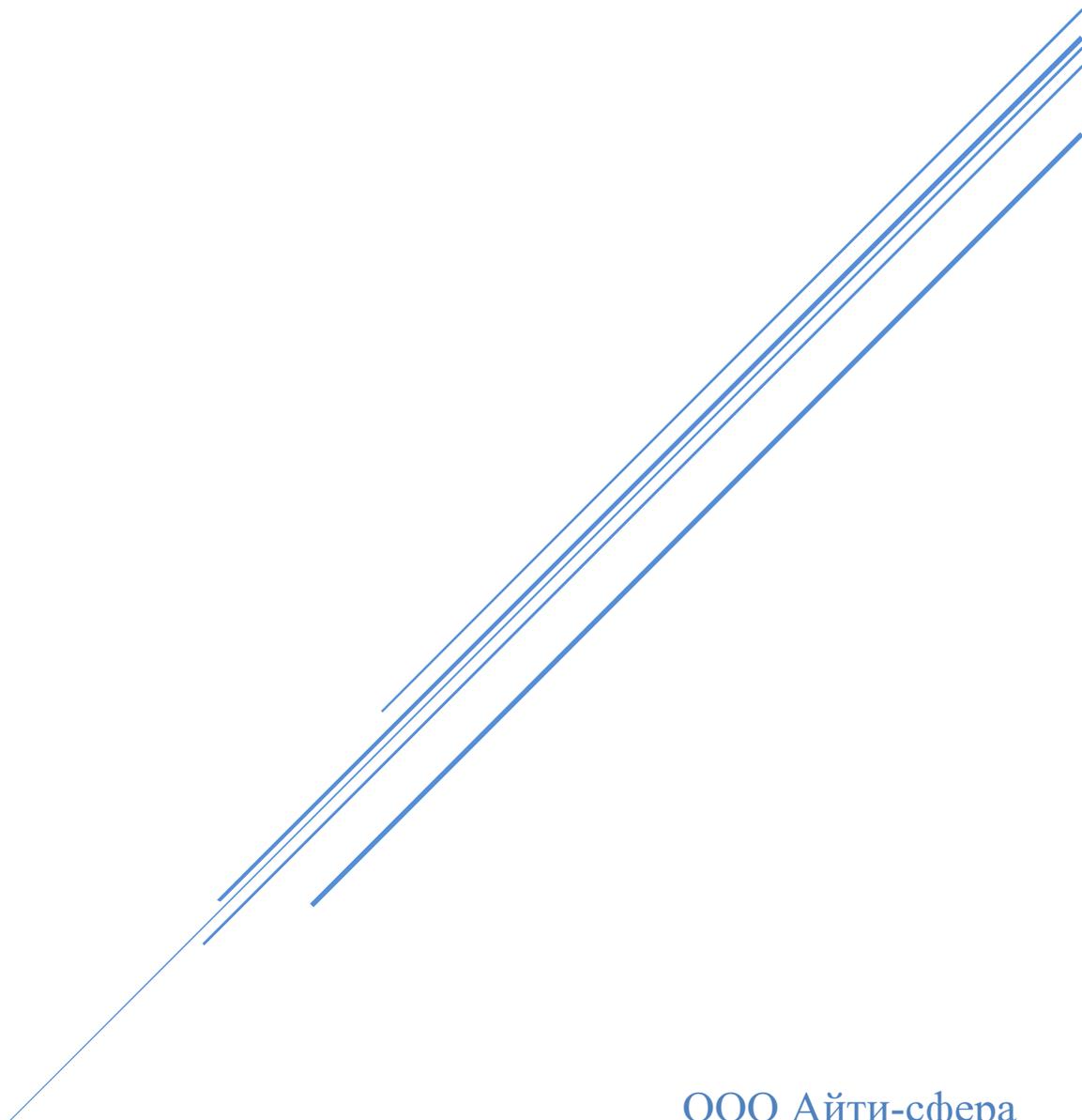

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Сервис для токенизации и хранения банковских карт



ООО Айти-сфера
Москва, 2023 г.

Оглавление

1. Введение	2
1.1 Наименование ПО.....	2
1.2 Область применения	2
1.3 Определения.....	2
1.4 Уровень подготовки пользователей.....	4
1.5 Перечень программной документации.....	4
2. Назначение и требования для эксплуатации ПО.....	4
2.1 Функциональные характеристики	4
2.2 Организация входных и выходных данных.....	5
2.3 Эксплуатационное назначение.....	5
2.4 Требования к эксплуатации серверной части.....	6
3. Подготовка к работе.....	6
3.1 Формат запросов.....	6
3.1.1 HTTP-заголовки	6
3.1.2 X-Data-Hash.....	6
4. Описание операций	7
4.1 card.save	7
4.1.1 Основные параметры	7
4.1.2 Формат запроса (пример).....	8
4.1.3 Формат ответа (пример)	8
4.2 card.get.....	8
4.2.1 Основные параметры	8
4.2.2 Формат запроса (пример).....	9
4.2.3 Формат ответа (пример)	9
5. Аварийные ситуации.....	9
6. Рекомендации по освоению	10

1. Введение

1.1 Наименование ПО

Наименование программного обеспечения “Сервис для токенизации и хранения банковских карт”.

1.2 Область применения

Настоящий документ (далее – Описание) распространяется на программное обеспечение (далее – ПО) “Сервис для токенизации и хранения банковских карт”. “Сервис для токенизации и хранения банковских карт” представляет собой техническое решение, позволяющее скрыть конфиденциальные данные банковской карты на уникальный идентификатор, называемый токеном карты. Скрытию подлежат такие данные, как:

- Номер карты;
- Срок действия;
- Держатель карты и так далее.

1.3 Определения

ПО	Программное обеспечение – совокупность компьютерных программ и связанных с ними данных, которая содержит инструкции по указанию компьютеру, что и как делать.
Конфиденциальные данные	Информация, доступ к которой ограничен в соответствии с законами государства и нормами, которые компании устанавливаются самостоятельно.
Банковская карта	Пластиковая, металлическая или виртуальная карта, обычно привязанная к одному или нескольким расчётным счетам в банке. Используется для оплаты товаров и услуг, в том числе через интернет, с использованием бесконтактной технологии, совершения переводов, а также снятия наличных.
Держатель карты	Физическое лицо, на имя которого выпущена пластиковая или виртуальная карта, в том числе, физическое лицо-владелец счёта либо другое лицо,

	указанное владельцем счета. Сама карта при этом является собственностью банка.
Номер карты	Комбинация из 13, 16, 18 или 19 цифр, размещенных на лицевой или оборотной стороне пластика (или виртуальной карты). Набор цифр уникален, он не повторяется и привязан к кредитной организации, держателю пластика и счету. В комбинации зашифрована информация о банке, который выдал карту, и платежной системе, обслуживающей пластик.
API	Программный интерфейс приложения — это набор способов и правил, по которым различные программы общаются между собой и обмениваются данными.
Очередь	Совокупность объектов, которые поддерживаются в последовательности и могут быть изменены путем добавления объектов на одном конце последовательности и удаления объектов с другого конца последовательности. Операции очереди делают ее структурой данных, которая обеспечивает хранение и передачу двоичных данных между различными участниками системы.
Инстанс	Дубликат объекта, сохраняющий неразрывную связь с оригиналом и полную зависимость от него. Модификация любого образца равносильна модификации оригинала - результаты сказываются как на оригинале объекта, так и на всех образцах.
Мерчант	Партнер, пользователь ПО, имеющий специальный счёт, который позволяет торговой компании принимать платежи с помощью банковских карт.
Сервис	Независимо компилируемый программный модуль, динамически подключаемый к основной программе и предназначенный для расширения и/или использования её возможностей. Сервисы обычно выполняются в виде библиотек общего пользования.
Токенизация карты	Обмен конфиденциальных данных банковской карты на специальный токен, который позволяет использовать банковскую карту без ввода личных данных банковской карты.

1.4 Уровень подготовки пользователей

Для интеграции API пользователь должен иметь квалификацию разработчика не ниже уровня Regular Middle.

1.5 Перечень программной документации

- “Сервис для токенизации и хранения банковских карт”. Техническое задание (ГОСТ 19.201-78);
- “Сервис для токенизации и хранения банковских карт”. Руководство пользователя;
- “Сервис для токенизации и хранения банковских карт”. Описание функциональных характеристик программного обеспечения;
- “Сервис для токенизации и хранения банковских карт”. Описание жизненного цикла разработки ПО;
- “Сервис для токенизации и хранения банковских карт”. Инструкция по развертыванию экземпляра ПО;
- “Сервис для токенизации и хранения банковских карт”. Инструкция для проверки в тестовой среде ПО.

2. Назначение и требования для эксплуатации ПО

Программное обеспечение “Сервис для токенизации и хранения банковских карт” предназначено для использования на стороне мерчанта.

2.1 Функциональные характеристики

- 1) Токенизация банковской карты;
- 2) Безопасное хранение данных банковских карт;
- 3) Передача данных в формате запросов в Базу данных и получение этих данных;
- 4) Масштабирование благодаря наличию ресурсов для запуска нескольких экземпляров сервиса;

- 5) Штатный функционал, который в свою очередь позволяет подписывать несколько инстансов в одну очередь, сообщения из которой случайным образом приходят в один из инстансов.

2.2 Организация входных и выходных данных

- 1) Сервис подписывает инстансы в одну очередь, сообщения из которой случайным образом приходят в один из инстансов;
- 2) “Сервис для токенизации и хранения банковских карт” валидирует входящие данные;
- 3) ПО передает полученные данные в формате запросов в БД;
- 4) “Сервис для токенизации и хранения банковских карт” получает ответ от БД на основе переданных данных;
- 5) Сервис осуществляет передачу полученных данных из БД в соответствующий внешний сервис;
- 6) Реализована возможность получения ответа от внешнего сервиса;
- 7) ПО модифицирует полученные данные от внешнего сервиса;
- 8) Сервис передает данные в общем формате мерчанту.

2.3 Эксплуатационное назначение

ПО интегрируется и эксплуатируется на стороне Заказчика. При использовании сервис предоставляет такие преимущества, как:

- Надежность очередей достигается благодаря возможности накапливать сообщения, амортизируя недостаток вычислительных возможностей системы, а также благодаря независимости компонентов;
- Независимость компонентов системы друг от друга;
- Экономия ресурсов благодаря возможности грамотного распределения информации, поступающей в очередь от одних процессов, между другими процессами, осуществляющими ее обработку.

2.4 Требования к эксплуатации серверной части

Обеспечение функционирования ПО серверной части “Сервис для токенизации и хранения банковских карт” реализовано на базе серверной операционной системы Linux. Минимальной конфигурацией аппаратной составляющей являются:

- ✓ Современная ОС: Linux;
- ✓ Оперативная память: 2 Гб;
- ✓ Свободное дисковое пространство: не менее 20 Gb;
- ✓ Количество логических ядер процессора: 2;
- ✓ Частота процессора: 3.50 GHz.

Возможно разворачивание экземпляра ПО и на других ОС, поддерживающих платформу для автоматизации развёртывания и управления приложениями в средах с поддержкой контейнеризации Docker, например Windows 10 (Профессиональная или Корпоративная).

3. Подготовка к работе

3.1 Формат запросов

Оповещения передаются на **POST** запросов на **url**, предоставляемый при подключении платформы. Важно проверить **X-Data-Hash** запроса.

3.1.1 HTTP-заголовки

Обязательные к передаче заголовки **HTTP** запроса:

```
Content-Type: application/json
X-Data-Hash
X-DATA-APPLICATION-ID
```

3.1.2 X-Data-Hash

Используется для подтверждения легитимности и подлинности запроса. Передается в **HTTP** заголовке **X-Data-Hash**.

```
X-Data-Hash = sha512(%request_body% + %secret_key%)
```

- `request_body` - объект запроса, сериализованный в виде JSON строки (берем исходную строку).
- `secret_key` - секретный ключ, выдаваемый при подключении приложения.

На выходе получаем ЭЦП к запросу.

Проверка производится следующим образом:

```
isValidRequest = X-Data-Hash == sha512(%request_body% + %secret_key%)
```

- `isValidRequest == true` - запрос легитимный;
- `isValidRequest == false` - запрос следует проигнорировать.

4. Описание операций

4.1 *card.save*

Данный метод необходим для безопасного сохранения данных банковских карт (`pan`, `card holder`, `expire`).

4.1.1 Основные параметры

Параметр	Тип	Обязательность	Описание
<code>method</code>	<code>string</code>	+	Для этого метода <code>card.save</code>
<code>params.client</code>	<code>string</code>	+	Идентификатор клиентского приложения.
<code>params.card.number</code>	<code>string</code>	+	Номер карты
<code>params.card.expire</code>	<code>string</code>	-	Срок действия карты (в формате ММ/YY)
<code>params.card.holder</code>	<code>string</code>	-	Владелец карты

4.1.2 Формат запроса (пример)

```
{
  "method": "card.save",
  "params": {
    "client": "test",
    "card": {
      "number": "1111222233334444",
      "expire": "10/23",
      "holder": "TEST HOLDER"
    }
  }
}
```

4.1.3 Формат ответа (пример)

```
{
  "success": true,
  "result": {
    "card": {
      "id": "043bd6b5-5336-4c98-84ef-61e01cf4d8a0",
      "mask": "111122*****4444"
    }
  }
}
```

4.2 *card.get*

Данный метод необходим для получения данных карты по токену

4.2.1 Основные параметры

Параметр	Тип	Обязательность	Описание
method	string	+	Для этого метода card.get

params.client	string	+	Идентификатор клиентского приложения.
params.card.id	string	+	uuid сохраненной карты полученный в результате метода card.save

4.2.2 Формат запроса (пример)

```
{
  "method": "card.get",
  "params": {
    "client": "test",
    "card": {
      "id": "043bd6b5-5336-4c98-84ef-61e01cf4d8a0"
    }
  }
}
```

4.2.3 Формат ответа (пример)

```
{
  "success": true,
  "result": {
    "card": {
      "id": "043bd6b5-5336-4c98-84ef-61e01cf4d8a0",
      "mask": "422272*****4301",
      "number":
"Jxc2s7w72fOC6i+HljzYrDkxODUxNTI1NmY1MDkzNDczMjNhZTkyNDNkYjBjZGUxM2Y2MmE5YzQ5
OTU4M2FmN2YxMWI4Y2FiMWNiMzUyNjg=",
      "expire":
"Q0zMDi1UCmkZSwq2Nu8Mzzc0NjQyZjY4NzkwOGQ5ODBhZDA3ZDZjMDM5MzVjOGIy",
      "holder": "YOpO4hmJoUFoYtvpqyqOWfTE0ZjMxYTIIN2U2NzllODZhOWRiZTlmNTNkOwM5ZmRh"
    }
  }
}
```

5. Аварийные ситуации

В случае аварийных ситуаций обращаться в техническую поддержку.

6. Рекомендации по освоению

Для успешной работы с ПО “Сервис для токенизации и хранения банковских карт” необходимо:

- ✓ Иметь квалификацию разработчика не ниже уровня Regular Middle;
- ✓ Иметь оборудованное рабочее место с подключением к сети Интернет;
- ✓ Рабочее место должно соответствовать минимальным требованиям, указанным в разделе “2.4 Требования к эксплуатации серверной части” данного документа;
- ✓ Ознакомиться с документом “Руководство пользователя “Сервис для токенизации и хранения банковских карт””;
- ✓ Ознакомиться с документом “Разворачивание экземпляра ПО “Сервис для токенизации и хранения банковских карт””.