(19) Евразийское патентное ведомство

(11) 044223 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2023.07.31

(21) Номер заявки
201700605

(22) Дата подачи заявки
2017.12.27

(51) Int. Cl. ***H04L 29/06*** (2006.01)
H04W 68/00 (2009.01)

(54) СИСТЕМА И СПОСОБ УПРАВЛЕНИЯ PUSH-УВЕДОМЛЕНИЯМИ

(31) **2017144644**
(32) **2017.12.19**
(33) **RU**
(43) **2019.06.28**

(71)(73) Заявитель и патентовладелец:
ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО "СБЕРБАНК РОССИИ" (ПАО СБЕРБАНК) (RU)

(72) Изобретатель:
Шацких Павел Павлович, Седых Сергей Александрович, Талагаев Петр Александрович, Поздняков Вячеслав Владимирович, Семочкин Станислав Андреевич, Марин Андрей Алексеевич, Леванов Алексей Александрович (RU)

(74) Представитель:
Астафьева С.А., Герасин Б.В. (RU)

(56) US-A-6064990
US-A1-20110171936
US-A1-20120158580
US-B2-7254614
US-A1-20150261774
US-A1-20160140550
RU-C2-2614582

(57) Настоящее изобретение в общем относится к области обмена сообщениями, а в частности к системе и способу управления push-уведомлениями для информирования клиентов о банковских событиях и операциях, происходящих с их счетами, картами, продуктами, и о предложениях от банка. Технической задачей, на решение которой направлено заявленное изобретение, является повышение эффективности доставки сообщений клиенту с информацией о банковских событиях и операциях. Техническим результатом, достигаемым при осуществлении данной технической задачи, является повышение скорости и надежности доставки текста уведомлений от системы интернет-обслуживания физических лиц к устройству связи пользователя. Для обеспечения указанного выше результата разработана система управления push-уведомлениями, содержащая облачное хранилище данных, выполненное с возможностью определять по меньшей мере одно устройство связи пользователя для отправки push-уведомления; отправлять короткое push-уведомление, полученное от push-платформы, по меньшей мере на одно устройство связи пользователя; push-платформу, соединенную с облачным хранилищем данных, содержащую профиль по меньшей мере одного устройства связи пользователя, выполненную с возможностью отправки короткого и полного push-уведомления и резервных СМС, сгенерированных системой интернет-обслуживания физических лиц, в соответствии с запросом по меньшей мере одного устройства связи пользователя и параметрами токена безопасности (Security Token); push-шлюз для соединения push-платформы с системой интернет-обслуживания физических лиц и сервером автоматизированной системы банка; система интернет-обслуживания физических лиц, выполненная с возможностью принимать по меньшей мере от одного устройства связи пользователя параметры токена безопасности (Security Token) и генерировать параметры и текст коротких и полных push-уведомлений и резервных СМС в зависимости от операций, которые выполнены в автоматизированной системе банка на основе полученного запроса от устройства связи пользователя, для их отправки по меньшей мере на одно устройство связи пользователя.

044223 B1

044223 B1

Область техники

Настоящее техническое решение, в общем, относится к области обмена сообщениями, а в частности к системе и способу управления push-уведомлениями для информирования клиентов о банковских событиях и операциях, происходящих с их счетами, картами, продуктами и о предложениях от банка.

Уровень техники

В настоящее время существующая технология push-уведомлений имеет ряд существенных недостатков. Размер передаваемых данных сильно ограничен, в частности, для устройств с операционной системой iOS всего составляет 256 байт. Нет гарантий, что доставленное уведомление будет доступно мобильному приложению, поскольку первичная обработка push-уведомлений выполняется средствами операционной системы, без запуска приложения. Запуск приложения осуществляется или при нажатии функциональной кнопки в момент просмотра полученного сообщения пользователем, или при нажатии на сообщение в общем списке push-уведомлений, принятых мобильным устройством. Если пользователь удалит уведомление из списка, или после просмотра только что полученного уведомления просто закроет его без запуска приложения, то в мобильном приложении никакие данные этого уведомления не будут доступны. Дополнительно, с помощью push-уведомлений нельзя передавать закрытые данные, которые должны быть доступны клиенту только после авторизации в мобильном приложении.

Из уровня техники известно техническое решение, раскрывающее способ и систему управления сообщениями, описанное в заявке US 2015106456 (A1), патентообладатель: JVL Ventures, LLC, опубликовано: 16.04.2015. В данном решении обмен сообщениями осуществляется между поставщиками услуг и мобильными устройствами, оснащенными программным обеспечением для обмена сообщениями, в том числе push-уведомлениями. Данное решение является наиболее близким аналогом.

Недостатками известного решения являются отсутствие возможности оперативного информирования клиентов о банковских событиях и операциях посредством push-уведомлений.

Раскрытие изобретения

Технической задачей, на решение которой направлено заявленное техническое решение, является повышение эффективности доставки сообщений клиенту с информацией о банковских событиях и операциях. Техническим результатом, достигаемым при осуществлении данной технической задачи, является повышение скорости и надежности доставки текста уведомлений от системы интернет-обслуживания физических лиц к устройству связи пользователя.

Для обеспечения указанного выше результата разработана система управления push-уведомлениями, содержащая: облачное хранилище данных, выполненное с возможностью:

определять по меньшей мере одно устройство связи пользователя для отправки push-уведомления;

отправлять короткое push-уведомление, полученное от push-платформы, по меньшей мере на одно устройство связи пользователя;

push-платформу, соединенную с облачным хранилищем данных, содержащую профиль по меньшей мере одного устройства связи пользователя, выполненную с возможностью отправки короткого и полного push-уведомления и резервных СМС, сгенерированных системой интернет-обслуживания физических лиц, в соответствии с запросом по меньшей мере одно устройство связи пользователя и параметрами токена безопасности (Security Token); push-шлюз для соединения push-платформы с системой интернет-обслуживания физических лиц и сервером автоматизированной системы банка; система интернет-обслуживания физических лиц, выполненная с возможностью принимать по меньшей мере от одного устройства связи пользователя параметры токена безопасности (Security Token) и генерировать параметры и текст коротких и полных push-уведомлений и резервных СМС в зависимости от операций, которые выполнены в автоматизированной системе банка на основе полученного запроса от устройства связи пользователя, для их отправки по меньшей мере на одно устройство связи пользователя.

Также разработан способ управления push-уведомлениями, содержащий этапы, на которых:

получают посредством системы интернет-обслуживания физических лиц от устройства связи пользователя запрос на совершение операций в автоматизированной системе банка, а также параметры токена безопасности (Security Token), в состав которого входит присвоенный облачным хранилищем данных устройству связи пользователя push-адрес;

посредством системы интернет-обслуживания физических лиц генерируют параметры и текст коротких и полных push-уведомлений и резервных СМС в зависимости от операций, которые выполнены в автоматизированной системе банка на основе полученного запроса от устройства связи пользователя; передают сгенерированные параметры и текст коротких и полных push-уведомлений и резервных СМС через push-шлюз на push-платформу, соединенную с облачным хранилищем данных, содержащую профиль по меньшей мере одного устройства связи пользователя, выполненную с возможностью отправки короткого и полного push-уведомления и резервных СМС по меньшей мере на одно устройство связи пользователя, причем короткие push-уведомления по меньшей мере на одно устройство связи пользователя передаются через облачное хранилище данных.

Краткое описание чертежа

Для лучшего понимания сущности изобретения и чтобы более ясно показать, каким образом оно может быть осуществлено, далее будет сделана ссылка, лишь в качестве примера, на прилагаемый чер-

теж, на котором

фиг. 1 - схема системы взаимодействия системы интернет-обслуживания физических лиц и устройства связи пользователя.

Подробное описание технического решения

В соответствии со схемой, приведенной на фиг. 1, система взаимодействия системы интернет-обслуживания физических лиц и устройства связи пользователя содержит: по меньшей мере одно устройство 100 связи пользователя, систему 110 управления push-уведомлениями и по меньшей мере один сервер 107 автоматизированной системы банка, отвечающей за обработку входящего потока sms-сообщений от клиентов. Устройство 100 связи пользователя может представлять собой любое вычислительное устройство, выполненное с возможностями проводной или беспроводной связи с элементами системы 110 управления push-уведомлениями, например, мобильный телефон, планшет, стационарный или портативный компьютер, ноутбук и т.д. В состав системы 110 управления push-уведомлениями входят: облачное хранилище 120 данных, которое может представлять собой такие платформы или провайдеры push-уведомлений как GCM, APNS, WNS, например представляющие собой сервера, но не ограничиваясь ими; push-платформа 130, содержащая блок хранения данных 130.1; push-шлюз 140, обеспечивающий соединение push-платформы с системой 150 интернет-обслуживания физических лиц и сервером 107 автоматизированной системы банка, отвечающей за обработку входящего потока sms-сообщений от клиентов, а также содержащий блок хранения данных 140.1; система 150 интернет-обслуживания физических лиц, содержащая сетевой адаптер 150.1 для взаимодействия с push-шлюзом 140, блок 150.2 генерации уведомлений, интерфейс 150.3 mAPI, блок 150.4 хранения данных; CMC-шлюз 160.

Все элементы системы 110 могут быть реализованы на базе по меньшей мере одного процессора или микроконтроллера, модифицированных в программно-аппаратной части таким образом, чтобы обеспечить выполнение приписанных им ниже функций.

После установки мобильного приложения 100.1 на устройство 100 связи пользователя (или мобильное устройство) и активации настроек push-уведомлений, устройство 100 связи пользователя отправляет запрос на получение push-адреса в облачное хранилище 120 данных, причем запрос содержит данные, идентифицирующие устройство 100 связи пользователя, например идентификатор устройства, и используемые для регистрации устройства, как показано в Приложении 1. Запрос могут направлять посредством использования протокола обмена сообщениями XMPP, HTTP/2, HTTP, но, не ограничиваясь им. В ответ на запрос облачное хранилище 120 данных генерирует уникальный push-адрес и направляет сгенерированный push-адрес в устройство 100 связи пользователя, которое присваивает полученный push-адрес установленному экземпляру мобильного приложения 100.1. Идентификатор push-адреса генерируется автоматически и должен быть глобально уникален на протяжении всего времени взаимодействия между системой и push-шлюзом. В некоторых вариантах осуществления идентификатор может иметь численное или символьное значение. Также устройство связи пользователя 100 формирует токен безопасности (Security Token), в состав которого входит присвоенный push-адрес. Токен безопасности может представлять собой Base64-закодированную JSON строку, содержащую информацию об устройстве 100 связи пользователя. Данная информация может содержать значение хеш-функции (SHA1) от данных аутентификации пользователя, идентификатор устройства, который по умолчанию генерируется в момент установки приложения, однако может быть назначен через API, серийный номер устройства, адрес устройства в Push-сети, IP-адрес устройства, модель устройства, GPS координаты устройства, имя локали устройства и так далее, не ограничиваясь.

Генерацию push-адреса осуществляют следующим образом. Для логина клиента на установленном экземпляре мобильного приложения происходит проверка прав для включения push- уведомлений. Если прав не предоставлено, мобильное приложение не инициирует проверку. Если права предоставлены, мобильное приложение производит регистрацию конкретного экземпляра мобильного приложения в облачном хранилище 120 данных. При регистрации конкретному экземпляру мобильного приложения присваивается push-адрес, который генерируется на основе идентификатора экземпляра мобильного приложения.

Для направления запроса в виде POST-данных в систему 150 интернет-обслуживания физических лиц с устройства 100 связи пользователя на совершение каких-либо операций в автоматизированной системе банка, пользователю необходимо авторизоваться в приложении 100.1. После прохождения пользователем этапов авторизации приложение 100.1 запрашивает параметры токена безопасности (Security Token) у устройства 100 связи пользователя и передает их вместе с запросом в в систему 150 интернет-обслуживания физических лиц посредством интерфейса mAPI по протоколу HTTPS/XML. Для входа в приложение клиенту необходимо авторизоваться (пройти аутентификацию). Аутентификацию можно считать завершенной, если в результате выполнения, какого либо шага аутентификации было получен успешный статус (например, код статуса 0), а также элемент логин мобильного приложения подтвержден. Приложение на мобильном устройстве должно поддерживать cookies. Cookies необходимы для хранения идентификатора сессии JSESSIONID, который в рамках одной сессии может неоднократно меняться.

В зависимости от операций, которые выполнены в автоматизированной системе банка на основе полученного от устройства 100 связи пользователя запроса, система 150 интернет-обслуживания физических лиц генерирует посредством блока 150.2 генерации уведомлений параметры и текст коротких и

полных push-уведомлений, а также текст резервных СМС, как показано в Приложении 3. Ответ может приходить в формате XML. В каждом ответе обязательно приходит статус ответа, по которому устройство пользователя может определить наличие ошибки в ответе. Для регулирования времени, через которое будет отправлена резервная СМС, используется тег, в значении которого передается время отправки резервной СМС в минутах. Для получения статуса отправки резервной СМС используется сервис, в котором для отображения статуса в данном вызове резервной СМС используется номер телефона, на которое отправлено сообщение, и статус резервной СМС.

В некоторых вариантах осуществления push-сообщения группируются по типам в соответствии с типом события, в связи с наступлением которого инициирована отправки сообщения.

В некоторых вариантах осуществления push-уведомления могут быть либо информационного характера (уведомление о выполнении авторизации в мобильном приложении, как аналог SMS-уведомления) либо запрашивать у клиента выполнение определенных действий (подтверждения операций, уточнение параметров операций).

В некоторых вариантах осуществления короткое push-уведомление имеет объем 2 Кб (в Unicod/UTF-8 - 1000 символов) или 4Кб (в Unicod/UTF-8 - 2000 символов). Короткое push-уведомление отправляется через push-сеть и может отображаться в виде системного сообщения (Alert), причем данное уведомление предназначено для отображения на мобильном устройстве в списке сообщений в виде заголовка. Короткие push-уведомления содержат текст, который должен быть отображен пользователю, служебные данные для операционной системы, а также уникальный идентификатор всего push-уведомления (с помощью идентификатора можно связать короткие и полные сообщения). При получении push-уведомления на мобильном устройстве может подаваться звуковой сигнал, меняться иконка приложения-получателя, может отображаться текст из уведомлений в окне с двумя кнопками. При нажатии первой кнопки окно уведомления закрывается, при нажатии другой кнопки выполняется запуск приложения, которому предназначено push-уведомление.

В некоторых вариантах осуществления полное push-уведомление выгружается в мобильное приложение, например, в формате XML. Выгрузка происходит по специальному запросу от мобильного приложения, причем для запроса используется идентификатор push-уведомления. Полное push-уведомление может содержать текст уведомления, служебные данные, вид приватности, идентификатор push-уведомления, максимальное время отправки, если не доставлено, а также дополнительные данные. Полные push-уведомления могут делиться по типам (назначению). У каждого типа определен вид приватности. Для просмотра секретной части данных сообщения с видом приватности "Закрытое" потребуется авторизация в мобильном приложении. Push-уведомления могут быть следующими типов: уведомление о входе в автоматизированную систему банка, оповещение службы помощи, уведомление о приёме на исполнение, одноразовый пароль для входа, одноразовый пароль для подтверждения операции, уведомление о сборе средств, уведомление о выставленном счёте, транзакционные уведомления, уведомления от мессенджера. Соответственно, если запрос, поступивший от устройства 100 связи пользователя, является запросом на авторизацию в автоматизированной системе банка, то блок 150.2 генерации уведомлений формирует уведомление о входе в автоматизированную систему банка при успешном прохождении пользователем этапов авторизации в автоматизированной системе банка. Аналогичным образом формируются и другие упомянутые выше типы уведомлений для соответствующих операций, которые могут быть выполнены в автоматизированной системе банка на основе полученного от устройства 100 связи пользователя запроса.

Параметры токена безопасности (Security Token) система 150 интернет-обслуживания физических лиц сохраняет в блоке хранения данных 150.4 в профиле пользователя, а также передает их посредством сетевого адаптера 150.1 через push-шлюз 140 на push-платформу 130. Взаимодействие между push-шлюзом и push-платформой осуществляется посредством протокола TCP/IP. Между push-шлюзом и push-платформой поддерживается TCP/IP сессия, в рамках которой происходит обмен данными в заранее заданном формате. Push-шлюз при этом взаимодействии с сетевой точки зрения является TCP сервером, а push-платформа является клиентом. То есть, push-шлюз подключается на выделенный TCP порт и принимает соединение от push-платформы.

Реализация описанного в данном техническом решении протокола взаимодействия между push-шлюзом и push-платформой предоставляет следующие возможности:

контроль состояния TCP сессии между push-шлюзом и push-платформой, причем контроль должен осуществляться как со стороны push-шлюза, так и со стороны push-платформы;

передача push-уведомлений и резервных SMS-уведомлений от push-шлюза push-платформе;

передача статусов доставки push-уведомлений от push-платформы на push-шлюз;

передача статусов доставки резервных SMS-уведомлений от push-платформы на push-шлюз;

передача информации для регистрации устройств-получателей push-уведомлений от push-шлюза на push-платформу;

передача информации для обновления данных об устройствах-получателях push-уведомлений от push-шлюза на push-платформу;

обновление информации об устройствах-получателях push-уведомлений на от push-платформы на

push-шлюз.

Если полученный запрос на совершение операции в автоматизированной системе банка с устройства 100 связи пользователя не содержит информации о параметрах токена безопасности (Security Token), система 150 интернет-обслуживания физических лиц посредством блока генерации уведомлений 150.2 генерирует резервное СМС, как показано на Приложении 5, которое направляется на устройство 100 связи пользователя. Данное сообщение информирует пользователя о том, что отправка push-уведомлений на устройство 100 связи пользователя невозможна. В некоторых вариантах осуществления резервное сообщение имеет уникального идентификатор, а также приоритет. Приоритет резервного СМС может принимать следующие возможные значения: LOW(1)- низкий; NORMAL(2) - нормальный; HIGH(3) - высокий; REALTIME(4) - максимальный.

В некоторых вариантах осуществления при обработке сообщений используется логика обработки вытесняющих приоритетов. Используется динамическое понижение приоритета при повторной отправке сообщения в случае, если предыдущая попытка отправки сообщения была неуспешна.

В дополнительных вариантах осуществления резервное СМС имеет статус, который может принимать следующие возможные значения:

ENQUEUED(1) - поставлено в очередь на отправку;

SENT(2) - отправлено message-уведомление;

DELIVERED(3) - пользователь скачал сообщение;

READ(4) - пользователь прочитал сообщение;

FAILED(5) - ошибка отправки.

Параметры токена безопасности для повышения надежности передачи данных кодируются перед отправкой. Push-платформа 130 декодирует параметры токена безопасности (Security Token) для получения push-адреса приложения 100.1 и определяет, зарегистрировано ли приложение 100.1 в блоке хранения данных 130.1.

Токен безопасности (Security Token) в декодированном виде может иметь следующий вид:

{"appPackage":"ru.sberbankmobile","IMSI":"250018524041548","screenResolutionY":"1776","locale":"ru_RU","memorySize":"1144","screenResolutionX":"1080","deviceUid":"290887d10c70003069087f4025564e63a7ad0000","userSecurityHash":"fscUTfRH0JtAOv27TJz3y18LGVM=","IMEI":"865800025607067","timeZoneUTCOffset":"10800000ms","appVersion":"2017092600","osName":"AndroidMSM8974","pushAddress":"cJeVXjBI3zo:APA91bGDQr6BU1H8aTQQQQG6fpSB58FH5mnCmcZn3VaN5jecpsTXzWCHNbSH5OqKCOzXwKQnM450fthTEnc1DdLALZ1lAILvQQQ9FZzKwne6X5mREZZ4zMbYQZ_jYTJUwHMIIEUbls","deviceSerialNumber":"4e1b955b","macAddress":"36:53:9A:2E:4B:F4","version":"1.0","osVersion":"6.0.1","deviceModel":"OnePlusA0001","providerUid":"PH47YU5vTjY6IkA+P1ZqYSQ4LiN+Pgo","routerMacAddress":"02:00:00:00:00:00","deviceName":"jenkinsinternal","generationTime":"2017.09.2711:22:54+0300","ipAddress":"fe80::fabc:169d:28:2e8%rmnet0"}.

Если приложение 100.1, соответствующее полученному push-адресу, не зарегистрировано в блоке 130.1 хранения данных, то push-платформа 130 создает профиль устройства для отправки push-уведомлений, в который включается информация о параметрах токена безопасности и push-адрес. Если приложение 100.1 уже зарегистрировано в блоке 130.1 хранения данных, то push-платформа 130 перезаписывает измененные параметры токена безопасности в соответствующем профиле устройства, чтобы обеспечить отправку push-уведомлений в соответствии с измененными параметрами.

Помимо параметров токена безопасности (Security Token) от системы 150 интернет-обслуживания физических лиц на push-платформу 130 также поступают сгенерированные параметры и текст короткого и полного push-уведомления и текст резервного СМС, которые необходимо отправить на устройство 100 связи пользователя в соответствии с выполненной операцией в автоматизированной системе банка и профилем устройства. Короткое push-уведомление push-платформа 130 передает на облачное хранилище 120 данных, которое определяет по меньшей мере одно устройство 100 связи пользователя для отправки push-уведомления и отправляет короткое push-уведомление на устройство 100 связи пользователя в соответствии с параметрами токена безопасности для отображения его текста пользователю, например, в баннерной зоне мобильного приложения.

Помимо текста короткое push-уведомление также содержит идентификатор push-платформы 130, например, URL и идентификатор push-уведомления. Таким образом, пользователь может запустить приложение 100.1 и на основе данных полученного коротко push-уведомления направить напрямую на соответствующую push-платформу 130 запрос на получение текста полного push-уведомления, соответствующего полученному короткому push-уведомлению. Дополнительно push-платформа 130 может быть выполнена с возможностью направить на устройство 100 связи пользователя через собственный интерфейс взаимодействия с СМС - шлюзом 160 резервное СМС, соответствующее тексту полного push-

уведомления в случае, если push-платформа 130 не получает запроса на скачивание текста полного push-уведомления в течении заданного интервала времени.

После получения полного push-уведомления приложение 100.1 направляет подтверждение получения контента на push-платформу 130, которая устанавливает статус прочтения отправленного push-уведомления, как показано в Приложении 4. История отправки и статусы push-уведомлений сохраняется в блок 130.1 хранения данных. Также статусы прочтения могут быть переданы по запросу в систему 150 интернет-обслуживания физических лиц для хранения в блоке 150.4 хранения данных.

Дополнительно облачное хранилище 120 данных может быть выполнено с возможностью проверки валидности push-адресов на устройствах 100 связи пользователя. С целью проверки валидности присвоенных push-адресов облачное хранилище 120 данных направляет на соответствующие устройства 100 связи пользователя соответствующие запросы и в случае, если от устройства 100 связи пользователя, которому присвоен push-адрес, не поступает соответствующего ответа на запрос по истечению заданного периода времени, данный push-адрес добавляется в список невалидных push-адресов. Список невалидных push-адресов передается в блок 130.1 хранения данных push-платформы 130 и по соответствующему запросу от системы 150 интернет-обслуживания физических лиц может быть передан в эту систему. Система 150 интернет-обслуживания физических лиц удаляет невалидные push-адреса из блока 150.4 хранения данных и направляет отчет об удалении на push-платформу 130 для удаления соответствующих адресов из блока хранения данных 130.1. Для того, чтобы уведомлять пользователя об операциях, совершенных вне автоматизированной системы банка, например, об изменении баланса карты, push-шлюз 140 дополнительно соединен с сервером 170 автоматизированной системы банка и выполнен с возможностью приема параметров и текста короткого и полного push-уведомления и текста резервного СМС, сгенерированных сервером 170 автоматизированной системы банка, а также с возможностью передачи полученной от сервера 170 автоматизированной системы банка информации на push-платформу 130. Полученные упомянутые параметры и текст от push-шлюза 140 обрабатываются push-платформой 130 аналогично описанному ранее способу. История о полученных push-шлюзом 140 уведомлениях сохраняется в блоке хранения данных 140.1. Взаимодействие системы 150 интернет-обслуживания физических лиц и push-шлюза 140 может осуществляется посредством web - сервиса, а в случае недоступности web - сервиса, может быть использована интеграция через Open Database Connectivity (ODBC).

Таким образом, за счет распределения функций обработки запросов от устройств 100 связи пользователя, генерации и доставки push-уведомлений между элементами системы 110 управления push-уведомлениями описанным выше способом, снижается вычислительная нагрузка на систему 150 интернет-обслуживания физических лиц. Дополнительно расширяется пропускная способность канала передачи данных между системой 150 интернет-обслуживания физических лиц и устройством 100 связи пользователя для обмена данными, а также между push-платформой 130, облачным хранилищем 120 данных и устройством связи 100 пользователя, вследствие чего повышается скорости доставки текста уведомлений от системы 150 интернет-обслуживания физических лиц к устройству 100 связи пользователя и снижается потеря данных, возникающая вследствие перегрузок канала передачи данных, т.е. повышается надежность обмена данными.

Приложения.

Приложение 1 (фиг. 2) - показан пример осуществления регистрации приложений на push-сервере.

Приложение 2 (фиг. 3) - показан пример осуществления отправки push-уведомлений в мобильное приложение.

Приложение 3 (фиг. 4) - показан пример осуществления доставки контента push-сообщений в мобильное приложение и получение статусов доставки.

Приложение 4 (фиг. 5) - показан пример осуществления резервирования доставки push-сообщений посредством СМС.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Система управления push-уведомлениями, содержащая

облачное хранилище данных, выполненное с возможностью:

определять по меньшей мере одно устройство связи пользователя для отправки push-уведомления;

отправлять короткое push-уведомление, полученное от push-платформы, по меньшей мере на одно устройство связи пользователя;

push-платформу, соединенную с облачным хранилищем данных, содержащую профиль по меньшей мере одного устройства связи пользователя, выполненную с возможностью отправки короткого и полного push-уведомления и резервных СМС, которые информируют пользователя о том, что отправка push-уведомлений на устройство пользователя невозможна, сгенерированных системой интернет-обслуживания физических лиц, в соответствии с запросом по меньшей мере одного устройства связи пользователя и параметрами токена безопасности (Security Token), в состав которого входит присвоенный облачным хранилищем данных устройству связи пользователя push-адрес;

push-шлюз для соединения push-платформы с системой интернет-обслуживания физических лиц;

система интернет-обслуживания физических лиц, выполненная с возможностью принимать по меньшей мере от одного устройства связи пользователя параметры токена безопасности (Security Token) и генерировать параметры и текст коротких и полных push-уведомлений и резервных СМС, которые информируют пользователя о том, что отправка push-уведомлений на устройство пользователя невозможна, в зависимости от операций, которые выполнены в автоматизированной системе банка на основе полученного запроса от устройства связи пользователя, для их отправки через push-шлюз на push-платформу в целях последующей передачи по меньшей мере на одно устройство связи пользователя;

при этом резервные СМС, информирующие пользователя о том, что отправка push-уведомлений на устройство пользователя невозможна, отправляются в случае, если полученный запрос на совершение операции в автоматизированной системе банка с устройством связи пользователя не содержит информации о параметрах токена безопасности.

2. Система по п.1, отличающаяся тем, что облачное хранилище данных дополнительно выполнено с возможностью

принимать запрос push-адреса по меньшей мере от одного устройства связи пользователя;

генерировать уникальный push-адрес по меньшей мере для одного устройства связи пользователя и направлять сгенерированный адрес в соответствии с принятым запросом;

проверять валидность push- адресов.

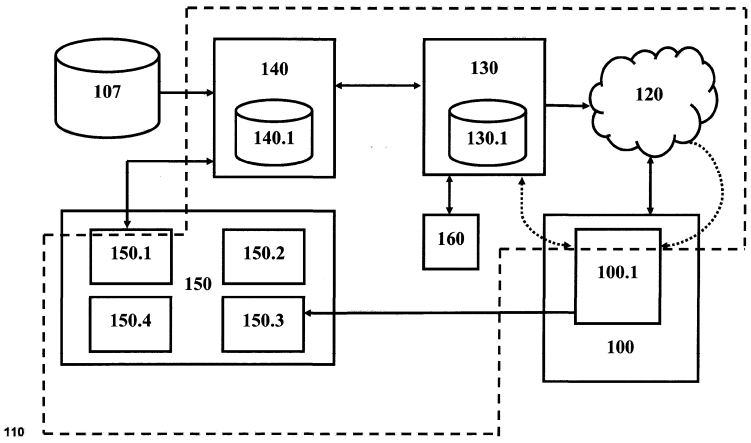
3. Способ управления push-уведомлениями, содержащий этапы, на которых

получают посредством системы интернет-обслуживания физических лиц от устройства связи пользователя запрос на совершение операций в автоматизированной системе банка, а также параметры токена безопасности (Security Token), в состав которого входит присвоенный облачным хранилищем данных устройству связи пользователя push-адрес;

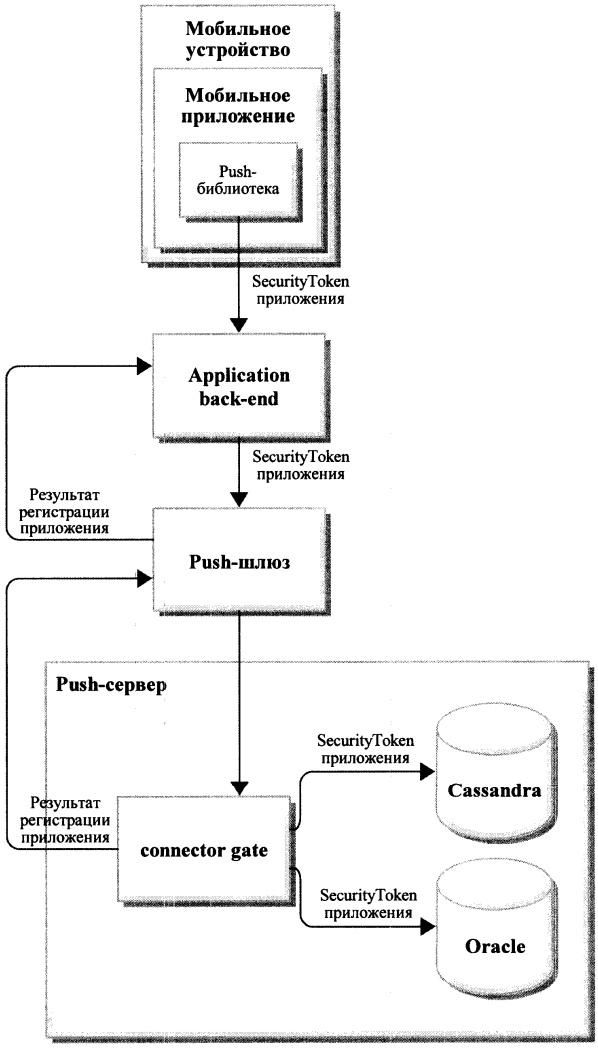
посредством системы интернет-обслуживания физических лиц генерируют параметры и текст коротких и полных push-уведомлений и резервных СМС, которые информируют пользователя о том, что отправка push-уведомлений на устройство пользователя невозможна, в зависимости от операций, которые выполнены в автоматизированной системе банка на основе полученного запроса от устройства связи пользователя;

передают сгенерированные системой интернет-обслуживания физических лиц параметры и текст коротких и полных push-уведомлений и резервных СМС посредством push-шлюза на push-платформу, соединенную с облачным хранилищем данных, содержащую профиль по меньшей мере одного устройства связи пользователя, при этом упомянутое облачное хранилище отправляет короткое push-уведомление, полученное от push-платформы, по меньшей мере на одно устройство связи пользователя;

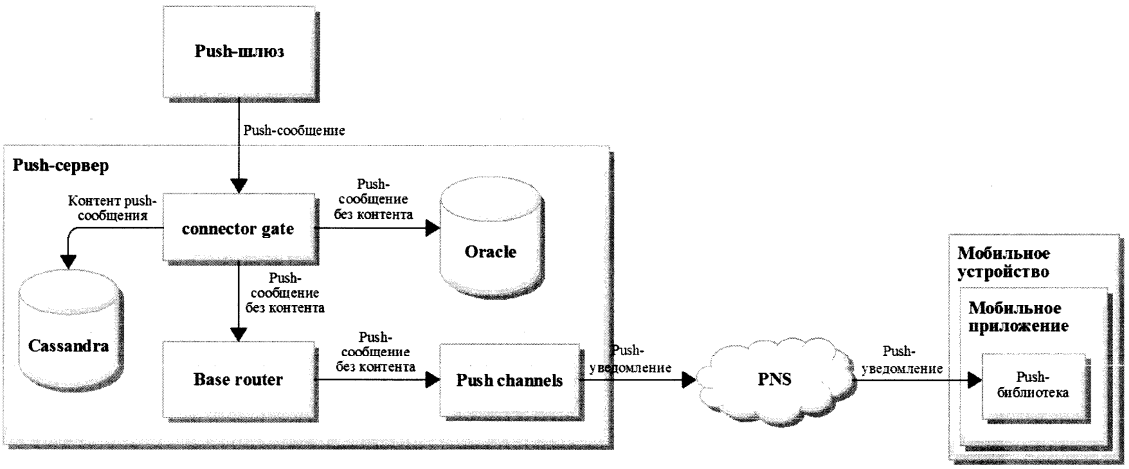
проверяют с помощью системы интернет-обслуживания физических лиц полученный запрос на содержание информации о параметрах токена безопасности (Security Token), и в случае, если полученный запрос на совершение операции в автоматизированной системе банка с устройством связи пользователя не содержит информации о параметрах токена безопасности, то на устройство пользователя посредством push-платформы направляется резервное СМС, информирующие пользователя о том, что отправка push-уведомлений на устройство пользователя невозможна.



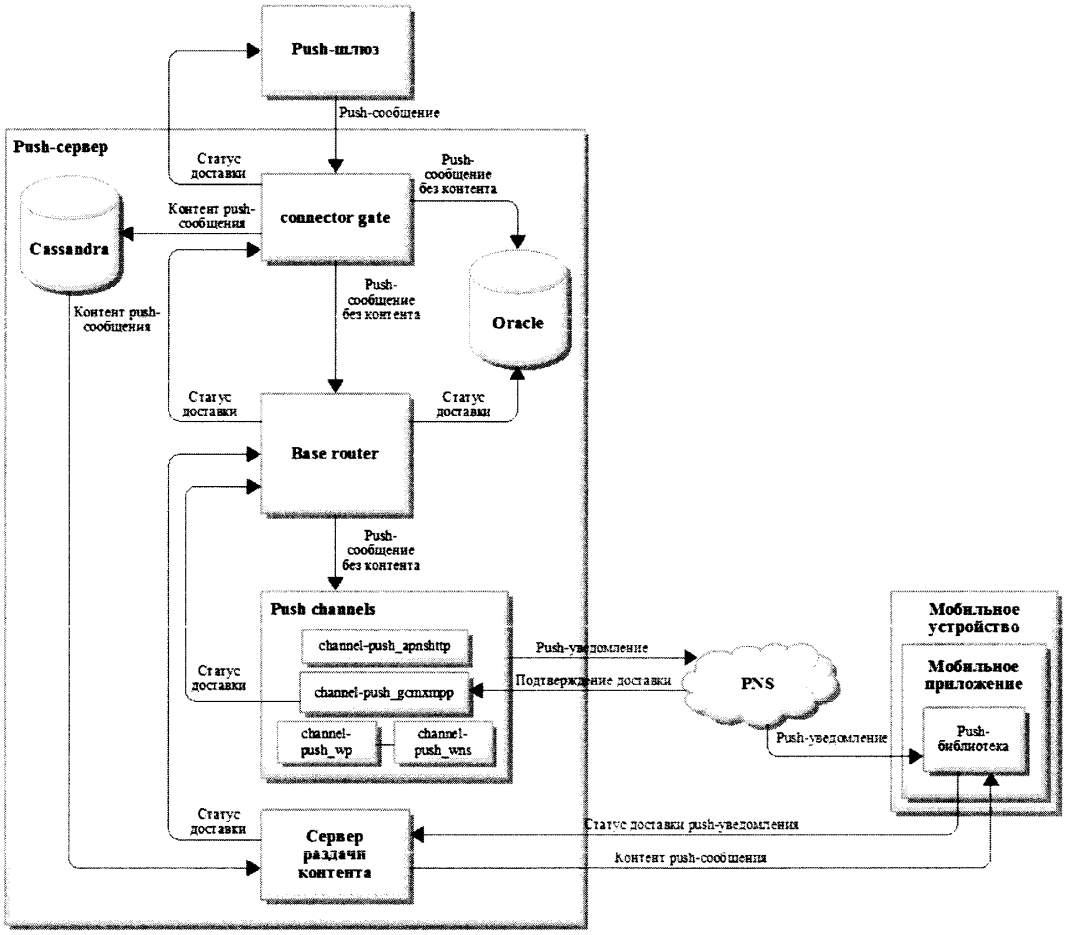
Фиг. 1


Мобильное устройство
Мобильное приложение
Push-библиотека
SecurityToken приложения
Application back-end
SecurityToken приложения
Результат регистрации приложения
Push-шлюз
Push-сервер
SecurityToken приложения
Cassandra
Результат регистрации приложения
connector gate
SecurityToken приложения
Oracle

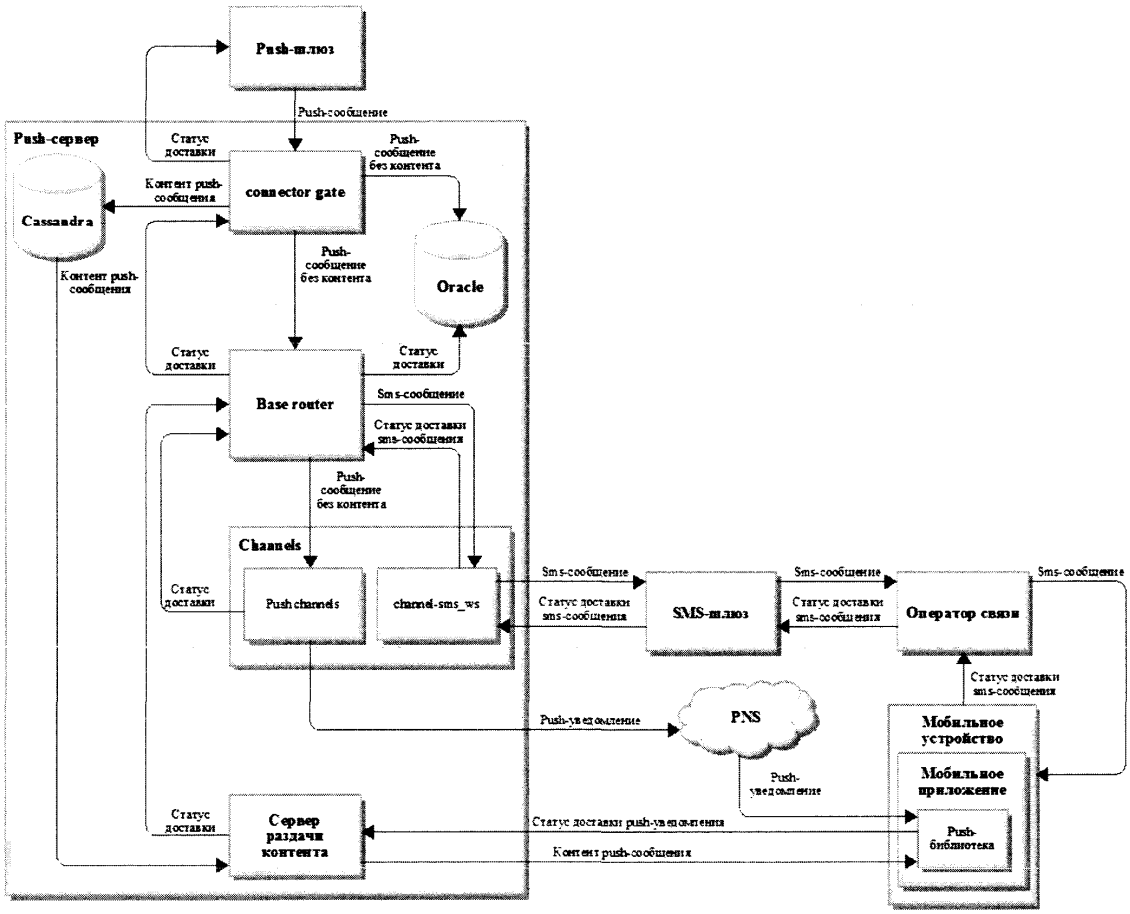
Фиг. 2


Push-шлюз
Push-сообщение
Push-сервер
Контент push-сообщения
connector gate
Push-сообщение без контента
Oracle
Cassandra
Push-сообщение без контента
Base router
Push-сообщение без контента
Push channels
Push-уведомление
PNS
Push-уведомление
Мобильное устройство
Мобильное приложение
Push-библиотека

Фиг. 3


Push-шлюз
Push-сообщение
Push-сервер
Статус доставки
Push-сообщение без контента
Контент push-сообщения
connector gate
Cassandra
Oracle
Push-сообщение без контента
Контент push-сообщения
Статус доставки
Статус доставки
Base router
Push-сообщение без контента
Push channels
channel-push_apnshttp
channel-push_gcmxmpp
channel-push_wp
channel-push_wns
Push-уведомление
Подтверждение доставки
PNS
Push-уведомление
Мобильное устройство
Мобильное приложение
Push-библиотека
Статус доставки
Статус доставки push-уведомления
Сервер раздачи контента
Контент push-сообщения

Фиг. 4


Push-шлюз
Push-сообщение
Push-сервер
Статус доставки
Push-сообщение без контента
Контент push-сообщения
connector gate
Cassandra
Oracle
Push-сообщение без контента
Контент push-сообщения
Статус доставки
Статус доставки
Base router
Sms-сообщение
Статус доставки sms-сообщения
Push-сообщение без контента
Channels
Статус доставки
Push channels
channel-sms_ws
Sms-сообщение
Статус доставки sms-сообщения
SMS-шлюз
Sms-сообщение
Статус доставки sms-сообщения
Оператор связи
Sms-сообщение
Статус доставки sms-сообщения
Push-уведомление
PNS
Мобильное устройство
Мобильное приложение
Push-библиотека
Push-уведомление
Статус доставки
Сервер раздачи контента
Статус доставки push-уведомления
Контент push-сообщения

Фиг. 5