

A COMMUNICATIONS SERVER, A METHOD, A USER DEVICE AND A SERVICE

Technical Field

The invention relates generally to the field of communications. One aspect of the invention relates to a communications server apparatus for a group e-wallet. Another aspect of the invention relates to a method, performed in a communications server apparatus for a group e-wallet related to an e-commerce service. Another aspect of the invention relates to a communications device for communicating with a group e-wallet payment gateway. Another aspect of the invention relates to a service for a group e-wallet. Another aspect of the invention relates to a method, performed in a service related to a group e-wallet.

One aspect has particular, but not exclusive, application in applying e-wallets in countries with a significant unbanked population. For example, where a group e-wallet may allow a single banked user to spawn a significant number of new users into the digital economy.

Background

Various forms of digital payment exist.

For example, TWM605832, US20140188719, US20120197794, US10445739, US20170243200, and US20180276655 disclose various shared e-wallets. These prior approaches generally share a primary user's main e-wallet, and/or do not limit or control how much or on what funds can be spent.

Summary

Embodiments may be implemented as set out in the independent claims. Some optional features are defined in the dependent claims.

Implementation of the techniques disclosed herein may provide significant technical advantages. Advantages of one or more aspects may include:

- Sharing a group e-wallet as a payment method with multiple secondary users to pay for authorized service categories;

- Reducing cash dependency for payment transactions by onboarding unbanked populations to an e-wallet and allowing them to share a common group e-wallet owned by a banked family member or friend or known person;

- Better security for unbanked populations;

- Minimising CO₂ emissions for taxi fares that were incorrectly authorised e.g.: family members who were not entitled to request taxi fares on a shared e-wallet, or have spent over their budget;

- Providing controlled access of group e-wallet's shared funds to secondary users;

- Allowing access of group funds only for authorized service categories;

- Allowing access of group funds only for authorized merchants;

- Checking validity of authorized Merchants through a merchant category validation process;

- Reduce fraud around group e-wallets;

- Better security for group e-wallets; and/or

- Improvements in scalability, high availability, lower latency, higher transactions per second (TPS).

In at least some implementations, the techniques disclosed herein may provide for using a group e-wallet that is separate from a primary user's main e-wallet, where each group e-wallet has limits of spending on authorized spending categories. This may allow the transaction to be authenticated against a secondary user, spending limits, privileges.

In an exemplary implementation, the functionality of the techniques disclosed herein may be implemented in software running on a server communications

apparatus, such as a cloud based geographically distributed database. The software which implements the functionality of the techniques disclosed herein may be contained in a computer program, or computer program product – which operates the database instances on each server node in the cloud. When running on, for example, a cloud server, the hardware features of the server may be used to implement the functionality described below, such as using the server network communications interface components to establish the secure communications channel for a group e-wallet in an efficient fashion.

In one aspect there is provided a communications server apparatus for a group e-wallet related to an e-commerce service, the communications server comprising a processor and a memory, the communications server apparatus being configured, under control of the processor, to execute instructions stored in the memory, to:

- receive a transaction request from a customer for the group e-wallet in relation to a service category;
- determine if the customer is authorised for the e-wallet;
- determine if the service category is valid for the customer; and
- allow the transaction if the customer is authorised and the service category is valid, and deny the transaction otherwise.

In another aspect there is provided a method, performed in a communications server apparatus for group e-wallet related to an e-commerce service, the method comprising, under control of a processor of the communications server apparatus:

- receiving a transaction request from a customer for the group e-wallet in relation to a service category;
- determining if the customer is authorised for the e-wallet;
- determining if the service category is valid for the customer; and
- allowing the transaction if the customer is authorised and the service category is valid, and denying the transaction otherwise.

In a further aspect there is provided a communications device for communicating with a group e-wallet payment gateway comprising a processor and a memory, the communications device being configured, under control of the processor, to execute instructions stored in the memory to:

- request the group e-wallet payment gateway process a transaction;

- if the customer is authorised for the e-wallet, and if the service category is valid for the customer, receiving a transaction confirmation from the group e-wallet payment gateway.

In a still further aspect there is provided a Service for a group e-wallet, comprising:
a communications server; and

a communications network equipment operable for the communications server, at least one merchant communications device, and at least one customer communications device, to establish communication with each other therethrough; wherein the customer communications device comprises a first processor and a first memory, the user communications device being configured, under control of the first processor, to execute first instructions stored in the first memory to:

- request a transaction to the communications server using the group e-wallet;

and wherein the communications server comprises a second processor and a second memory, the communications server being configured, under control of the second processor, to execute second instructions stored in the second memory to:

- determine if the customer is authorised for the e-wallet;

- determine if the service category is valid for the e-wallet; and

- allow the transaction if the customer is authorised and the service category is valid, and deny the transaction otherwise.

and wherein the merchant communications device comprises a third processor and a third memory; the merchant communications device being configured, under control of the third processor, to execute third instructions stored in the third memory to:

- receive data from the communications server confirming the transaction has been successfully processed.

In a still further aspect there is provided a method, performed in a service related to a group e-wallet, the method comprising, under control of a processor for one or more server instances:

- receiving a transaction request from a customer for the group e-wallet in relation to a service category;
- determining if the customer is authorised for the e-wallet;
- determining if a transaction value is valid for the e-wallet, and/or the customer;
- determining if the service category is valid for the customer; and
- allowing the transaction if the customer is authorised, the transaction value is authorised, and the service category is valid, and denying the transaction otherwise.

Brief Description of the Drawings

The invention will now be described, by way of example only, and with reference to the accompanying drawings in which:

Fig. 1 is a schematic block diagram illustrating an exemplary ride hailing service.

Fig. 2 is a schematic block diagram illustrating an exemplary communications server apparatus for a group e-wallet related to a transportation service.

Fig. 3 is a schematic block diagram illustrating an exemplary group e-wallet architecture.

Fig. 4 is a flow diagram illustrating an exemplary e-wallet creation process.

Fig. 5 is a screenshot of the steps in Figure 4.

Fig. 6 is a flow diagram illustrating an exemplary e-wallet secondary user adding process.

Fig. 7 is a screenshot of the steps in Figure 6.

Fig. 8 is a flow diagram illustrating an exemplary e-wallet top up process.

Fig. 9 is a screenshot of the steps in Figure 8.

Fig. 10 is a flow diagram illustrating an exemplary e-wallet transaction process.

Fig. 11 is a screenshot of the steps in Figure 10.

Fig. 12 is a schematic of an example database structure.

Fig. 13 is a schematic of an exemplary authentication process.

Fig. 14 is a schematic of an exemplary e-commerce payment option selection

Detailed Description

The techniques described herein are described primarily with reference to use in point of sale transactions, ecommerce transactions, taxi, ride hailing, ride sharing, food delivery, online groceries, service / trade exchanges, and pet transport, but it will be appreciated that these techniques have a broader reach and can be usefully implemented in other fields where a group e-wallet may be useful.

One or more embodiments may have particular application in a country where the unbanked (people without bank account) population is high. In countries like that, where people depend mostly on cash transactions; e-wallet adoption is low due to the need to have a bank account to fund the e-wallet. One or more embodiments may help when an e-wallet holder wants to share portion of his or her e-wallet money to specific set of people but wants to have control over what service categories those people can spend the group e-wallet funds on.

The segment of people which may be potential beneficiaries of Group e-wallet are: Middle class families with single(or 2) bank account holder where other unbanked members are heavily dependent on cash for their day to day purchase, small time business owners, Friends Group, Children(who gets cash as pocket money from their parents).

Figure 1 shows a ride hailing system 100, with a number of users each having a communications device 104, a number of drivers each having a user interface communications device 106, a server 102 (or geographically distributed servers) and

communication links 108 connecting each of the components. Each user contacts the server 102 using an app on the communications device 104. The user app may allow the user to enter their pick-up location, a destination address, a level of service and/or after ride information such as a rating. The level of service may include the number of seats of the vehicle, the style of vehicle, level of environmental impact and/or what kind of transport service. It may be also used to order food, groceries, trades or services or deliveries. Each driver contacts the server 102 using an app on the communications device 106. The driver app allows the driver to indicate their availability to take jobs, information about their vehicle, their location and/or after ride info such as a rating. The server 102 may then match users to drivers, based on: geographic location of users and drivers, maximising revenue, user or driver feedback ratings, weather, driving conditions, traffic levels / accidents, relative demand, environmental impact, and/or supply levels. This allows an efficient allocation of resources because the available fleet of drivers is optimised for the users' demand in each geographic zone.

Referring to Figure 2, a communications apparatus 100 is illustrated which may be used to implement the system of Figure 1. The communications apparatus 100 comprises the communications server 102, and it may include a user communications device 104 and a merchant or driver communications device 106. These devices are connected in the communications network 108 (for example, the Internet) through respective communications links 110, 112, 114 implementing, for example, internet communications protocols. The communications devices 104, 106 may be able to communicate through other communications networks, including mobile cellular communications networks, private data networks, fibre optic connections, laser communication, microwave communication, satellite communication, etc., but these are omitted from Figure 2 for the sake of clarity.

The communications server apparatus 102 may be a single server as illustrated schematically in Figure 2, or have the functionality performed by the server

apparatus 102 distributed across multiple server components. In the example shown in Figure 2, the communications server apparatus 102 may comprise a number of individual components including, but not limited to, one or more microprocessors 116, a memory 118 (e.g. a volatile memory such as a RAM, and/or longer term storage such as SSD (Solid State or Hard disk drives (HDD)) for the loading of executable instructions 120, the executable instructions defining the functionality the server apparatus 102 carries out under control of the microprocessor 116. The communications server apparatus 102 also comprises an input/output module 122 allowing the server to communicate over the communications network 108. User interface 124 is provided for user control and may comprise, for example, computing peripheral devices such as display monitors, computer keyboards and the like. The server apparatus 102 also comprises a database 126, the purpose of which will become readily apparent from the following discussion.

The user communications device 104 may comprise a number of individual components including, but not limited to, one or more microprocessors 128, a memory 130 (e.g. a volatile memory such as a RAM) for the loading of executable instructions 132, the executable instructions defining the functionality the user communications device 104 carries out under control of the microprocessor 128. The user communications device 104 also comprises an input/output module 134 allowing the user communications device 104 to communicate over the communications network 108. A user interface 136 is provided for user control. If the user communications device 104 is, say, a smart phone or tablet device, the user interface 136 will have a touch panel display as is prevalent in many smart phone and other handheld devices. Alternatively, if the label communications device is, say, a desktop or laptop computer, the user interface 136 may have, for example, computing peripheral devices such as display monitors, computer keyboards and the like.

The merchant or driver communications device 106 may be, for example, an e-commerce website. It may be a point of sale terminal. It may be a smart phone or tablet device with the same or a similar hardware architecture to that of the user communications device 104. Alternatively, the functionality may be integrated into a bespoke device such as a taxi job management device.

Thus, it will be appreciated that Figures 2 and 3 and the foregoing description illustrate and describe a communications server apparatus 102 comprising a microprocessor 116 and a memory 118, the communications server apparatus 102 being configured, under control of the microprocessor 116, to execute instructions 120 stored in the memory 118:

- receive a transaction request from a customer for a group e-wallet in relation to a service category;

- determine if the customer is authorised for the e-wallet;

- determine if the service category is valid for the customer; and

- allow the transaction if the customer is authorised and the service category is valid, and deny the transaction otherwise.

Further, it will be appreciated that Figure 4 and the foregoing description illustrates and describes a method performed in a communications server apparatus 102, the method comprising, under control of a microprocessor 116 of the server apparatus 102:

- receiving a transaction request from a customer for a group e-wallet in relation to a service category;

- determining if the customer is authorised for the e-wallet;

- determining if the service category is valid for the customer; and

- allowing the transaction if the customer is authorised and the service category is valid and denying the transaction otherwise.

The following terminology will be used throughout:

e-Wallet	an electronic device, online service, or software program that allows one party to make electronic transactions with another party bartering digital currency units for goods and services. The digital currency units may be based on or backed by real currency, or by virtual currencies such as bitcoin.
e-Wallet provider	a financial institution similar to a credit card provider that holds funds for users in e-wallets.
Merchant	a provider of goods or services who accepts payment from a payment gateway.
Merchant type	categories of merchants according to the type of goods or services e.g.: medical expenses would cover doctors, pharmacies.
Primary User	a user with a main e-wallet who may create a group e-wallet
Secondary User	a user who is has a privilege to a group e-wallet added by a primary user.
Spending limit	total amount a secondary user can spend from group e-wallet.
AVL Limit	Available or remaining amount for a secondary user from a group e-wallet for spending.
Budget	Total Capacity of a group e-wallet. Cumulative monthly spending from a group e-wallet cannot breach this amount.
Balance	Available/current balance of the group e-wallet.
MCC	Merchant Category Code is a four-digit number listed in ISO 18245 for retail financial services. A MCC is used to classify a business by the types of goods or services it provides.
MCG	Merchant Category Groups are broader categories of MCC. Each MCG group defines a set of MCCs of similar/related category of services. Each MCG is an example of a Service category.
Service Category	Categories of services that are valid to be used for each group e-wallet. This may be internal goods categories, internal service offerings, or universal goods of services categories. For example, a Grab primary group e-wallet use may be able to limit secondary

users' use of the group e-wallet funds to transaction types including Grab Transport, and Grab Food, and/or MCG broad categories using Online or Offline transactions.

Virtual Account	Identifier account created for each internal good/service categories or merchants.
Grab Transport	Taxi or ride hailing booking service provided by Grabpay app. This is an example of a Service category.
Grab Food	Food delivery service provided by Grab app. This is an example of a Service category.
Purchase	Buying of Online & Offline Merchandise/services.
Transaction Type	unique Transaction Types may be assigned for internal goods/services categories . E.g.: BOOKING_CHARGE for Grab Transport Service, FOOD_CHARGE for Grab Food delivery Service , P2M_CHARGE for Purchase Service etc for online or offline P2M transactions. Transaction types may be selected according to the requirements of the application.

With traditional e-wallets, each user has their own e-wallet, although it is sometimes possible to share your e-wallet with other users. Embodiments may seek to provide a group e-wallet, which is separate from the primary user's main e-wallet, which may include restrictions and monitoring on the group e-wallet to allow effective management of the group e-wallet by the primary user.

In an example embodiment of ride hailing, the customer may be a secondary user. In order for a customer to pay for a ride hailing trip using a designated app on their mobile phone, they must be authorised as a secondary user for a particular group e-wallet, that group e-wallet must include transport (or Grab Transport, for example, in the Grab implementation) as an allowed service category, and there are sufficient funds for that secondary user for the transaction. Other examples will be provided below.

Figure 3 illustrates an example payment processing system 300 using a group e-wallet. A customer 302 makes a transaction request 304 to a merchant 306. The request may include details of the respective group e-wallet and/or the e-wallet provider. The Merchant passes the request to group e-wallet provider 308. A group e-wallet service platform 310 checks whether the customer is authorised as a secondary user for a particular group e-wallet, whether the group e-wallet balance will be breached, whether the secondary user's spending limit will be breached, whether the AVL limit for that secondary user will be breached, and whether that secondary user has the privileges for that service category. On successful authorisation, the transaction amount will be deducted from the group e-wallet and merchant virtual account will be credited. At the end of each day, the Merchant's bank account 312 will be credited via a settlement 314 process.

For example:

1. A primary user wants to manage expenses the family household expenses, a road trip expenses with friends, and manage small business expenses like lunch expenses for co-workers, smaller maintenance expenses for your office space etc.
2. If the primary user shares his/her e-wallet with family members, friends, co-workers, there is no easy way to configure category wise expense limits, or spending limits for the other users.
3. There may be no easy or direct way to find out how much is spent on household expenses, how much on business or how much on a road trip. The Primary user may have to sum up each user's expenses and do mathematical calculations to get these answers. It adds another layer of difficulty if the same users are part of family expenses and business expenses.
4. With a group e-wallet all these things become easy, and it is possible to drill down the expense management to a much more granular level. ex: Out of \$1500 of household expenses how much have been spent on food expenses, entertainment expenses, grocery exp, children's pocket money etc.

Referring to Figure 4 a method 400 of creating a group e-wallet is shown. The primary user provides 402 a group name, maximum spending limit, any auto top up details. In the next step he/she needs to choose list of transaction types / service categories authorized for the group e-wallet. For example, if Purchase is chosen as an authorized transaction type, in that case the primary user will have option to authorize either all MCGs or selection from a list of MCGs as shown in Figure 5. The system 300 checks whether the group name is unique for primary user 404, and if it is, the group is created 406.

The privileges of a primary user and a secondary user are shown below in Table 1:

Primary User	Secondary User
Create new group	View Group e-Wallet Balance(For that member)
Add/edit/remove members to the group	Choose group e-wallet as payment option
Configure spending limits for secondary users	
Add funds to the group e-wallet	
View Group e-Wallet Balance (Overall)	
View member list	
View spending history for all members of a group	

Choose group e-wallet as payment option	
---	--

Referring to Figure 6 a method 600 of adding a secondary user to a group e-wallet is shown. The primary user chooses an existing e-wallet to add secondary users to 602. For the new secondary user, identification information is entered 604 as shown in Figure 7. If that person exists within the database 126 then a one time password “OTP” is sent 606 to the prospective secondary user’s mobile phone. If not, the primary user is informed 608 the secondary user is not registered in the system. Once the primary user receives the OTP from the prospective secondary user, and if entered correctly 610, in the next screen primary user will choose allowed transaction types / service categories for the secondary user, and then the secondary user is added 612 to the group e-wallet. The List of allowed service categories for secondary users in a Group e-wallet will always be sub-set of allowed service categories for that group e-wallet.

Referring to Figure 8 a method 800 of adding value to a group e-wallet is shown. The primary user chooses 802 an existing e-wallet to add value to. The primary user chooses 804 a value to add, and if the balance after top-up doesn’t exceed 806 the spending limit of the group e-wallet, the top up is processed 808 as shown in Figure 9. The source of funds may be the primary user’s main e-wallet, a credit card, or funds transfer from a bank account.

Referring to Figure 10 a method 1000 of transacting using a group e-wallet is shown. The primary or secondary user initiates 1002 a transaction. The user selects 1004 a group e-wallet as a source of funds for the payment. If the transaction is valid 1006 the payment is processed 1008, otherwise it fails 1010.

Determining if the transaction is valid 1006 may involve several checks. First it may check if the Group e-wallet balance is more than transaction value. Secondly it may check if the transaction amount is less than the secondary user's spending limit. Thirdly it may check if transaction amount is less than the secondary user's AVL limit .

Fourthly it may check if the user is authorised for the Service Category of the transaction. When a user tries to use the Group e-wallet as payment method to pay using a mobile app, the payment App may send applicable TRANSACTION TYPE along with other payment metadata to the group e-wallet service platform 310. The service platform 310 may choose to allow or restrict that payment depending upon user's privilege which have been assigned to the user by the primary user while adding him/her in the group e-wallet.

In case of P2M_CHARGE transaction type, it may validate the merchant by checking if the merchant is part of user's authorized MCGs for this group e-wallet. If not, transaction request will be rejected.

In Figures 5, 7, 9 and/or 11 a Pie chart is shown. This is an example of a spend analysis graph that may be included for the group e-wallet. Primary user will have access to that chart as well as a history screen, where he /she can analyse the spending of each secondary user.

MCCs are used to identify the type of business in which a merchant is engaged. The selection of service categories may depend on the requirements of the application. It may rely on a customised MCG list or they may refer to any of the card processing system's MCG list.

An example list of MCCs is provided below:

Merchant Category Code	Description	Examples
5411	Grocery stores and supermarkets	D'Agostino, Fairway Market, Whole Foods
5812	Eating places and Restaurants	TGI Friday's
5814	Fast Food Restaurants	McDonald's, Burger King, Subway
5912	Drug Stores and Pharmacies	CVS, Duane Reade, Walgreens
8062	Hospitals	Mount Elizabeth Hospital
5611	Men's Boys clothing and accessories stores	Dockers
5621	Women's Ready to wear stores	Forever21
5441	Candy Stores	Hershey's Chocolate World, Candy Empire
5451	Dairy Products Stores	Lactalis Singapore Pte Ltd Fresh Milk Suppliers Pte Ltd
5399	Merchandise Stores	Shopee, Qoo10.sg,
5999	Miscellaneous and Specialty Retail Stores Online Shopping	Amazon.sg
5311	Department Stores Online shopping	Lazada
5045	Computers, peripherals and software	Helping
5734	Computer software store	Adobe Creative Cloud subscription
5732	Electronics Stores	Challenger, Best Denki Etc.
5541	Service Stations (With or Without Ancillary Services)	7-Eleven
5542	Fuel Dispenser, Automated	Shell Petrol Kiosks

4121	Taxicabs and Limousines	UBER, GRAB
7011	Lodging - Hotels, Motels, Resorts	the Marina Bay Sands, MANDARIN ORIENTAL SINGAPORE
7298	BEAUTY OR HEALTH SPAS	Aramsa - The Garden Spa Bio Beauty Aromatic Spa
7230	BARBER OR BEAUTY SHOPS	Rogue and Beyond , Lily Head & Hair Spa

An example list of MCGs is provided below:

MCG	MCC
Online merchandise	5399,5999,5311
Fashion	5611,5621
Medical	8062,5912
Glossary	5411,5441,5451
Food & Dining	5812,5814
Personal Care	7298,7230
Travel & Acco	7011,4121
Fuel	5541,5542

While processing a P2M_CHARGE transaction type for a group e-wallet, the group wallet service platform 310 will get the Merchant information from the payment request payload, then it will make a service call to the merchant database 316 to get metadata for that merchant. The metadata may contain the MCC along with other merchant information. Then group e-wallet service will fetch the Merchant category group(MCG) for that merchant category code. Once MCG is retrieved from MCG store, then the service will retrieve user privileges from GROUP_WALLET_MEMBER_PREV and PURCHASE_PREV table (described later) and validates if that MCG is authorized to that secondary user. In case of a validation failure, the transaction request will be rejected, else it will be processed after the sufficient funds validation steps.

MCG store can be persistent in the database DB, but it can also be cached. Caching a MCG store can utilise a simple key value store which is highly available, and fault tolerant.

The process of onboarding a merchant into system 316 may include storing in a database, information similar to the below:

GrabID:xxxx-e995-4b82-a310-xxxxxxxxx

GrabPayID:538575217xxxxxx

MerchantID:931315558xxxxxx

Timezone:Asia/Jakarta

RegdDate:01-OCT-2019 04:31:17

RegdNumber: XXXX

RegdAddress: XXXX

RegdDocumentID: XXX

ISOCurrency:360

BranchName:Chixxxxx

City: jakarta, Indonesia

BusinessLegalName:xxxxx

BusinessTradingName:xxxxx

CDDExempted:false

CDDExemptedReason:

MCC:5812

MCG:Dining & Entertainment

ReserveAmount:0

SanctionCheck:false

WithdrawAllowed:false

ReserveTypeID:

BusinessTypeID:0

BusinessActivityID:

UBOSearchExempted:false
UBOSearchExemptedReason:
RiskCategoryID:0
MerchantRiskComments:
EstimatedMonthlyTurnOver:0
SanctionDocumentID:
Comments:
KycLevel:0
WalletType:0
RiskCategoryComplianceID:0
MerchantRiskCommentsCompliance:
BusinessActivityByGrabPayID:
AgentID:
TerminalID:
TerminalsIDs:[2359e913e5885460b3979xxxx 0f09e03989990666e0913xxxx
e47ab03093746a73d9779xxxx ed0f94d07e7ff0890fcc3xxxx
b7fb0cebff54637c67513xxxx c7d943a7d6d60eff6fafdxxxx]
PartnerID:ID001
UserBlockedStatus:{Transaction:false Withdrawal:false}
KycDetails:{KYCLevel:1 TransactionLimit:{WithdrawalAllowed:false
WalletStorageLimits:0 UnlimitedTransactionLimit:false TransactionLimits:0
PreApprovedTimeStamp: TimeFrameLimitInMins:0}}

Payment ledger:

The Group e-wallet may maintain a double ledger for all it's transactions. A Debit ledger will be maintained for Customer accounts. And a Credit ledger will be maintained for internal goods of services accounts. Virtual account may be created for all Merchants. This ledger system will be used by offline settlement system for End Of The Day Settlement. The transaction ledger information will be stored in TRANSACTION_LEDGER table shown in Figure 12. For each payment transaction, one

entry is made for debit transactions and one for credit transaction to maintain double entry book keeping standards. The amount field will have a signed value to identify Debit or Credit transactions. This ledger table may be used to find any discrepancy in payment processing. Total amount of debit and total amount of credit should be same at any point of time. This table may be used for audit compliance as well.

The payment processing system 300 may be implemented as a microservice based distributed architecture to handle high traffic with minimal processing latency. This design will ensure high availability of the service. A load balancer manages the distributed microservices, together with a series of nginx servers for request re-routing. This nginx servers provide the ability to scale up to dedicated servers for certain sets of high traffic requests. App instances will be auto scaled to support horizontal scaling of traffic.

The database 126 may be an ACID compliant relational DB based on Master-worker architecture. Master nodes may be used for all write transactions, and Replicas may be used for any read request. A time series based columnar database may be used, for example, NoSql DB, may be used for historical data (as opposed to the transactional data which needs an ACID compliant database). The transaction history can be streamed via a messaging system and dumped to NoSql for transaction history search, and optimised for better read performance with lower latency.

Transactional tables may be partitioned to handle higher scalability. The data model will be flexible enough to be extended to sharding if the application requires it. An example table structure is shown in Figure 12.

For example, the spending limit is stored in SPENDING_LIMIT in Group_Link table. The budget is stored under HOLDING_AMOUNT column in GROUP_WALLET table. Secondary user's Privileges are stored in ALLOWD_TXNS in Group_Link table.

MCC may be retrieved from the Merchant onboarding system 316 via a Restful API which will respond with MCC code along with other Merchant Metadata. Group e-wallet service platform 310 will use those merchant metadata and Group e-wallet or secondary user's Privileges to validate secondary user's transactions.

The Customer_Transaction table may be partitioned on TXN_DATE. The partitions may be a monthly partition. For example, the total number of Partition may be 13. Any data which is more than 12 months old may be archived and that partition will be deleted.

Advantages of partitioning Customer_Transaction Table may include write throughput and read throughput increases as data will be divided among multiple partition, so volume of a single partition will be less (only 1 month data) compared to total volume, and/or once Archived, purging an older partition is easy.

Vertical scaling can be helpful up to a certain threshold, beyond that horizontal scaling may be useful. Partitioning may be helpful up to certain threshold, if data grows beyond that level, we may shard the data to horizontally scale the DB for seamless scaling. Vitress, TiDB, CockroachDB can be used to horizontally shard the data. Sharding can be done on account_id. So, a single customer's data will always reside in same shard and data will be evenly distributed among all shards which may provide seamless scaling.

Authentication

Authentication between the user device 104 and the server 104 may use OAuth 2.0.

Authentications between other internal micro services and the group e-wallet microservice may use HMAC (SHA 256 based message authentication code), where the services will maintain a shared public key, which will be used together with the

message to generate a signature. This may avoid sending the user credentials over the network. All the calls will be made over SSL/TLS.

Another alternative is JWT token based authentication. A JWT based authentication design is shown in Figure 13. JWT authentication may provide:

- Tokens are stateless. The token is self-contained and contains all the information it needs for authentication. This is great for scalability as it frees the server from having to store session state.
- Tokens can be generated from anywhere. Token generation is decoupled from token verification allowing the option to handle the signing of tokens on a separate server or even through a different company such as Auth0.
- Fine-grained access control. Within the token payload you can easily specify user roles and permissions as well as resources that the user can access.

As mentioned above adding members to a group will be done via OTP based authentication. This ensures that a member's consent is provided before being added into a group.

Transaction privileges will be handled by an application-based roles and permission based framework where each member will be assigned a role to have access to a certain set of transaction permissions. The permissions are stored in the database 126.

e-Commerce website example (P2M):

In the event a secondary user wishes to pay for a transaction on an e-Commerce website using a group e-wallet, the following steps may be taken. These may be varied according to the requirements of the application.

Each merchant is onboarded as an e-commerce vendor in Group e-wallet internal or external merchant onboarding system. The e-commerce vendor enables Group e-wallet as a payment option in their e-commerce checkout page.

1. A Customer places an order on website by pressing the 'Submit Order' or equivalent button together with the option to pay using a group e-wallet from a particular e-wallet provider.
2. If the customer's e-wallet is already linked with that e-commerce account, a payment authorization request will be sent from e-commerce vendor to e-wallet service platform via pre-defined service contract.
3. If customer's e-wallet is not linked in that ecommerce's account, another pop up will open where customers need to authenticate them in e-wallet login page. This will get validated in the e-wallet website to verify their e-wallet account and post that a payment authorization request will be sent from e-commerce platform to e-wallet service platform via a pre-defined service contract.
4. The payment request will contain payment metadata information like customer information, merchant information, txn amount, date, payment description etc.
5. On receiving the payment request, based on the request payload that the service platform receives, the platform is able to identify the Customer, merchant, transaction amount, date/time of transaction, transaction type etc. e-wallet back end will evaluate if the customer has only primary e-wallet or combination of primary e-wallet and one or more group e-wallet.

If the customer has just a primary e-wallet,

- A. Customer can be asked to authenticate using a Pin if the transaction amount is above a certain threshold. Threshold will be a configurable value which could be defined based on the product/regulatory/risk-check requirement.
- B. Once PIN is authenticated, payment request is validated against various business rules.

i) Business rules validation includes checks like (not limited to) account status check, transaction permissions, transaction limit, etc.

C. Once the validations are successful, the authorization amount will be held against the Customer's primary e-wallet. This can impact the customer's ability to spend further (because it reduces the group e-wallet funds available). This is known as the Authorization or "Auth.". A response will be sent back to the Merchant [ecommerce platform in this case], via the same process as the request for authorization, with a response code (i.e.: approved, denied (in case validation fails)). In addition to communicating the fate of the authorization request, the response code is also used to define the reason why the transaction failed (i.e.: insufficient spending limit, or not authorised group member).

If the customer has combination of primary wallet and group e-wallet, the e-wallet service platform will send a push notification to the customer's app. The customer will open the push notification and choose the e-wallet [either primary e-wallet or one of the group e-wallet] as shown in Fig 14 from the dropdown and submit the button "PAY" or equivalent button. On successful submission, e-wallet service platform will receive the payment method information for that transaction.

The customer can be asked to authenticate using a Pin if the transaction amount is above a certain threshold. The threshold will be a configurable value which could be defined based on the product/regulatory/risk-check requirement.

The e-wallet service platform will interact with merchant platform and get merchant meta data (which can include status, mcc, location etc) required for processing the transaction.

D. Once the Authorisation is received from the merchant platform, Customer and Merchant are validated against various business rules.

- i) Business rules validation includes checks like (not limited to) account status check, transaction permissions, transaction limit etc.
- ii) Other validations related to group e-wallet like if the user is a verified member of the Group, Group transaction permission check, authorized merchant category group check [this check will evaluate if the merchant is part of the user's authorized MCG list] ,member spending limit check, group available balance check.

Once the validations are successful, the authorization amount will be hold in Customer's primary e-wallet. This can impact the customer's ability to spend further (because it reduces the group e-wallet funds available). This is known as the Authorization or "Auth.". A response will be sent back to the Merchant [ecommerce platform in this case] (via the same process as the request for authorization) with a response code (i.e.: approved, denied (in case validation fails)). In addition to communicating the fate of the authorization request, the response code is also used to define the reason why the transaction failed (i.e.: insufficient spending limit, or not authorised group member).

6. The merchant platform receives the response. For "approved" response, the merchant then fulfils the order and the above process can be repeated but this time to "clear" the authorization by consummating the transaction.

Typically, the "Clear" is initiated only after the merchant has fulfilled the transaction (i.e.: shipped the order). This results in the group e-wallet provider to debit the held amount from customer e-wallet and credit to merchant's virtual account.

7. After every successful auth clear transaction, group e-wallet service platform will send an intimation to settlement processor.

8. The settlement processor will run at the end of the day to collect all merchant transactions and initiate a cash out of the cumulative amount from merchant virtual account.
9. Once the cash out transaction is triggered, each merchant's virtual account gets debited with total settlement amount and the group e-wallet provider calculates fee amount (if any) and makes a settlement payment of remaining amount to the acquiring bank (the next day in most cases).
10. The group e-wallet provider makes a settlement payment to the acquiring bank (the next day in most cases).
11. The acquiring bank subsequently deposits the total of the approved funds into the merchant's nominated account (the same day or next day). This could be an account with the acquiring bank if the merchant does their banking with the same bank, or an account with another bank.

Merchant Payment using QR code (Example):

In the event when a secondary user wishes to pay at a merchant location using a group e-wallet and a mobile payment app using QR code:

1. Customer will scan the merchant's QR code using the mobile app, enters the amount to be paid and selects a group e-wallet as the payment method and submits.
2. Upon Submitting, the request will reach e-wallet service platform for processing. It receives the customer and merchant details for processing of transaction.
3. Based on the request payload that the service platform receives, the service platform is able to identify the customer, merchant, Transaction amount, date/time of transaction, transaction type etc.
4. Customer can be asked to authenticate using a Pin if the transaction amount is above a certain threshold. Threshold will be a configurable value which could be defined based on the product/regulatory/risk-check requirement.
5. e-wallet service platform will interact with merchant platform and get authorisation and other meta data (which can include status, mcc, location etc) required for processing the transaction.

6. Once the Authorisation is received from the merchant platform, Customer and Merchant are validated against various business rules.
7. Business rules validation includes checks like (not limited to) account status check, transaction permissions, transaction limit etc.
8. Other validations related to group e-wallet like whether the user is a verified member of the Group, Group transaction permission check, member spending limit check, group available balance check etc
9. Once the validations are successful transaction is processed. Customer's group e-wallet is debited, and a success notification is sent to the customers Mobile app and also to the merchant platform.
10. The transaction details are stored in the database.
11. The settlement processor will run at the end of the day to collect all merchant transactions and initiate a cash out of cumulative amount from merchant virtual account.
12. Once cash out transaction is triggered, merchants virtual account gets debited with total settlement amount and group e-wallet provider calculates fee amount (if any) and makes a settlement payment of remaining amount to the acquiring bank (the next day in most cases).
13. The group e-wallet provider makes a settlement payment to the acquiring bank (the next day in most cases).
14. The acquiring bank subsequently deposits the total of the approved funds into the merchant's nominated account (the same day or next day). This could be an account with the acquiring bank if the merchant does their banking with the same bank, or an account with another bank.

Similar steps can be followed for various other types of merchant payments like Merchant payment using Merchants phone number, QR code based Online Merchant Payment etc. In a of a POS scenario the acquiring platform will push the transaction request to e-wallet service platform instead of Customer's Phone. The way customer interacts with merchant might be different, but the other steps will remain same.

POS example (P2M)

In the event a secondary user wishes to pay for a transaction at a point of sale terminal using a group e-wallet and a mobile payment app, the following steps may be taken. These may be varied according to the requirements of the application.

1. The customer submits their mobile phone to a NFC scanner for payment. Prior to this the customer must have loaded the mobile payment app onto their phone for the group e-wallet provider, and authenticated with the group e-wallet provider. For each transaction the group e-wallet provider may require additional authentication such as a pin code or fingerprint recognition, such as with a transaction over a certain threshold.
2. On receiving the payment request, based on the request payload that the service platform receives, it is able to identify the Customer, merchant, transaction amount, date/time of transaction, transaction type etc. e-wallet back end will evaluate if the customer has only primary e-wallet or combination of primary e-wallet and one or more group e-wallet.

If customer has just primary e-wallet,

- A. Customer can be asked to authenticate using a Pin if the transaction amount is above a certain threshold. Threshold will be a configurable value which could be defined based on the product/regulatory/risk-check requirement.
- B. Once PIN is authenticated, payment request is validated against various business rules.
 - i) Business rules validation includes checks like (not limited to) account status check, transaction permissions, transaction limit, etc.

C. Once the validations are successful, the authorization amount will be hold in Customer's primary e-wallet. This can impact the customer's ability to spend further (because it reduces the group e-wallet funds availability). This is known as the Authorization or "Auth.".

A response will be sent back to the Merchant [ecommerce platform in this case] (via the same process as the request for authorization) with a response code (i.e.: approved, denied (in case validation fails)). In addition to communicating the fate of the authorization request, the response code is also used to define the reason why the transaction failed (i.e. insufficient spending limit, or not authorised group member).

If customer has combination of primary wallet and group wallet,

- A. e-wallet-service platform will send a push notification to app. Customer will open the push notification and choose the e-wallet [either primary e-wallet or one of the group e-wallet] as shown in Fig 14 from the dropdown and submit the button "PAY" or equivalent button. On successful submission, e-wallet service platform will receive the payment method information for that transaction
- B. Customer can be asked to authenticate using a Pin if the transaction amount is above a certain threshold. Threshold will be a configurable value which could be defined based on the product/regulatory/risk-check requirement.
- C. e-wallet service platform will interact with merchant platform and get merchant meta data (which can include status, mcc, location etc) required for processing the transaction.
- D. Once the Authorisation is received from the merchant platform, Customer and Merchant are validated against various business rules.

- i) Business rules validation includes checks like (not limited to) account status check, transaction permissions, transaction limit etc.
- ii) Other validations related to group e-wallet like if the user is a verified member of the Group, Group transaction permission check, authorized merchant category group check [this check will evaluate if the merchant, the user choose pay is part of the user's authorized Merchant category group] , member spending limit check, group available balance check etc

E. Once the validations are successful, the authorization amount will be hold in Customer's primary e-wallet. This can impact the customer's ability to spend further (because it reduces the group e-wallet funds available). This is known as the Authorization or "Auth.". A response will be sent back to the Merchant [ecommerce platform in this case] (via the same process as the request for authorization) with a response code (i.e.: approved, denied (in case validation fails)). In addition to communicating the fate of the authorization request, the response code is also used to define the reason why the transaction failed (i.e.: insufficient spending limit, or not authorised group member).

3. The merchant platform receives the response. For "approved" response, the merchant then fulfils the order and the above process can be repeated but this time to "clear" the authorization by consummating the transaction.

Typically, the "Clear" is initiated only after the merchant has fulfilled the transaction (i.e.: shipped the order). This results in the group e-wallet provider to debit the hold amount from customer e-wallet and credit to merchant's virtual account/sub account [depending on if split sub account is configured for the merchant or not] .

4. After every successful auth clear transaction, group e-wallet service platform will send an intimation to settlement processor.

5. The settlement processor will run end of the day to collect all merchant transactions and initiate a cash out of cumulative amount from merchant virtual account. In case Split-subaccount is enabled for the merchant, settlement process will trigger intermediate money movement transaction to move amount from all virtual sub accounts to the parent virtual account and then triggers a cash out transaction for the merchant.

6. Once cash out transaction is triggered, merchants virtual account gets debited with total settlement amount and group e-wallet provider calculates fee amount (if any) and makes a settlement payment of remaining amount to the acquiring bank (the next day in most cases).

7. The group e-wallet provider makes a settlement payment to the acquiring bank (the next day in most cases).

8. The acquiring bank subsequently deposits the total of the approved funds into the merchant's nominated account (the same day or next day). This could be an account with the acquiring bank if the merchant does their banking with the same bank, or an account with another bank.

It will be appreciated that the invention has been described by way of example only. Various modifications may be made to the techniques described herein without departing from the spirit and scope of the appended claims. The disclosed techniques comprise techniques which may be provided in a stand-alone manner, or in combination with one another. Therefore, features described with respect to one technique may also be presented in combination with another technique.

Claims

1. A communications server apparatus for a primary user's main e-wallet and a group e-wallet, comprising:

a communications server; and

a communications network equipment operable for the communications server, at least one merchant communications device, and at least one customer communications device, to establish communication with each other therethrough;

wherein the customer communications device comprises a first processor and a first memory, the customer communications device being configured, under control of the first processor, to execute first instructions stored in the first memory to:

request a transaction to the communications server using the group e-wallet;

and wherein the communications server comprises a second processor and a second memory, the communications server being configured, under control of the second processor, to execute second instructions stored in the second memory to:

determine if the customer is authorised for the group e-wallet;

determine if the service category is valid for the group e-wallet; and

allow the transaction if the customer is authorised and the service category is valid, and deny the transaction otherwise;

and wherein the merchant communications device comprises a third processor and a third memory; the merchant communications device being configured, under control of the third processor, to execute third instructions stored in the third memory to:

receive data from the communications server confirming the transaction has been successfully processed;

wherein the group e-wallet is separated from the primary user's main e-wallet.

2. The communications server apparatus of claim 1 wherein the service category includes merchant category groupings.
3. The communications server apparatus of any preceding claim wherein the communications server apparatus is further configured to determine if the transaction value is under a remaining balance for the group e-wallet.
4. The communications server apparatus of claim 3 wherein the communications server apparatus is further configured to determine if the transaction value is under a predetermined spending limit for the customer.
5. The communications server apparatus of claim 4 wherein the communications server apparatus is further configured to determine if the transaction value is under a remaining value limit for the customer.
6. The communications server apparatus of any preceding claim wherein the communications server apparatus is further configured to provide analytics of the group e-wallet spending history, and to display the analytics to the customer.
7. The communications server apparatus of any preceding claim wherein the customer has one or more privileges selected from the group consisting of: creating the group e-wallet, topping up the group e-wallet, adding secondary users to the group e-wallet, imposing spending limits for the group e-wallet or the secondary users, imposing merchant type limits for the group e-wallet or the secondary users, imposing transaction type limits for the group e-wallet or the secondary users.
8. The communications server apparatus of any preceding claim wherein the customer communication device is further configured to receive a request to transfer funds from the primary user's main e-wallet to the group e-wallet.

9. The communications server apparatus of any preceding claim further comprising a plurality of group e-wallets.
10. A method, performed in a service related to a primary user's main e-wallet and a group e-wallet, the method comprising, under control of a processor for one or more server instances:
- receiving a transaction request from a customer for the group e-wallet in relation to a service category;
 - determining if the customer is authorised for the group e-wallet;
 - determining if a transaction value is valid for the group e-wallet, and/or the customer;
 - determining if the service category is valid for the customer; and
 - allowing the transaction if the customer is authorised, the transaction value is authorised, and the service category is valid, and denying the transaction otherwise,
- wherein the group e-wallet is separated from the primary user's main e-wallet.
11. A computer program or computer program product comprising instructions for implementing the method of claim 10.
12. A non-transitory storage medium storing instructions, which when executed by a processor, cause the processor to perform the method of claim 10.