	Story	[WDM] Comparison method violates its general contract (IllegalArgumentException)

8.1.7   Feature Drop FD-2212

🖥 **Release date** ➜ 06 Jan 2023

What's New

No changes in this version.

Fixed Issues

No changes in this version.

8.1.8   Feature Drop FD-2211

🖥 **Release date** ➜ 02 Dec 2022

What's New

No changes in this version.

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-3693	WDM	Bug	WDM considers MC18 device to have OUT_OF_SERVICE status incorrectly

8.1.9   Feature Drop FD-2210

🖥 **Release date** ➜ 04 Nov 2022

What's New

No changes in this version.

Fixed Issues

No fixes in this version.

8.2   5.22 Versions

Version 5.22.0 is an intermediate release and not intended for Premium Qualification. It is based on feature drop **5.22.0-FD-2209** and will also include the issues fixed in any previous feature drop.

🖥 **Release date** ➜ 06 Oct 2022

8.2.1 Key Features

8.2.2 5.22.0-FD-2209 (Feature Drop)

🖥 **Release date** ➜ 06 Oct 2022

What's New

No updates

Fixed Issues

Issue Key	Component(s)	Issue Type	Summary
POSS-4526	WDM	Bug	[WDM] There was an error during WDM installation (missing client security placeholder) and the installation could not be completed.

8.2.3 5.22.0-FD-2208 (Feature Drop)

🖥 **Release date** ➜ 02 Sep 2022

What's New

No changes in this version.

Fixed Issues

No changes in this version.

8.2.4 5.22.0-FD-2207 (Feature Drop)

🖥 **Release date** ➜ 29 Jul 2022

What's New

No changes in this version.

Fixed Issues

No changes in this version.

8.2.5 5.22.0-FD-2206 (Feature Drop)

🖥 **Release date** ➜ 01 Jul 2022

What's New

/

Fixed Issues

No changes in this version.

8.2.6 5.22.0-FD-2205 (Feature Drop)

🖥 **Release date** ➜ 03 Jun 2022

What's New

No changes in this version.

Fixed Issues

No changes in this version.

8.3 5.21 Versions (SAP 7.5)

Version 7.5 (5.21.0) is released based on feature drop 5.21.0-FD-2204 and will also include the issues fixed in any previous feature drop.

🖼 **Release date** ➜ 03 May 2022

8.3.1 Key Features

8.3.1.1 New Branding

- Wall Device Manager UI shows the new GK theme.

8.3.1.2 Technical Maintenance

- We reduced the package size significantly to speed up the app loading time and footprint.
- We updated the log4j libraries to the newest version to mitigate the possible risks of exploiting the log4shell vulnerability.

8.3.2 5.21.0-FD-2204 (Feature Drop)

🖼 **Release date** ➜ 29 Apr 2022

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-3666	WDM	Story	[Self Scanning] Support for Fortify source code uploading process

Fixed Issues

No changes in this version.

8.3.3 5.21.0-FD-2202 (Feature Drop)

🖼 **Release date** ➜ 28 Feb 2022

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-3307	WDM	Story	WDM master - Resolve Fortify issues after migration to UI5 v1.71.31
POSS-3269	WDM	Story	WDM master - Migration to UI5 v1.71.31
POSS-2957	WDM	Story	Update WDM with new screen design

Fixed Issues

No changes in this version.

8.3.4 5.21.0-FD-2112 (Feature Drop)

🖼 **Release date** ➜ 07 Jan 2022

What's New

Issue Key	Component(s)	Issue Type	Summary
POSS-2499	Wall Device Manager	Story	[WDM] Package size reduction - 5.21 / master
POSS-3048	Wall Device Manager	Story	[WDM] Ensure safe use of log4j in WDM 5.21

Fixed Issues

No changes in this version.

9 User Guide – Employee App

9.1 Introduction

This document is the user guide for the Employee App of the GK/Retail Business Suite. This application will provide support to the employee in the store.

With this application, employees can, for example, approve sales restrictions in direct contact with the customer or perform partial rescans, if this was triggered by the Fraud Detection Service. This removes the need to queue at a stationary POS or Self Checkout station just to get an approval.

It is also possible to perform a partial rescan on the Employee App. Rescans might be triggered by the Fraud Detection Service and require a member of the store staff to scan a random selection of items in the given basket. If this scan does not reveal any differences, the customer is allowed to continue with the payment on their mobile device.

A further functionality allows the Fraud Detection configuration to be temporarily overridden. When there is a high volume of customers in the store and the current configuration of the Fraud Detection Service generates more rescan requests than viable, the employee is able to adjust this behavior or switch it off completely. After the specified time, the fraud detection will be switched on again automatically.

The Employee App also shows events from SCO stations and POS Clients, such as help requests, notifications, or other technical events.

9.2 Employee App Functions

The functions available in the application are displayed as tiles on an overview screen. The user can select the corresponding tile to start the function.
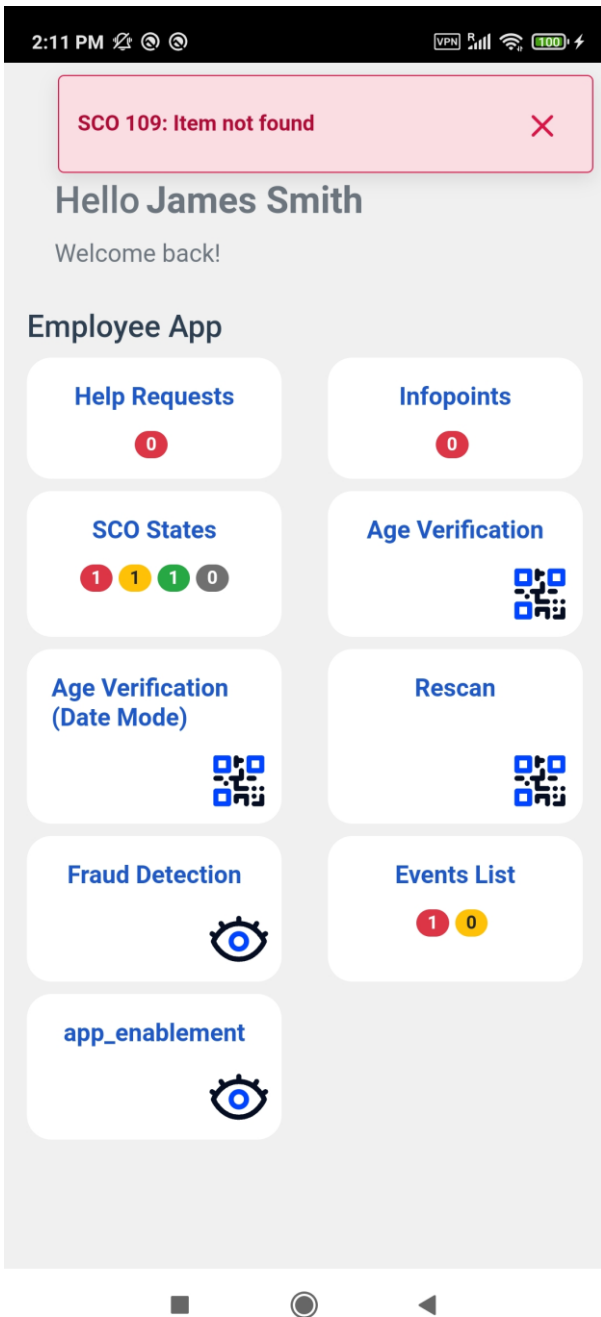
9.2.1 Help Requests

The Employee App provides a dedicated function for displaying all help requests triggered by an SCO station or POS Client.

The number of open requests is displayed as a red number inside the function tile. To see the details of the request, the user has to:

- Navigate to the **Help Requests** function and start the function

The application will show the list of open requests together with the timestamp and SCO Station or POS Client name. The user can mark the request as resolved by pressing the corresponding button.
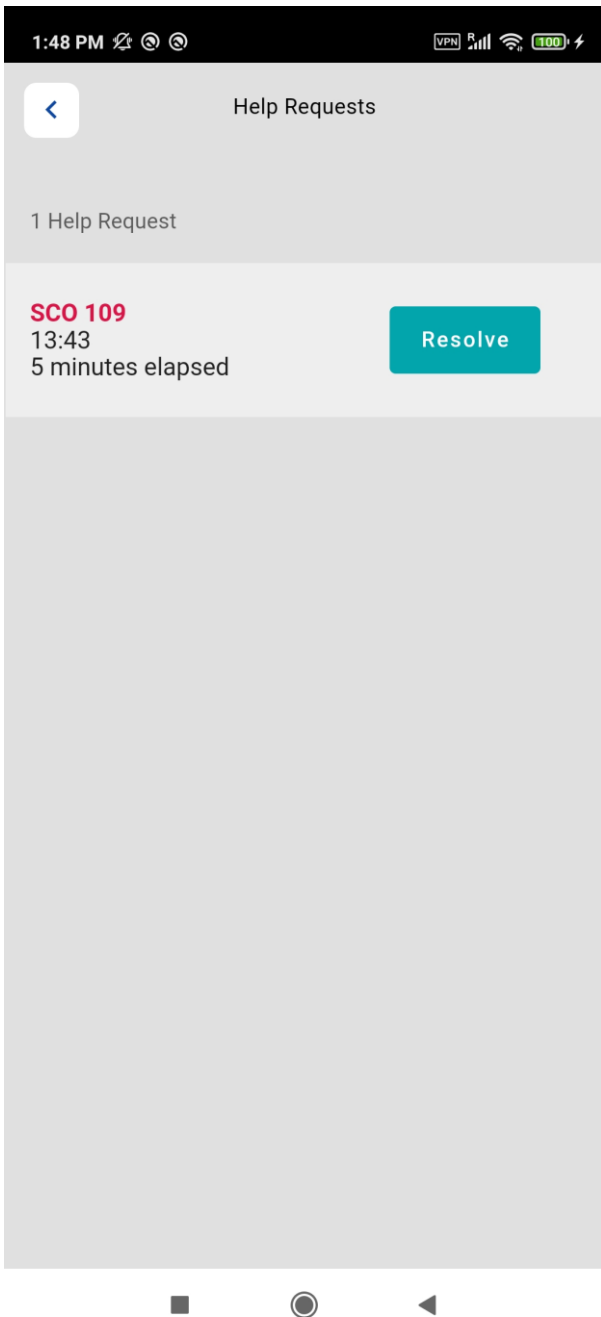
9.2.2 SCO Overview

The SCO Overview function provides the state of the SCO stations, so the employee can have a real-time overview.

On the function tile, the user can see the number of SCO stations in a specific state. The basic states are Available, Warning, Blocked, and Offline.

By opening the function, the user will see a list of all SCO stations together with their state. The list can be ordered by priority of their state or by their station number.

When the user selects a station status, the Employee App displays an overview of the events associated with that station, including a timestamp and the SCO Station name. The list can be sorted by event ID in ascending or descending order.
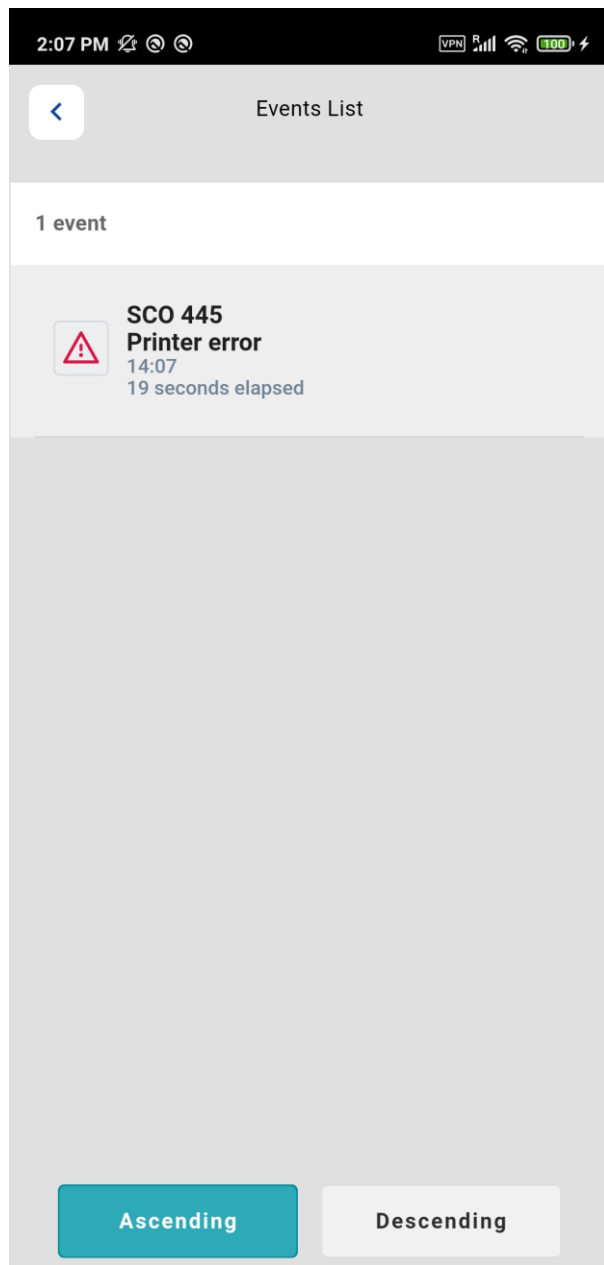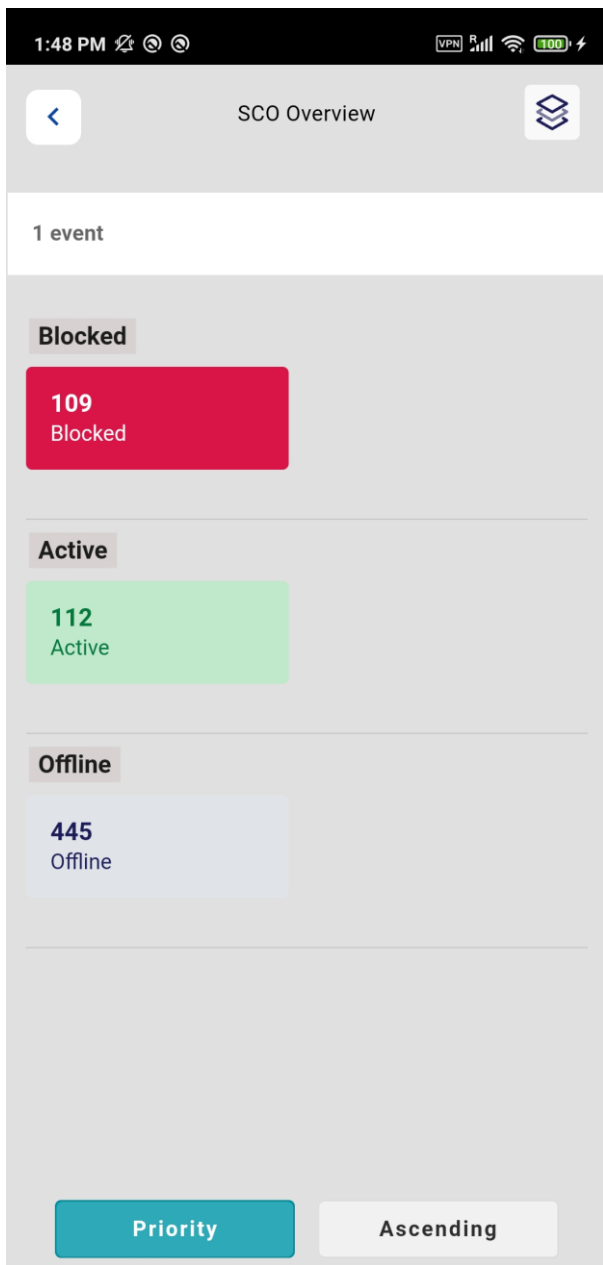
In general, the events are information for the store employee that manual interaction is required at the given SCO station. Therefore, most events have to be resolved at the station itself. This includes events for a **printer error** (the attached printer returned an error), **item not found** (the scanned item could not be identified in the master data), **item locked** (the scanned item was blocked for sale), **manual quantity** (the item master data requires a store employee to enter the quantity manually).

Timeout on open receipt events are generated when an SCO station has not performed an operation on an open receipt for more than 5 minutes. This event can be resolved by pressing the appropriate button. The Employee App then sends the information back to the affected SCO station, which cancels the open receipt.
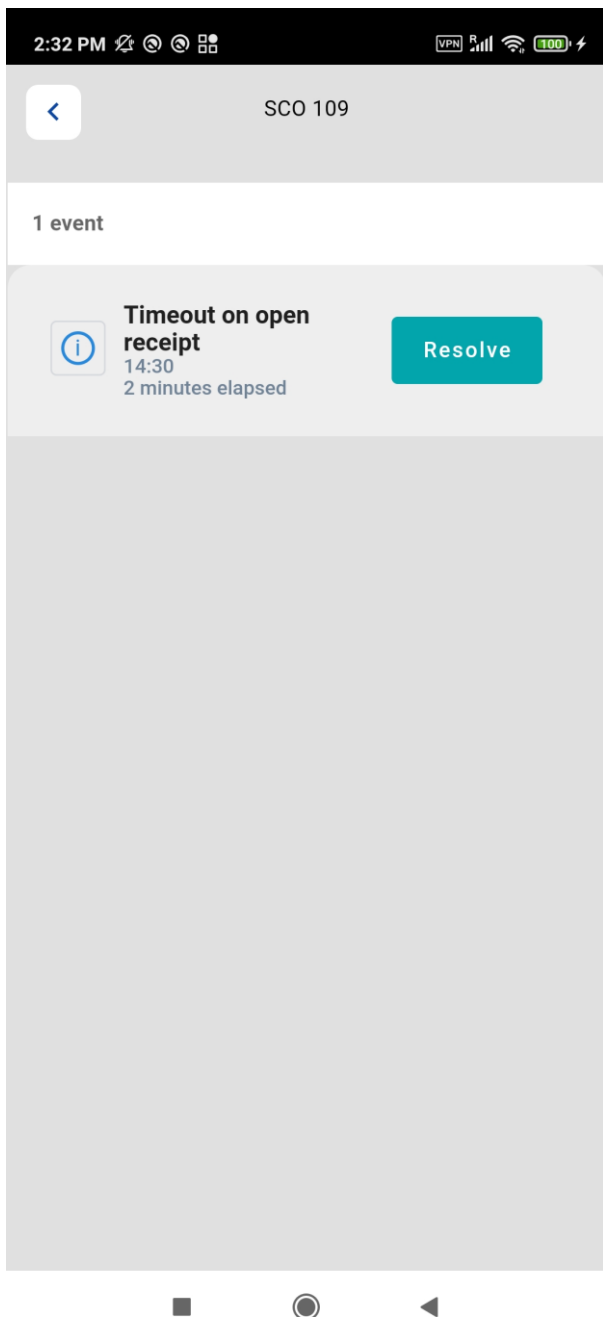
An **age verification** event is generated on the SCO when the receipt contains an item that may only be sold to customers of a defined minimum age. This has to be approved by a store employee. The employee can do this either on the station itself or by:

- clicking on the age restriction event
- selecting the customers age in the pop-up

The information is then sent back to the SCO station, which saves the approval in the receipt. In this case, the customer can proceed with the payment.
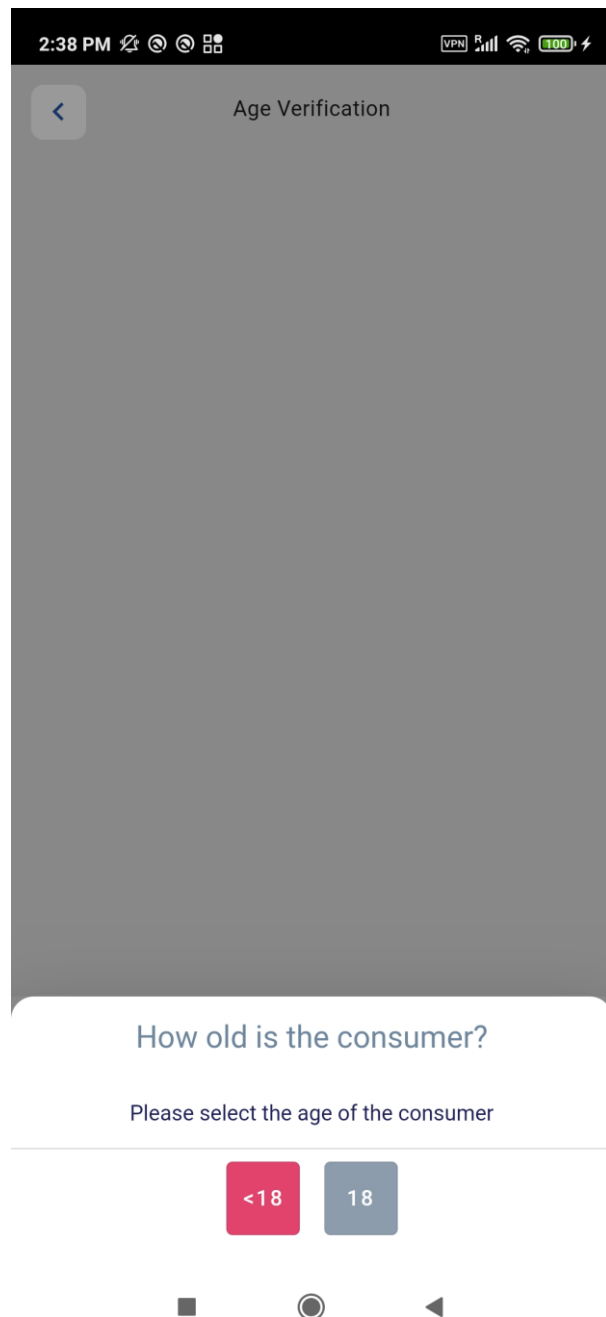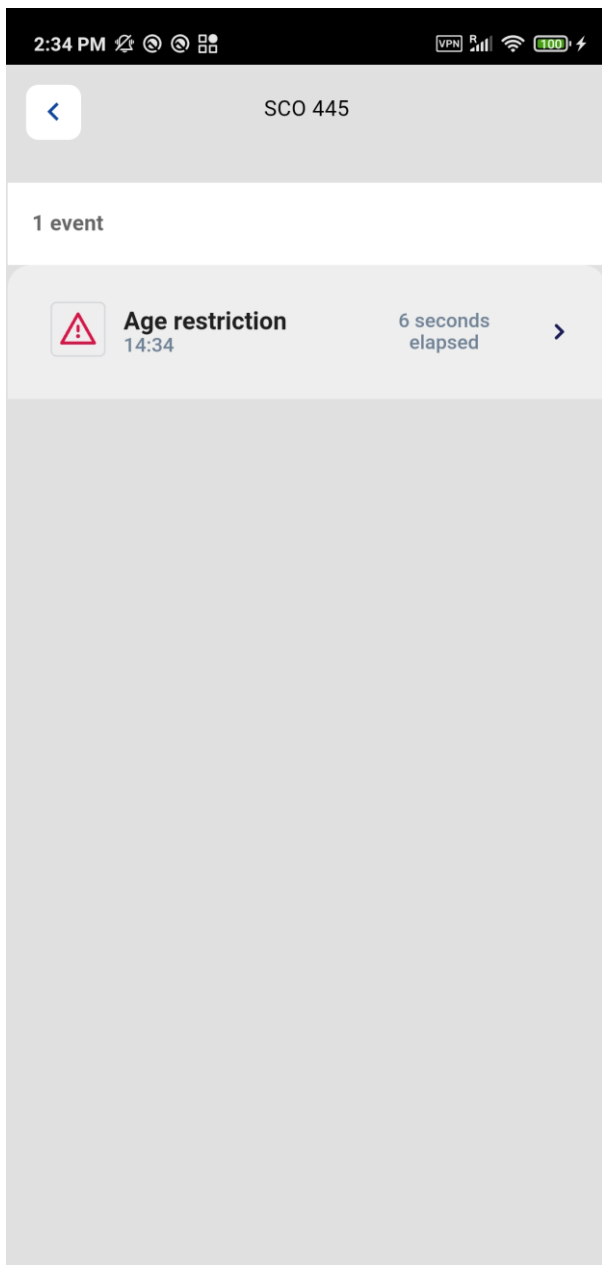
This section describes how age approval is carried out on an SCO station, which announces the age verification requests via Kafka/EventService. Age verifications for self-scanning use cases are described in the following sections

### 9.2.3   Age Verification

Certain product categories can only be sold to customers after a manual age check to prevent these products from being purchased by customers under a certain age. The Employee App also offers the option of performing this age check during self-scanning trips in direct contact with the customer, allowing them to enjoy the benefits of a virtually frictionless shopping experience.

If such items are scanned on a self-scanning device, the customer will be informed about this restriction. The customer can now chose to resolve this instantly by requesting approval from an employee. The customer can also decide to go to an Infopoint. It is also possible for the customer to continue shopping and resolve this directly before paying for their purchase.

Either way, this restriction is sent to the Employee App. The age request can be approved by following these steps:

- Launch the **Age Verification** function in the Employee App
- Scan the QR code displayed by the Self Scanning Client app
- Select the age of the customer by entering the date of birth or age

The result is provided back to the Self Scanning Client app and the age should be approved. If the request was declined, the items will be removed from the customers basket automatically.
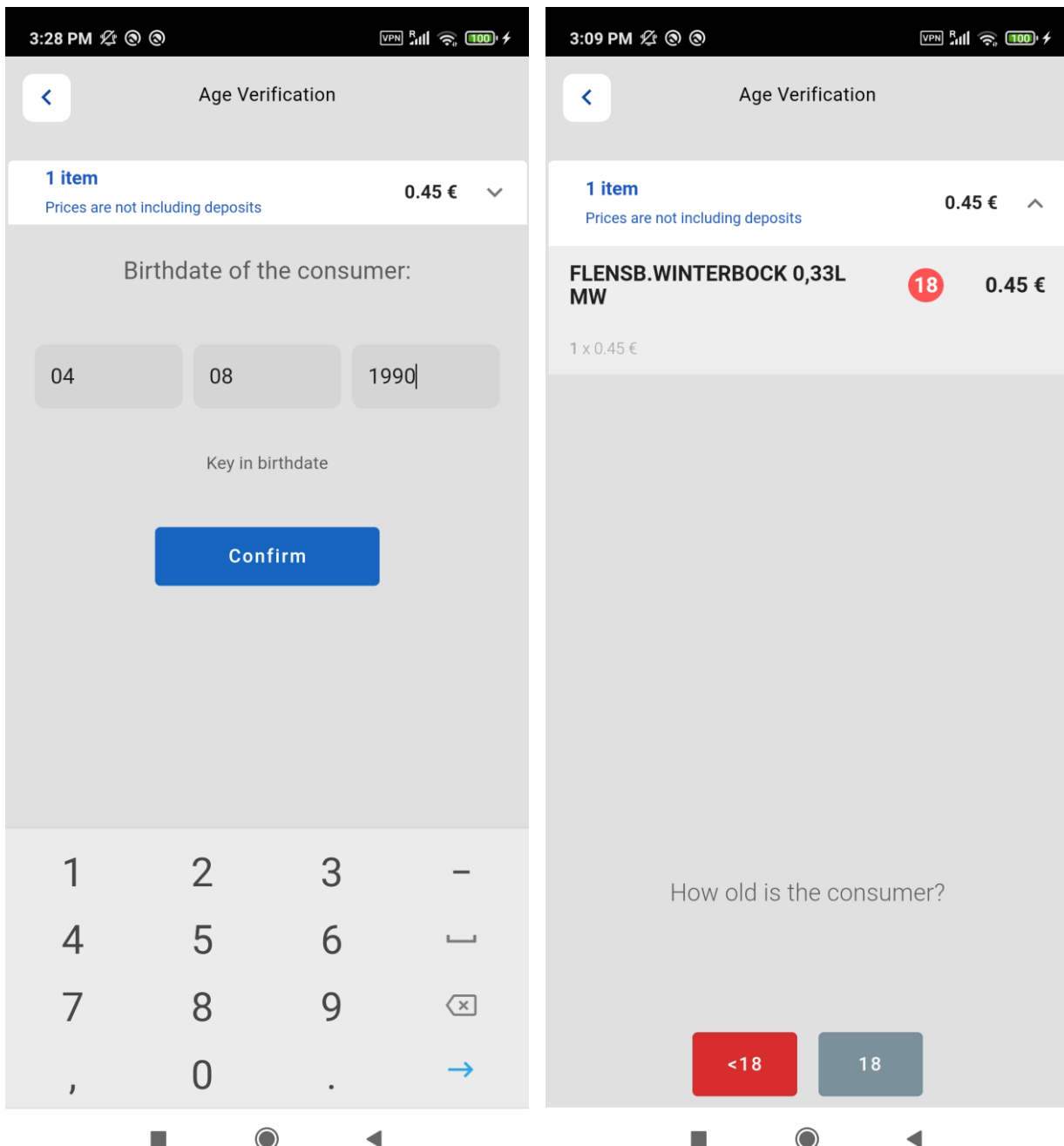

9.2.4 Infopoints

The Employee App provides a dedicated function for displaying all age restriction events at store Infopoints and is able to resolve them.

- Launch the **Infopoint** function in the Employee App

- The Infopoint, including the location where the age restriction approval is required, should be visible in the list. The Employee App user has the choice of either scanning the barcode displayed in the Self Scanning Client application or selecting "Load transaction" for the corresponding entry.

- Select the age of the customer

The result is provided back to Self Scanning Client in the same way as described in the section Age Verification.
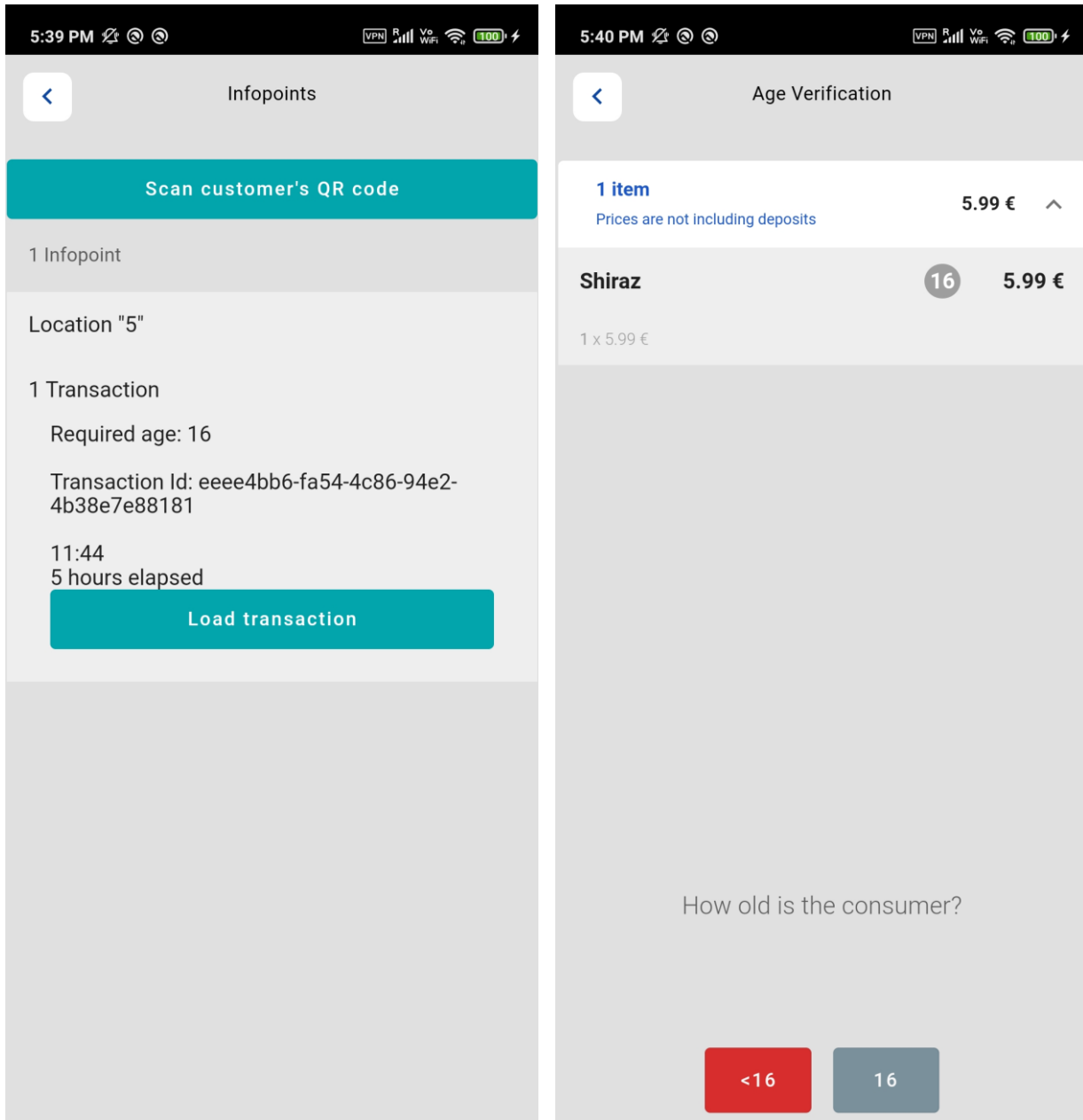
9.2.5   Partial Rescan

In accordance with a defined set of rules, the Fraud Detection Service can decide whether a customer is at a higher risk of fraud based on the items in the shopping cart, on the customer's purchase history, or through a random check.

The rescan is only triggered during the end-of-trip procedure. In this case, the Self Scanning Service informs the customer to call an employee to perform the rescan together with them. The customer cannot pay for

their purchase before the rescan. Instead, a QR code is displayed on the customer app with the message "You can proceed with mobile payment after successful rescan".

The rescan is performed as follows:

- Launch the **Rescan** function in the Employee App

- Scan the QR code from the customer app

- Scan the items that the customer has in the basket

The Employee App confirms/declines the partial rescan by sending a new transaction to the transaction pool with the additional fields required. If a discrepancy is detected, the customer must be subject to a full rescan at a stationary POS or SCO station.

globaler Füller Grün 15.71 €

1 x 15.71 €

Void

Scan Item

Scan Item
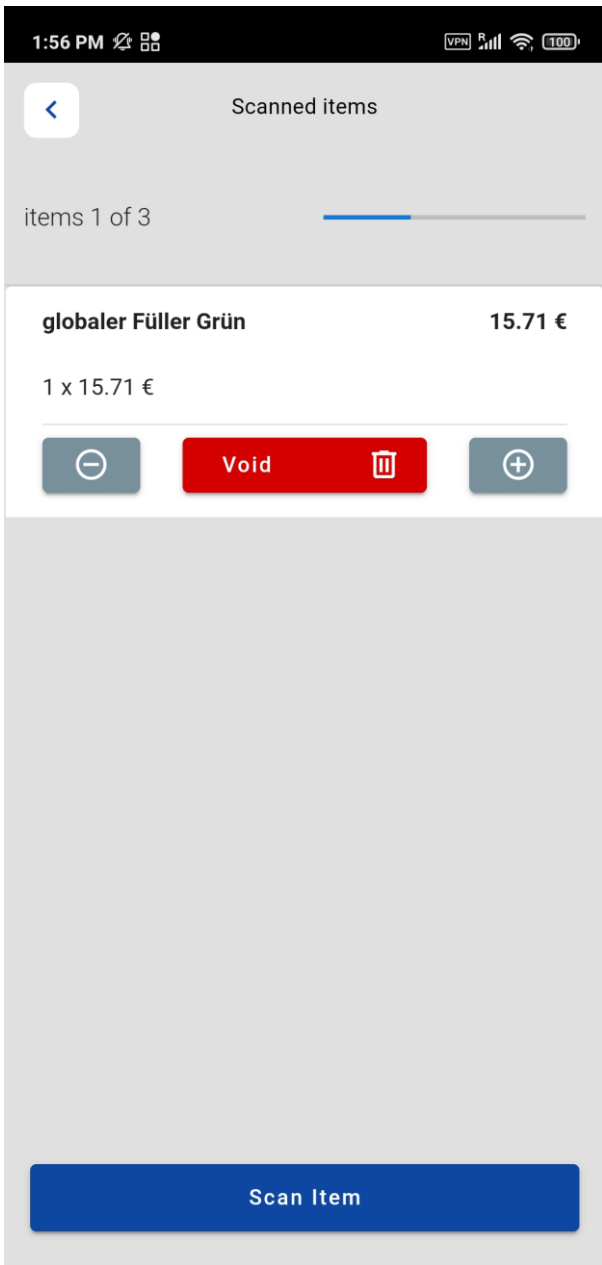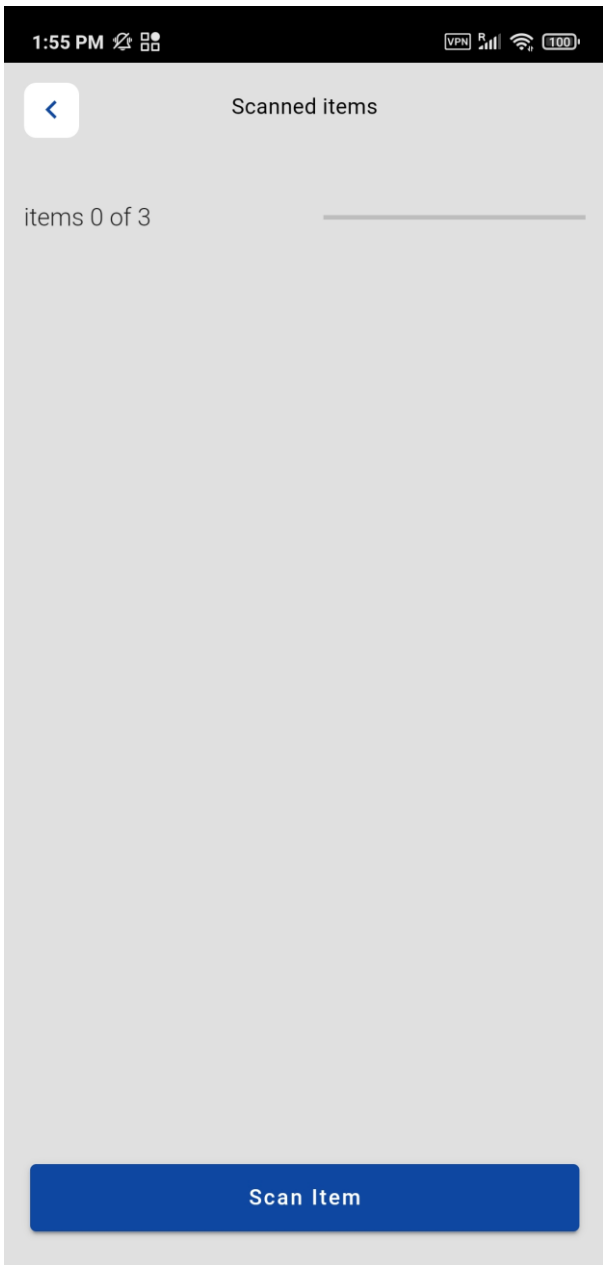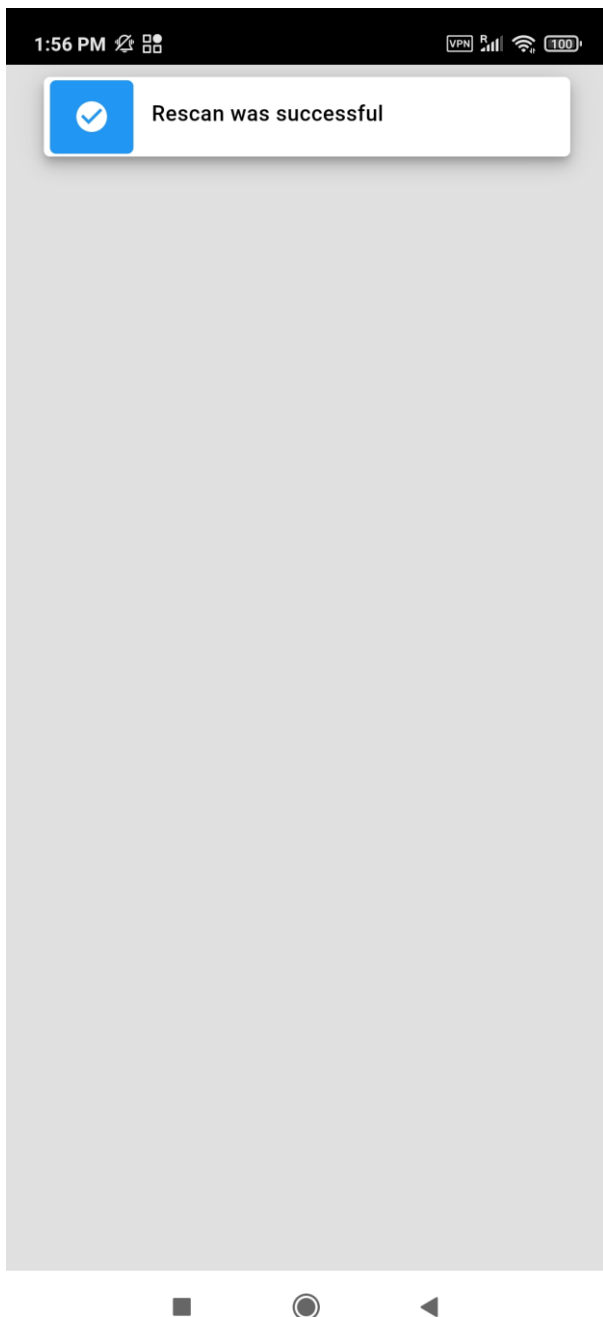
9.2.6 Fraud Detection Configuration

The Fraud Detection Service is normally configured via the Storemanager Server. However, it may also be necessary to completely override the Fraud Detection Service for short periods of time to reduce or prevent queues at the stationary POS and SCO. The employee can do this by disabling the fraud detection for a certain amount of time:

- Launch the Fraud Detection function in the Employee App
- Select the period that the Fraud Detection Service configuration should be overridden for
- Disable fraud detection by pressing the "disable" button

Afterwards, a timer will show how long this config change still applies. When the timer reaches zero, the currently configured profile will be active again. The timer can be canceled early by pressing the "Stop disabling" button.
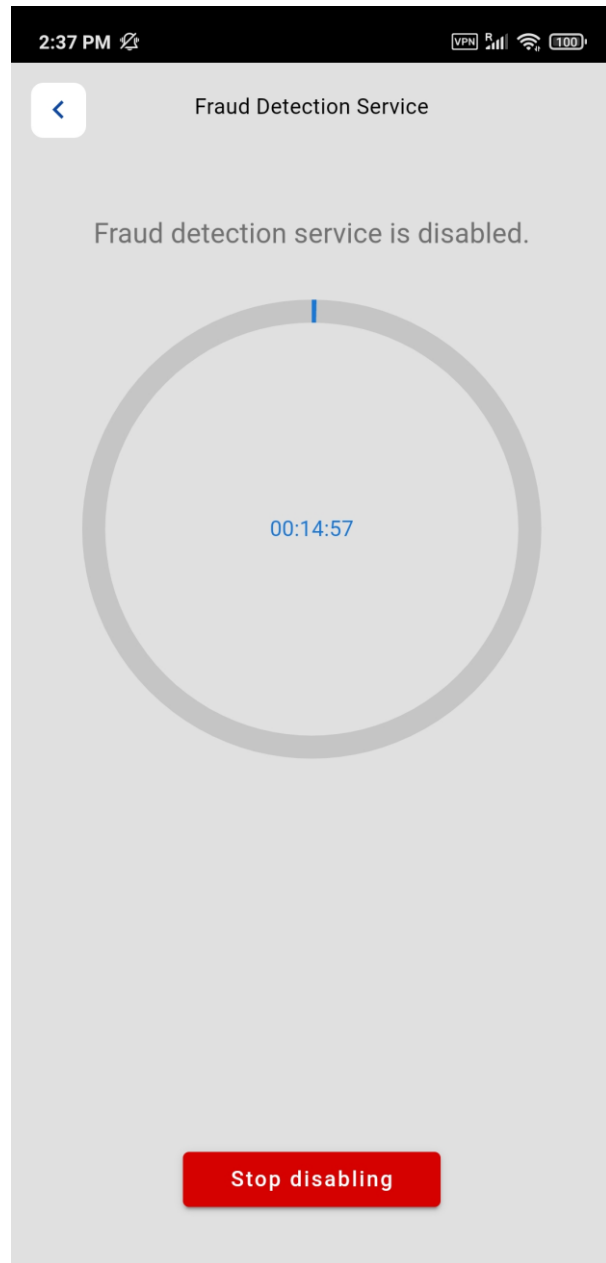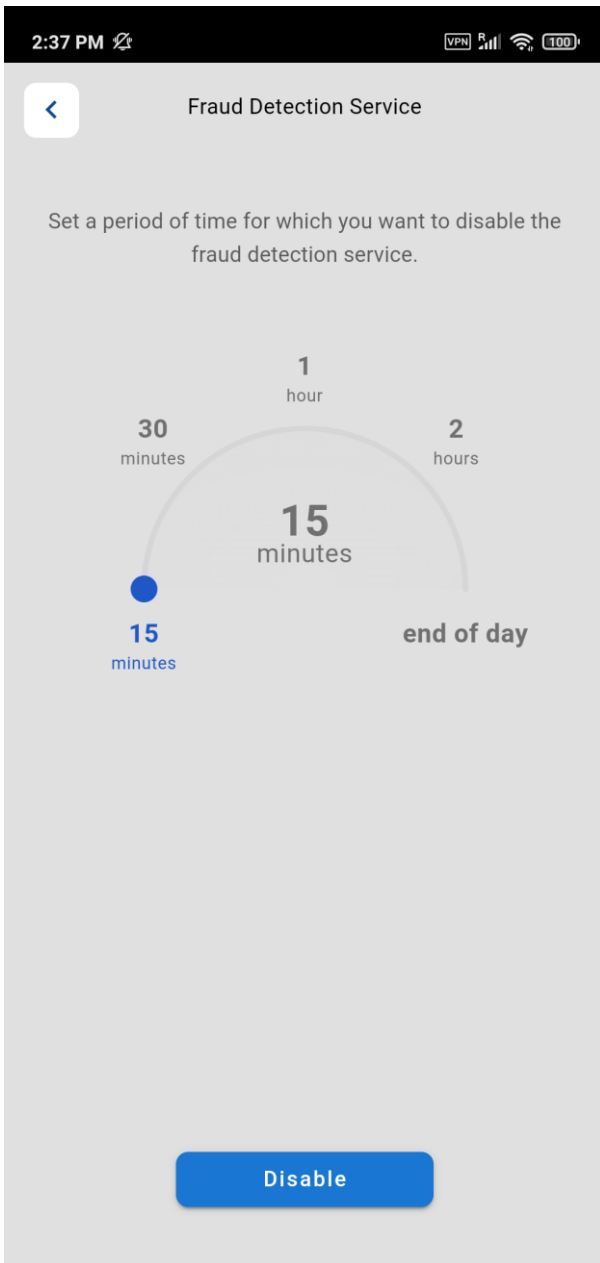
10 User Guide – Self Scanning Client (Industry scanning device)

10.1 Introduction

This document is the user guide for the Self Scanning Client of the GK/Retail Business Suite. The Self Scanning Client enables a customer to scan and enter items unaided by a cashier. The Self Scanning Client also transfers the total purchase amount of the virtual shopping basket at the end of the shopping trip to the GK/Retail OmniPOS, where the customer can pay with the usual payment methods. The customer can choose to use an industry scanning device, which is preconfigured and provided by the retailer.

The customers always know the value of their current virtual shopping basket, which saves time during checkout. The Self Scanning Client from GK Software helps employees in retail businesses to cater for customer needs more extensively. The Self Scanning Client increases customer throughput.

10.1.1   Self Scanning Client

10.1.1.1   Functions

The Self Scanning Client supports the following functions:

1. Logging in to the system

2. Scanning items (item entry)

3. Moving and (optionally) restoring the virtual shopping basket:

    o   As part of the regular shopping process

    o   When the customer stops the shopping trip unexpectedly

    o   When the battery of the industry scanning device reaches a defined charge level

10.1.2   Interface Layer

The Self Scanning hardware interface is necessary to execute certain commands on the Self Scanning industry scanning device. It is the layer between the Self Scanning Client and the operating system of the device.

The supported commands are:

*   Unlock the cradle

*   Lock the cradle when inserting

*   Lock the cradle after a defined period (if the industry scanning device is not removed by the customer after the cradle is initially unlocked)

*   Make the cradle LED blink (with unlock command)

*   Read the cradle ID when inserting the industry scanning device into the cradle

*   Read the wall ID when inserting the industry scanning device into the cradle

*   Read the column ID when inserting the industry scanning device into the cradle

*   Read the battery status (defined intervals)

*   Send the battery status

*   Read the status

*   Send the status

10.1.3   Wall Device Manager

The Wall Device Manager manages the industry scanning devices and the cradles. It checks the availability of scanners, the battery statuses, and disability flags in the zones. The Wall Device Manager communicates with the customer database and, if available, the validation engine to check the customer number and fetch the corresponding validation flag.

For more information on the Wall Device Manager, please read the document: Product Description – Wall Device Manager.

10.2   Self Scanning Processes

10.2.1   Device Dispensing and Return Process

10.2.1.1   Device Dispensing Area

The customer identifies themselves by scanning their customer card or a barcode in the device dispensing area. The customer then takes an industry scanning device and their customer number is assigned to the virtual shopping basket of the industry scanning device.

The device dispensing area consists of the Wall Device Manager as a computer system with a touchscreen, a scanner[2] and a device dispensing wall with cradles. A typical dispensing area consists of several terminals and dispenser walls.

[2]For example, the Vuquest 3320g scanner manufactured by Honeywell. For more information about this scanner, please visit the website: https://www.honeywellaidc.com/products/barcode-scanners/hands-free/vuquest-3320g

10.2.1.2   Device Return Area

The cradles for the return of scanners are located in the check-out area of the store. The check-out area may consist of several return walls.

A defined process leads the customer from closing the virtual shopping basket, to the return of the handheld at the return walls, to the actual payment. The virtual shopping basket is moved from the industry scanning device to the central GK/Retail OmniPOS environment.

> A common configuration for the retailer is that GK/Retail OmniPOS runs in Pay Tower mode. The customer can therefore perform a self check-out, where they pay the total purchase amount without interaction with a shop assistant or cashier.

10.2.2   Item Scanning

10.2.2.1   General

When picking up an industry scanning device from the device dispensing area, the device sends a request to open a receipt at the GK/Retail OmniPOS Self Scanning Service. Unless the user is shopping as an anonymous user (with no account), the customer number must be assigned to the opened receipt. Afterwards, the status *shopping* is assigned to the device and a welcome message is displayed on the device screen.

When the customer scans an item, the handheld displays the item name, price, and an image/picture.

In general, two screens are available: *Item List View* and *Item View*. It is possible to switch to the *Item View* by clicking on a particular item in the *Item List View*. When the *Back* button is clicked in the *Item View*, the screen returns to the *Item List View*. Images/pictures of the items are available in both the *Item View and Item List View* screens.

10.2.2.2   Offline Case

If the industry scanning device or the customer's personal device loses its connection to the GK/Retail OmniPOS Self Scanning Service due to network issues, the customer can continue with their shopping trip and scan more items without any interruption. While the industry scanning device or the customer's personal device is still stably connected to the network in the device dispensing area, it downloads a mini version of the store inventory in the form of a SQLite database, which operates autonomously from the store network. The mini database contains the most important item information for the customer, such as the barcode, price and item name, to keep the database file size as small as possible. The size of the SQLite database file depends on the total business unit inventory. When scanning items offline, the Self Scanning Client is still able to calculate and display the total purchase amount but cannot display images/items.

- The industry scanning devices download the SQLite database when they are turned on and still connected to the dispensing wall in the device dispensing area. A customer who brings their own mobile device to the store will download the SQLite database to their phone when they scan the login barcode to signal the Self Scanning Client to start the shopping trip. The time it takes to download the SQLite database to the personal mobile device depends on the wireless network connection within the store and the SQLite database file size.
- The customer will always know whether the price shown in the virtual shopping basket of the Self Scanning Client has been calculated online or offline. If the price of the scanned item is shown in *gray*, the device is *offline*. If the price of the scanned item is shown in *blue*, the device is *online*.

When the network connection is re-established, the GK/Retail OmniPOS Self Scanning Service processes the items which were scanned offline in the background and it is possible to continue scanning additional items.

10.2.3 End of Trip

When the customer scans the End of Trip barcode in the device return area, the Wall Device Manager checks how many positions the virtual shopping basket contains. A message appears on the Self Scanning Client screen and asks the customer whether they scanned all of the items in their physical shopping basket. If the customer confirms this question, the industry scanning device displays a message, prompting the customer to put the industry scanning device back into the cradle. Otherwise, the Self Scanning Client returns to the list view so that the customer can scan items which they forgot to scan before.

In the current version of the Self Scanning Client, an empty virtual shopping basket is not supported. Therefore, a customer cannot finish their shopping trip without buying at least 1 item in the store. When the industry scanning device is put back into the cradle, the display switches back to the start screen and the device status changes to *Not available*. The customer then starts the payment process at the check-out area with the help of the GK/Retail OmniPOS in the Pay Tower Self Checkout mode.

10.3 System Context

The UI looks like a normal costumer app and can be used intuitively. All applications have a responsive design: The UI adapts the screen size of the appropriate platform on the smartphone or tablet device and can therefore be used on all systems without screen adaptions.

Internally, the Self Scanning solution utilizes the Self Scanning services of the GK/Retail Business Suite. The GK/Retail OmniPOS service also provides the central functions and web services for the Self Scanning Client. A layer between the Self Scanning Client and the mobile operating system secures the communication with the hardware device.

To use Self Scanning, customers have to sign up to a customer program with a customer card. Therefore, it is absolutely necessary to have a customer database to assign the customer number to an open shopping basket.

Customer card management is not part of the Self Scanning product.
The customer can only connect their customer card/customer number to one store at a time. However, customer-specific deviations from these rules are possible. Once the customer is in possession of a customer card from a retailer, they can use their customer card in the retailer's stores in other locations without needing to sign up for each individual store again.

Barcode information for the stores
- Typically, customers scan the barcode of an item. If items do not have a barcode (e.g. bread), there must be a barcode that can be scanned in the shelf.
- The customer usually weighs fruits or vegetables on a scale in the appropriate shop area. The scale receipt must contain a barcode for the customer to scan.

10.4 Customer Sign-in

To use the Self Scanning Client on the industry scanning device or on the personal device, the customer can either sign up for a customer account and sign in to the Self Scanning Client using the customer card, or sign-in as an anonymous user (without an account).

10.4.1 Store-Specific Check-In

Upon entering a store, the customer must scan a QR code with their app (regardless of whether they are registered or anonymous). Some retailers use different tenants for different purposes, dividing tenants into geographical zones, or management hierarchy. The tenant is therefore not the same for all stores and using a default tenant defined in the bundle does not meet all retailers' needs.

For this reason, this QR code at the entrance will share the "tenantId", "businessUnitId" and "businessUnitName" with the SSC BYOD. The QR code is planned for the entrance area of the store, so the tenant can be defined specifically for the store. If the check-in code contains a tenantId, the following business process will use it.

- StartOfTrip (all requests from here)
- Recalculate-transaction (POSService)
- EndOfTrip
- Payment (all requests)

Some requests should not use the specific tenant (especially if they are made after scanning a check-in code). These are CPS-related requests (in particular: Login, registration, fetching profile information).

Structure of a new check-in code:

```
{
    "tenantId": "001",
    "businessUnitId": "R104",
    "businessUnitName": "GK Store Germany",
    "simpleMdType": "v2"
}
```

10.4.2 Initial Sign-in for Customers without a Customer Card

Customers who do not have a customer card yet must get a temporary customer card in order to sign in to the Self Scanning Client application. The customer can get a temporary customer card after filling out the required general terms and conditions documents at the service counter inside the retailer stores. The customer must return the documents within one month after the initial sign-up, for completion and conclusion of the initial capturing process. The temporary customer card remains anonymous as long as the customer is on their first shopping trip and can be used immediately. The customer goes to the device dispensing area, scans the temporary customer card and receives an industry scanning device.

10.4.3 Sign-in for Customers with a Customer Card

Customers who already have a customer card must scan their customer card in the device dispensing area to activate the Self Scanning Client and connect their customer account to the virtual shopping basket. The customer must scan their customer card only once for their personal device, whereas for industry scanning devices, they must scan their card each time they take an industry scanning device from the device dispensing area.

> Please note that minor changes to the sign-in process are possible depending on the customer relationship management (CRM) software in use. For instance, a password prompt can be integrated for security reasons. If the customer uses their own device, the Self Scanning Client is also able to save the login data on the individual device. Therefore, the customer does not have to re-enter their password every time they open the Self Scanning Client.

10.4.4 Anonymous User

Customers who do not have either an account or a temporary customer card can still use the devices as anonymous users. Their data is neither processed nor stored and functionalities relying on customer data (such as loyalty programs) are not accessible.

10.5 Device Dispensing Area

The device dispensing area is the area where the customer picks up the industry scanning device inside the store. The device dispensing area consists of a hardware component in the form of a dispensing wall with industry scanning device cradles and a software component in the form of GK/Retail OmniPOS – Wall Device Manager. There are both high and low rows of cradles so that disabled customers are also able to use the industry scanning devices. The number of dispensing walls is not limited and, depending on the retailer size and their needs, extra dispensing walls can be added to the store.

The process for returning the industry scanning devices to the device return area is described later on in this document.

10.5.1 Role of the Wall Device Manager

As the software component of the device dispensing area, the Wall Device Manager uses internal algorithms to ensure that the industry scanning devices are, if possible, fully charged when customers remove them. Lights on the cradles indicate to the customer that the corresponding industry scanning devices are ready for removal. Special lights installed in the area of the dispensing wall for disabled customers light up when the customer requests the disabled option via a special electronic note on their customer card.

### 10.5.2 Dispensing an Industry Scanning Device

To pick up an industry scanning device in the store, the customer must do the following:

1. Go to the device dispensing area within the store.

2. Scan their customer card at the dispensing wall.

3. The Wall Device Manager processes the scanned customer card and assigns it to a fully charged industry scanning device.

4. The cradle of the industry scanning device is unlocked and the dispensing wall lights up green to indicate to the customer where to find the respective industry scanning device.

10.5.3 Standby Screen and Welcome Screen on the Industry Scanning Device

As long as the industry scanning device remains inside the dispensing wall cradle, the industry scanning device shows a standby screen to the customer.

Once the customer picks up a released industry scanning device, a screen welcoming the customer is displayed.
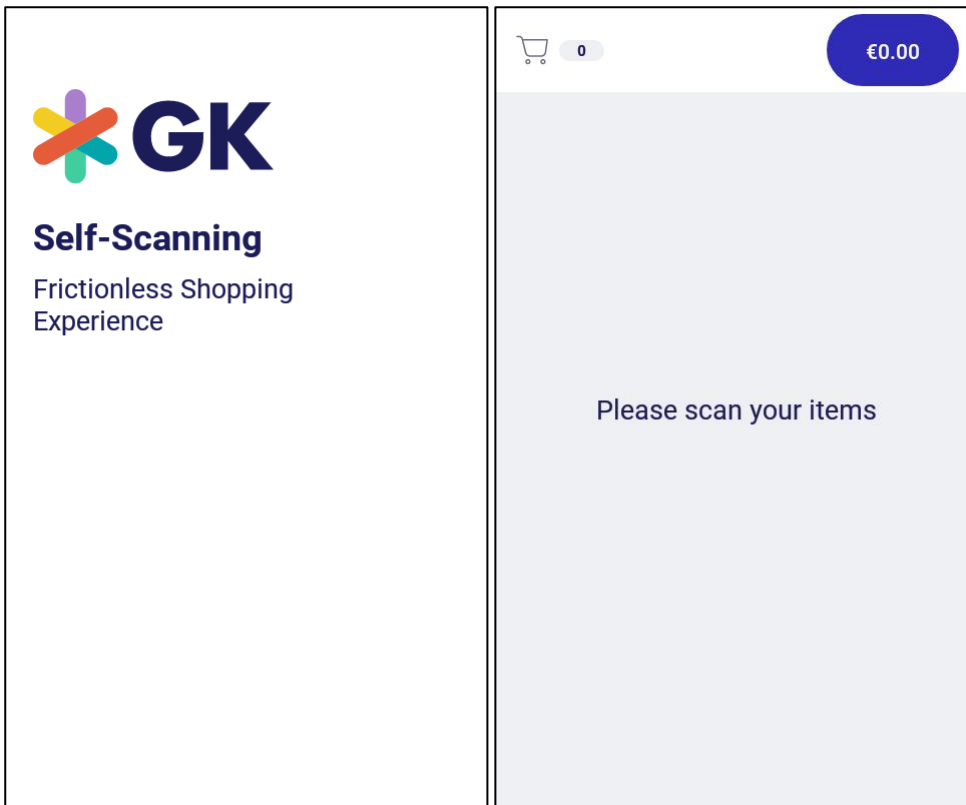
10.6 Shopping Process

After the customer leaves the device dispensing area, they enter the shop floor. The customer then selects the items they want to buy and scans them before putting them into their shopping basket. The Self Scanning Client shows all items in a detailed list view and calculates the total purchase amount of the shopping basket at all times.

10.6.1 Item Views

The Self Scanning Client has two different views that can be used to look at the scanned items in the virtual shopping basket. The customer can choose between the list view and the detail view.

The list view is the default view for the customer. In this view, all of the scanned items are shown in a list in chronological order. If the customer taps an item in the list view, the Self Scanning Client shows the detail view. By tapping the blue arrow pointing left (←), the customer switches back to the list view.

When a customer scans an item that they have already scanned before (for example a second bag of rice after a first bag was already scanned), the new item and the already scanned item are merged and displayed together on one line with the corresponding number of items.
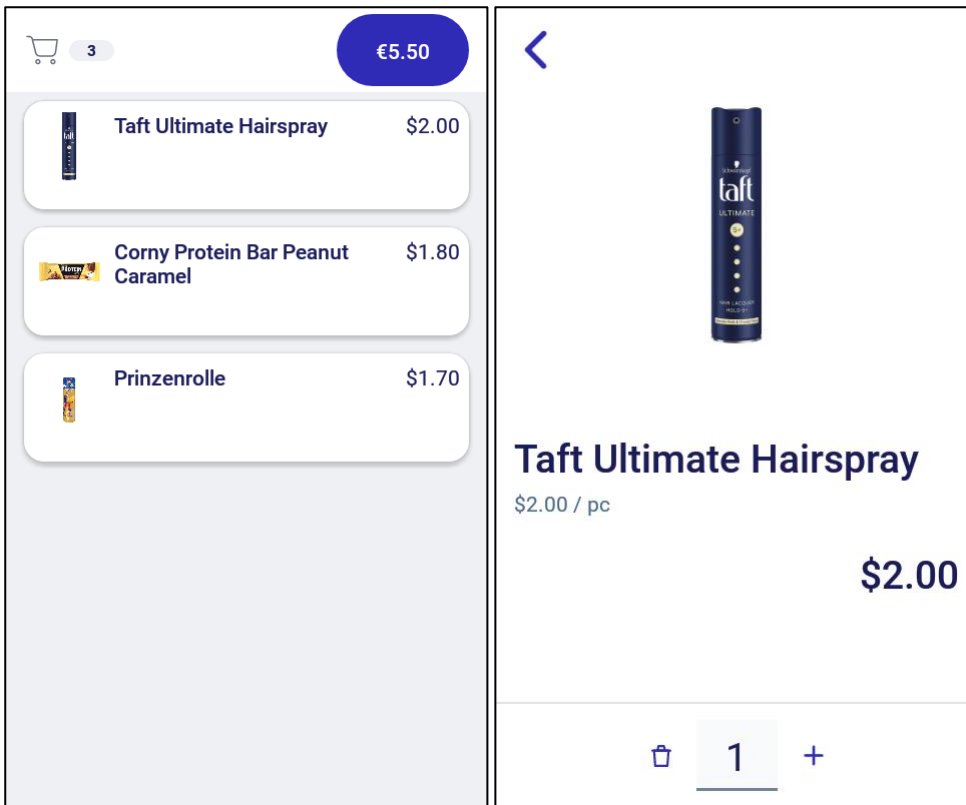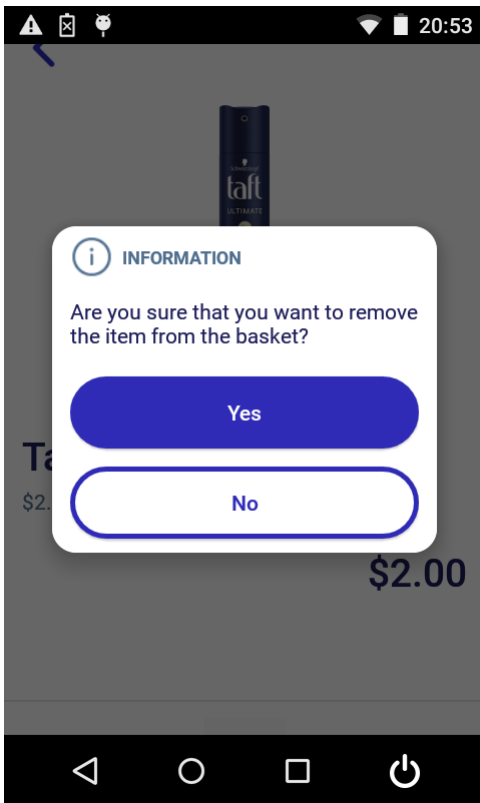
10.6.2   Scanning Items

10.6.2.1   Industry scanning devices

The customer scans a new item by pressing the middle button on the industry scanning device, which activates the laser scanner on the back of the device. The customer must point the laser at the barcode on the product so that the Self Scanning Client can read and interpret the barcode. After the item has been scanned and has appeared on the screen, the customer can use the *plus* and *minus* buttons on the screen to increase or decrease the quantity of the scanned item. In this way, the customer only has to scan an item once even though they are buying multiple quantities of the same item.

10.6.2.2   Deleting Items from the Virtual Shopping Basket

The customer can delete any item they scanned by decreasing the item quantity to 0. A specific "Delete" button is not available. After the customer uses the *minus* button to decrease the item quantity from 1 to 0, the Self Scanning Client will ask the customer one last time if they really want to delete the item from the virtual shopping basket.

10.6.3   Special Items

Special items are items which require an additional action from the customer or retailer, or show up differently in the virtual shopping basket compared to normal items. Simply scanning the item and putting it into the shopping basket is usually not enough; the customer must perform additional actions.

10.6.3.1   Sales Restrictions

The sale of some items is restricted to a specific age bracket (e.g. alcohol or tobacco products), some items are only sold with special permission (e.g. guns or medicine) and some items cannot be sold without the interaction of a shop assistant (e.g. a T-shirt with a security tag).

After the customer scans a sales restricted item, the Self Scanning Client will show a customized message. The customer must follow the instructions on the Self Scanning Client screen and confirm their action by tapping *OK*.

> Please note that the workflow for sales restricted items can be freely configured by the retailer during the software set-up process. The retailer can decide how to handle sales restricted items and is responsible for obeying local laws. For further information, you can contact your technical consultant at GK Software.
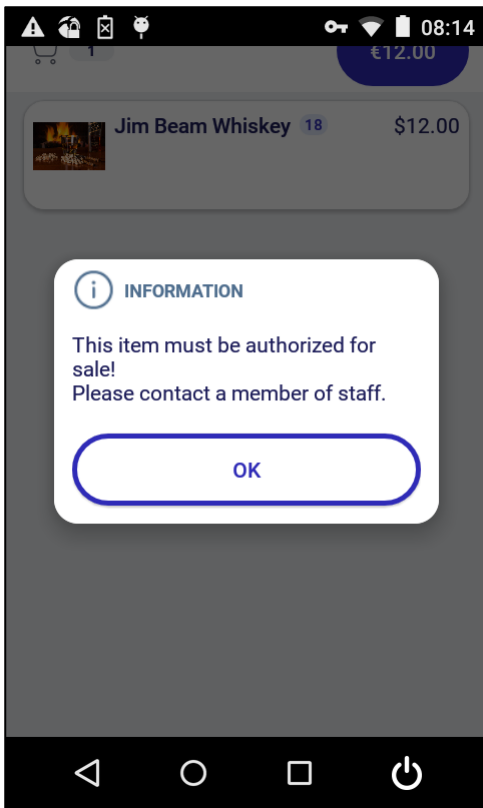
10.6.3.2 Follow-on Deposit Items

Follow-on deposit items are items automatically connected to a main item, which the customer has put into their shopping basket. For example, a customer buys a large quantity of beer bottles. A crate of beer is automatically added to the virtual shopping basket and the customer has to pay a deposit for this. The deposit item itself cannot be selected. If the customer removes the main item, the deposit item is automatically removed too. A change in the quantity of the main item leads to a change in the quantity of the deposit item too.
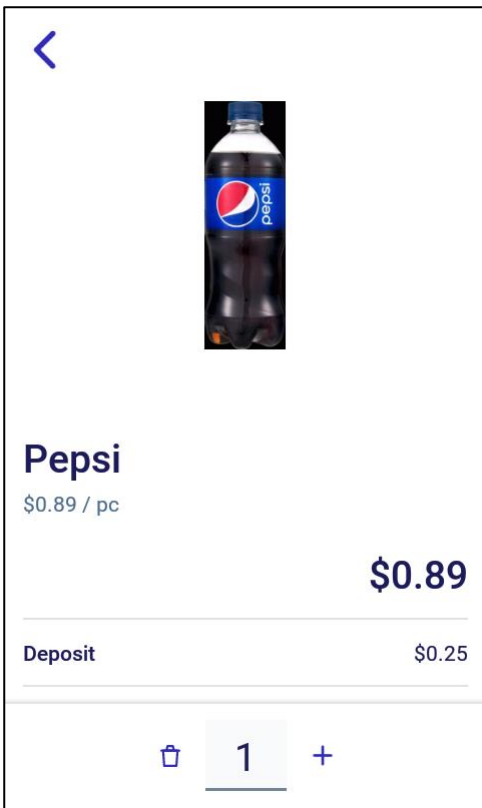
10.6.3.3   Discount Items, Coupons, Promotions

The Self Scanning Client supports different discount coupons in digital or analog form. The retailer has to decide in which form their customers can scan these discount coupons and configure the Self Scanning Client accordingly. For example, the customer may be able to scan their discount coupons at any time during the shopping trip, or the retailer could stipulate that discount coupons can only be scanned and used once the customer has reached the check-out area of the store at the end of their shopping trip.

Depending on the configuration of the Self Scanning Client, the application can show an error message during the scanning process, informing the customer that they must scan their discount coupons later in the shopping trip.

If the retailer allows their customers to scan the discount coupons during their shopping trip, the Self Scanning Client displays the promotions in the virtual shopping basket. The original price of the item is shown, the discount is shown, and the new price is calculated automatically. If the customer wants to know which promotions are applicable to a specific item, the customer can tap the specific item in the virtual shopping basket and all applicable promotions are displayed in a scrollable list in the detailed item list.
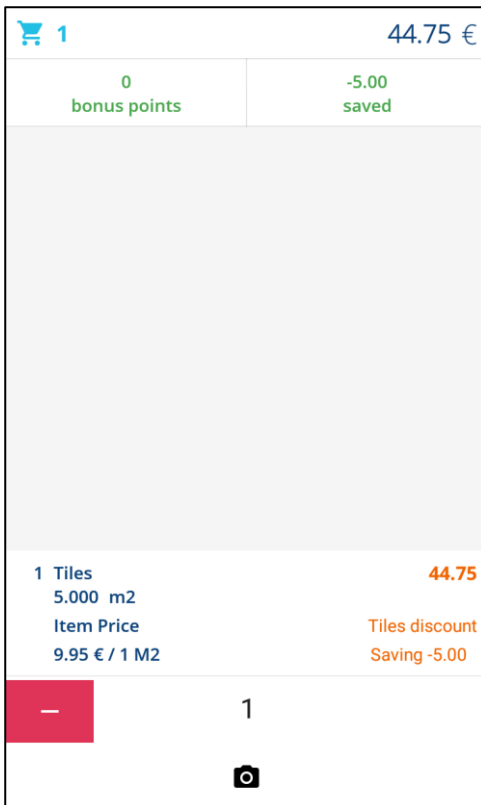
10.6.3.4   Special Price / Reduced Price

Depending on the item, a special price can apply. For example, an item was put in the shop window in November and is now sold at a drastically reduced price in February. In this case, the customer can scan the item but the *plus* button for increasing the quantity is not available. Only the *minus* button for removing the item from the virtual shopping basket is shown.

10.6.3.5   Multiple-priced Items

If an item has multiple price labels (for example, a new price label was stuck on top of the old label due to a price change of the item, but this new label subsequently falls off, revealing the old original label), the Self Scanning Client automatically selects the most recent price of the item and displays it correctly in the virtual shopping basket.

10.6.4 Troubleshooting

10.6.4.1   Barcode Cannot be Scanned

If the Self Scanning Client is not able to scan a barcode (because the barcode is damaged or dirty, for example), the Self Scanning Client shows a warning message to the customer. The message prompts the customer to ask a member of staff for help during the shopping trip or, at the latest, to ask a member of staff at the check-out area of the store so that they can scan the items for the customer. The message displayed to the customer can be configured by the retailer, depending on the number of employees in the stores.
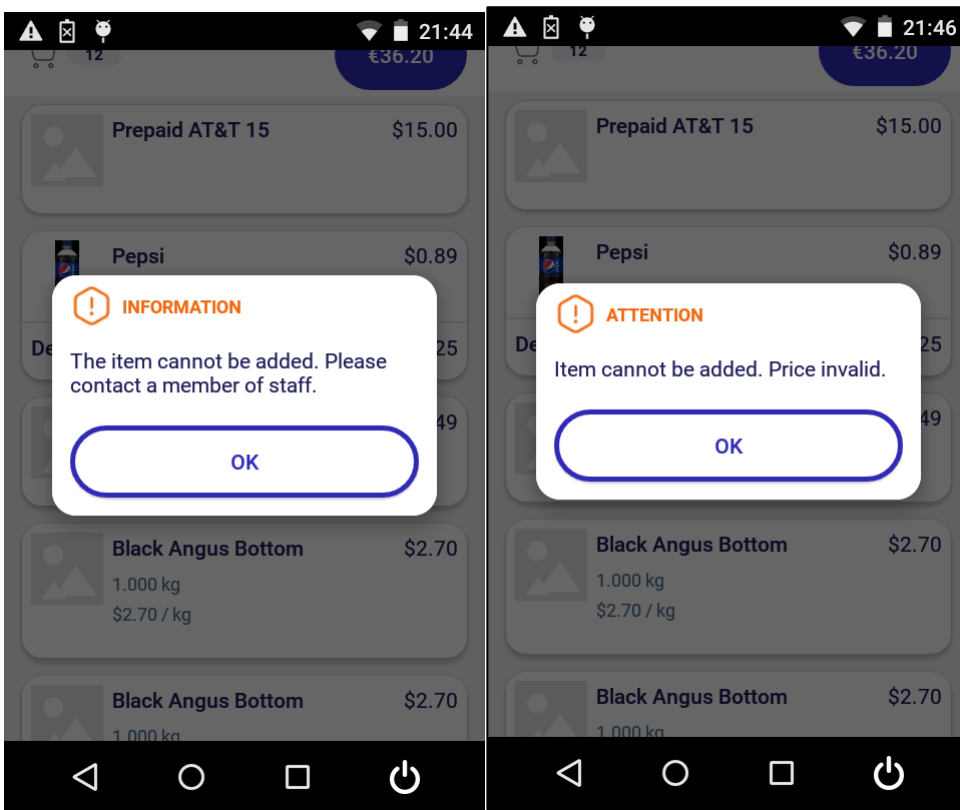
10.6.4.2   Customer Orders

The customer cannot scan customer orders with the Self Scanning Client. A corresponding message is shown on the display.

10.6.4.3   Returning Items to the Store

It is not possible for the customer to capture items that they want to return to the store. The customer has to talk to a member of staff in the store in order to return their items.

10.6.4.4   Self Scanning Client is Offline

If the Self Scanning Client loses the online connection to the GK/Retail OmniPOS Self Scanning Services, the customer can still use the Self Scanning Client without any restrictions. For further information about the technical specifications, make sure to read the section *Offline Case* in the document: Product Description – Self Scanning Client.

The customer can determine whether the Self Scanning Client is online or offline by looking at the color of the prices. Blue item prices in the virtual shopping basket represent live online prices, which are stored and changed in the enterprise resource planning (ERP) software. Common developers of this type of ERP software include SAP, Oracle and Microsoft. The Self Scanning Client is able to read the item prices from these systems in real-time with the help of the GK/Retail OmniPOS Self Scanning Service. Gray item prices in the virtual shopping basket represent offline prices, which are not currently connected to the ERP software. The Self Scanning Client is still able to calculate the total purchased amount based on the offline prices, but the customer must be aware that the prices in the virtual shopping basket can change when the Self Scanning Client reconnects to the store network and shows blue item prices again.

The Self Scanning Client must be online at the end of the shopping trip. Otherwise, the customer cannot proceed to the payment process.

10.7   Device Return Area – Ending the Shopping Trip

Once the customer finishes their shopping trip, they enter the check-out area of the store. The customer has to confirm that they scanned all of the items in their shopping basket and have therefore entered the items into the virtual shopping basket within the Self Scanning Client. To confirm the end of the scanning process and proceed to the payment process within the check-out area of the store, the customer has to scan the End of Trip barcode. After the customer has scanned the End of Trip barcode, the Self Scanning Client will ask the customer to confirm the end of their shopping trip by pressing the *YES* button, which will appear on the Self Scanning Client. Otherwise, the Self Scanning Client returns to the list view so that the customer can scan items which they forgot to scan before.
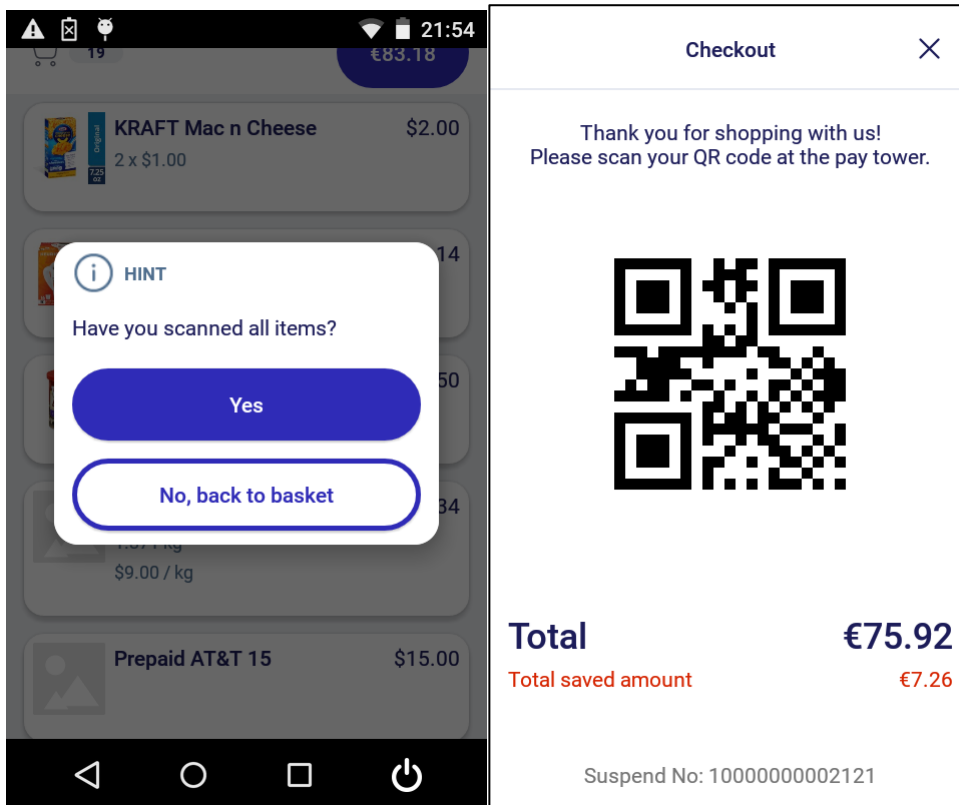
10.7.1   Validation

To avoid misuse, members of staff perform random checks on their customers' shopping. The customer is informed of the check after scanning the End of Trip barcode and has to wait for a member of staff to check their shopping basket and compare it to the items in the virtual shopping basket in the Self Scanning Client.

10.7.2   Payment and Exit

If the customer used the Self Scanning Client on an industry scanning device and not on one of their own devices, they have to return the industry scanning device to the device return area within the store. After returning the industry scanning device, the customer moves to the payment kiosk, where they can pay for their items. Since the GK/Retail OmniPOS runs in the Pay Tower Self Checkout mode in most stores, the customer can pay for their shopping basket without any interaction with members of staff and leave the store afterwards.

10.8   Special Functions

10.8.1   Bulk Removal

In special cases, such as for cleaning, members of staff can release all industry scanning devices from the device dispensing area and the device return area within the store at the same time. To perform a bulk

removal in the device dispensing area, the store staff must scan a special service barcode, which must otherwise be kept private.

The bulk removal starts with the industry scanning device in the top left corner and ends in the bottom right corner. The Wall Device Manager, which was mentioned earlier in this document, makes the industry scanning device in the device dispensing area flash in a predefined order so that the member of staff always knows which industry scanning device they have to pick up.

After the Wall Device Manager has lit up all of the industry scanning devices in the device dispensing area and the member of staff has picked up all industry scanning devices one by one, the bulk removal process is completed and no further action is necessary.

10.8.2   Swapping Self Scanning Devices

For industry scanning devices that have to be replaced during the shopping trip (because the device runs out of battery, for example), the Self Scanning Client supports a swapping function. An industry scanning device with an empty battery can be replaced by a device with a full battery and the virtual shopping basket can be transferred so that the customer can continue their shopping trip without too much of an interruption.

Generally, there are 3 different scenarios in which the industry scanning devices are swapped after the industry scanning device battery status drops below a defined battery level. These scenarios are described in the following sections.

10.8.2.1   Standard Case – Swapping the Industry Scanning Device Under Normal Circumstances

1. The customer receives a warning message about the battery level and contacts a member of staff within the store.

2. The member of staff takes the industry scanning device with the low battery and scans a special service barcode, which is not normally accessible to the customer.

3. The virtual shopping basket, which is connected to the customer number, is backed-up with help of the GK/Retail OmniPOS Self Scanning Service, and is deleted from the industry scanning device at the same time.

4. The member of staff takes a fully charged industry scanning device from the device dispensing area within the store and scans the special service barcode and customer card with this device.

5. The GK/Retail OmniPOS Self Scanning Service restores the virtual shopping basket on the Self Scanning Client and the customer can continue their shopping trip.

6. The member of staff puts the industry scanning device with the low battery back into the device dispensing area, where the next customer can pick up the industry scanning device once it is fully recharged.

10.8.2.2   Exceptional Case 1 – Forced Reset of the Industry Scanning Device

1. The customer receives a warning message about the battery level but ignores this message and does not contact a member of staff within the store.

2. After a defined amount of time, the industry scanning device shows a second warning message about the battery level, which the customer cannot ignore any more.

3. The Self Scanning Client runs an automatic backup of the virtual shopping basket, which is connected to the customer card number.

4. The industry scanning device with the low battery deletes the saved virtual shopping basket within the device and shuts down. The device cannot be used any more.

5. The customer contacts a member of staff for help.

6. A member of staff scans a special service barcode and the customer card with a new fully charged industry scanning device and the GK/Retail OmniPOS Self Scanning Service restores the virtual shopping basket on this new device.

7. The customer can use the new industry scanning device.

8. The member of staff puts the industry scanning device with the low battery back into the device dispensing area, where the next customer can pick up the industry scanning device once it is fully recharged.

10.8.2.3 Exceptional Case 2 – Resetting the Industry Scanning Device Is Not Possible

1. The customer receives a warning message about the battery level but the device is offline or damaged, so a connection to the GK/Retail OmniPOS Self Scanning Service is not possible.

2. The customer contacts a member of staff within the store.

3. The member of staff takes the industry scanning device with the low battery and scans a special service barcode, which is not normally accessible to the customer.

4. The member of staff browses the customer database on the new industry scanning device and compares the scanned items in the virtual shopping basket in the Self Scanning Client with the actual shopping basket. Depending on the last point at which the old industry scanning device was online, the virtual shopping basket and the actual shopping basket are nearly identical.

5. If they are not there already, the member of staff scans any missing items and makes sure that all of the items in the virtual shopping basket are correct.

6. After the member of staff finishes their work, they have to confirm their action on the Self Scanning Client.

7. The customer can use the newly charged and restored industry scanning device and continue their shopping trip.

8. The member of staff puts the industry scanning device with the low battery back into the device dispensing area, where the next customer can pick up the industry scanning device once it is fully recharged. All personal data on the old industry scanning device is deleted automatically.

11 User Guide – Wall Device Manager

11.1 Introduction

The Self Scanning solution of GK SOFTWARE SE allows customers to scan their shopping basket themselves.
The customers know the value of their current shopping basket at all times, which saves time during checkout. The Self Scanning solution of GK SOFTWARE SE supports employees in retail businesses to cater for customer needs more extensively. The solution increases customer throughput.

11.2 Customer Registration

11.2.1 Initial Registration of Customers Without a Customer Card

Initial registration is performed by customers who do not possess a customer card yet. During initial registration, customers receive a temporary customer card and registration documents at the service counter. The customer must return the registration documents within one month of filling them out, for completion and conclusion of the initial registration process. The temporary customer card remains anonymous until the initial registration has been completed but can be used immediately. The customer goes to the terminal on the device dispensing station, scans the temporary customer card and receives a mobile self scanning device.

11.2.2 Registration of Customers with a Customer Card

This type of registration is performed by customers who already possess a customer card but who have not used the self scanning service before. To do this, customers must scan their customer card on the Wall Device Manager terminal.

11.3 Dispensing the Mobile Self Scanning Device - Device Dispensing Station

11.3.1 Systems at the Device Dispensing Station

Physical systems	Count	Purpose of use
Wall Device Manager Client	1-n	• The customer can select the language and enable the handicap button in the 'Welcome screen' • Registering a customer card for self scanning and remove a device • Displaying all possible error messages • First use of self scanning (General Terms and Conditions have to be accepted) • Setting a wall to out-of-service mode
Wall Device Manager Terminal	1-n	• Registering customers with a customer card prior to initial use of the self scanning functionality • Scanning the customer card to dispense a mobile self scanning device • Managing the position of self scanning devices on the dispensing wall
Dispensing wall with handicap zone	1-n	• Cradles containing mobile self scanning devices for removal by the customers o The cradles are arranged into two areas; an upper area with device removal zones and a lower area with handicap zones

11.3.1.1 Wall Device Manager Terminal

The Wall Device Manager uses internal logic to ensure that the self scanning devices are always fully charged, if possible, when customers remove them. The cradle produces a light signal to indicate that its device is ready for removal. Furthermore, customers who have chosen the handicap option when registering their cards are able to see the available devices in the handicap zone. The Wall Device Manager functionality for returning self scanning devices to the device disposal station is described further below.

11.3.1.2 Wall Device Manager Client

Employees and customers can use the Wall Device Manager Client to interact with the Wall Device Manager Terminal and set some of the self scanning device's parameters.

It is important to note that the Wall Device Manager Client is a user interface attached to the Wall Device Manager Terminal and NOT the self scanning device that the customers will use to shop.

11.3.2 Dispensing to Customers

The device dispensing stations may be located on several floors of a store. The device dispensing stations have terminals for registering customer cards and one or more dispensing walls with mobile self scanning devices.
Customers scan their customer cards on the terminals and a self scanning device is allocated to them. The cradle of the allocated device in one of the dispensing walls nearby produces a light signal. The customer has to remove the unlocked self scanning device from the cradle. Upon removal, the self scanning device is immediately assigned to the customer or customer card. The customer can now start their shopping trip.

11.3.3 Mobile Self Scanning Device

Usually, the device dispensing stations and the device disposal stations are located in different places. When the self scanning device is on the dispensing wall or in standby mode, the idle screen is displayed. When the customer removes the self scanning device, the welcome screen is displayed.

11.4 Returning the Mobile Self Scanning Device - Device Disposal Station

A customer must confirm with **OK** that they have scanned all the items in the shopping basket. This process should be completed before handing over the self scanning device, but before beginning payment at the latest.

11.4.1 Systems at the Device Disposal Station

Physical systems	Count	Purpose of use
End-of-trip barcode	1-n	The customer scans this barcode to end their shopping trip.
Device disposal wall	1-n	Contains cradles that are ready for the return of mobile self scanning devices. Customers put the self scanning devices back into the cradles.

11.4.2 Ending the Trip

To end the trip, the customer must scan the end-of-trip barcode located near the device disposal wall.

A customer must confirm with **OK** that they have scanned all of the items in the shopping basket. This process is a security measure required for legal reasons and should be completed before handing over the self scanning device, but before beginning payment at the latest.
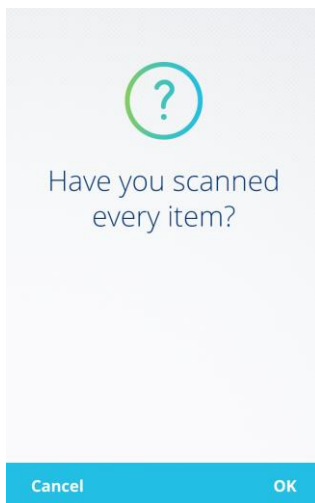

Abbildung 5 All Items [18]

11.5 Service

11.5.1 Removing the Self Scanning Device

A member of staff must remove the mobile self scanning devices from the cradles on the device disposal station periodically and return them to the dispensing station. The member of staff scans the service barcode on the Wall Device Manager terminal, the cradles are unlocked, and the self scanning devices can be removed. The removed self scanning devices can then be put back into the empty cradles on the dispensing station. The software installed on the Wall Device Manager then controls which self scanning devices are dispensed so that they are sufficiently charged.

11.5.1.1 Bulk Removal

It is possible to remove one single self scanning device from the device disposal wall or to unlock and remove all devices in a defined zone. The number of devices that can be removed at once from a zone is configurable. To perform bulk removal, scan the service barcode on the Wall Device Manager terminal. Bulk removal generally takes place from top left to bottom right.
When the cradles flash, it means the Wall Device Manager has released these devices for removal. The first

device that can be removed flashes. When the member of staff removes the flashing device, the next device that can be removed begins to flash and so on. The device to be removed next is always the one that is flashing. This procedure is repeated until the last removable device is removed.

11.5.2   Swapping Self Scanning Devices

11.5.2.1   Standard Case - Manual Reset

The self scanning device monitors its battery status continuously and displays a corresponding warning message when the charge status drops below a defined level.
The customer contacts a member of staff. The member of staff scans the service barcode, which initiates the reset of the shopping basket with the customer number. The data is no longer available on the self scanning device previously used. The member of staff scans the service barcode and then the customer card using a fully-charged self scanning device. The customer's shopping basket is transferred to the new self scanning device and the device switches to capture mode automatically. The customer can continue shopping. The self scanning device with the low battery is returned to the cradle for charging.

11.5.2.2   Special Case 1 - Automatic Reset

The self scanning device monitors its battery status continuously and displays a corresponding warning message when the charge status drops below a defined level.
The customer ignores the warning message. The battery charge level continues to drop. When the charge level drops below another defined level, a corresponding warning message is displayed on the self scanning device.
The self scanning device initiates the reset of the shopping basket and customer number automatically and shuts down. The data is no longer available on the self scanning device previously used. The customer contacts a member of staff. The member of staff scans the service barcode and then the customer card using a fully-charged device. The customer's shopping basket is transferred to the new self scanning device and the device switches to capture mode automatically. The customer can continue shopping. The self scanning device with the dead battery is returned to the cradle for charging.

11.5.2.3   Special Case 2 - Reset Not Possible

If the self scanning device cannot reset the shopping basket because of a low battery, because the device is currently offline, or due to a device defect that prevents the reset process, the customer must contact a member of staff. The member of staff removes another self scanning device and uses it to scan the service barcode. The member of staff then scans the customer card. The system searches for a reset or open shopping basket that matches the scanned customer number. The member of staff must confirm that the shopping basket and its corresponding customer number have been transferred to the new device. The new self scanning device subsequently changes to capture mode. The customer can continue shopping.