PROTECTIMUS

Technical Overview

Версия 1.0.2 RU
от 10 июля 2014

Содержание

Обзор решения

Аутентификация на основании только лишь одного фактора - паролей не может считаться достаточно надежной для систем с высокими требованиями к безопасности. Использование сразу нескольких факторов в системе аутентификации значительно повышает уровень защищенности системы от несанкционированного доступа.

Множество компаний предлагают свои решения для внедрения многофакторной аутентификации, но их проблема в том, что они являются бюрократическими монстрами со всеми вытекающими последствиями: плохая коммуникация и низкий уровень обслуживания; громоздкий, неудобный и неповоротливый продукт; отсутствие актуальной информации и невозможность ее получить так быстро, как бы этого хотелось. Вдобавок к этому они являются монополистами, выставляют огромные счета после этапа согласования с каждым клиентом, не выставляя свои цены публично.

Цель Protectimus - предложить лучшее решение в области двухфакторной аутентификации с точки зрения цены и простоты использования при обеспечении высокого уровня качества и надежности системы.

Разработанный продукт позволит:

1. **Клиентам** строить на его базе более безопасные сервисы просто и доступно вне зависимости от размеров компании.
2. **Пользователям клиентов** надежно защитить свои аккаунты от несанкционированного доступа

Protectimus предлагает комплексное решение, которое включает в себя как систему аутентификации, так и широкий выбор программных и аппаратных токенов.

Система аутентификации может функционировать как отдельное приложение, устанавливаемое на серверах клиента, так и в режиме облачного сервиса, предоставляя SaaS-решение. Protectimus уже позаботился об устойчивой и безотказной работе своей системы.

Protectimus решает проблему двухфакторной аутентификации на всех уровнях. Каждый клиент сможет найти для себя решение, которое максимально удовлетворит его потребностям.

Характеристики системы

Платформа Protectimus поддерживает работу в широком спектре ОС (от Linux, FreeBSD до любой версии Windows).

Система поддерживает текущие и предыдущие версии популярных браузеров:
Google Chrome, Mozilla Firefox, Internet Explorer.

Все компоненты системы поддерживают существующие стандарты разработки программного обеспечения, а также стандарты OATH в области OTP-аутентификации, благодаря чему в Protectimus возможно использовать токены сторонних производителей или конкурентов.

Protectimus обеспечивает функционирование нескольких не связанных между собой копий приложения в разных географических зонах вблизи пользователей клиента. Также предусмотрена возможность работы нескольких нод для одного крупного клиента, пользователи которого расположены в разных уголках нашей планеты.

Алгоритмы, используемые для генерации одноразовых паролей

Для получения одноразового пароля используются следующие алгоритмы:

- HMAC - hash-based message authentication code: RFC2104
- HOTP - hash-based one-time password: RFC4226
- TOTP - time-based one-time password: RFC6238
- OCRA - OATH Challenge-Response Algorithms: RFC6287

Они разработаны инициативной группой Initiative For Open Authentication (OATH), направленной на стандартизацию методов аутентификации. Де-факто, эти алгоритмы хорошо себя зарекомендовали и стали стандартом в области двухфакторной аутентификации.

Стек технологий

#	Tools	Name (Version)
1	Java	7
2	Web/App Server	Tomcat 7.0
3	Framework	Spring 3.1.0, Apache Tapestry 5.3.7
4	GUI	Twitter Bootstrap, JQuery
5	ORM	Spring JDBC
6	Database	Postgres SQL 9.3
7	Building	Maven 3
8	High-performance, distributed memory object caching system	Memcached
9	Application Load Balancing and Content Caching	Nginx

Атрибуты качества программного обеспечения

В процессе разработки ПО использованы:

- Стандартные механизмы и библиотеки
- Java Programming Style Guidelines (Java™ Coding Style Guide)
- Принципы DRY (Don't Repeat Yourself) and DIE (Duplication Is Evel).
- Разработка через тестирование (TDD)

Архитектура решения

Protectimus построен по лучшим канонам SOA, MVC, RESTful и другим духовным практикам. Рассмотрим общую архитектуру решения, которая представлена на рисунке1.

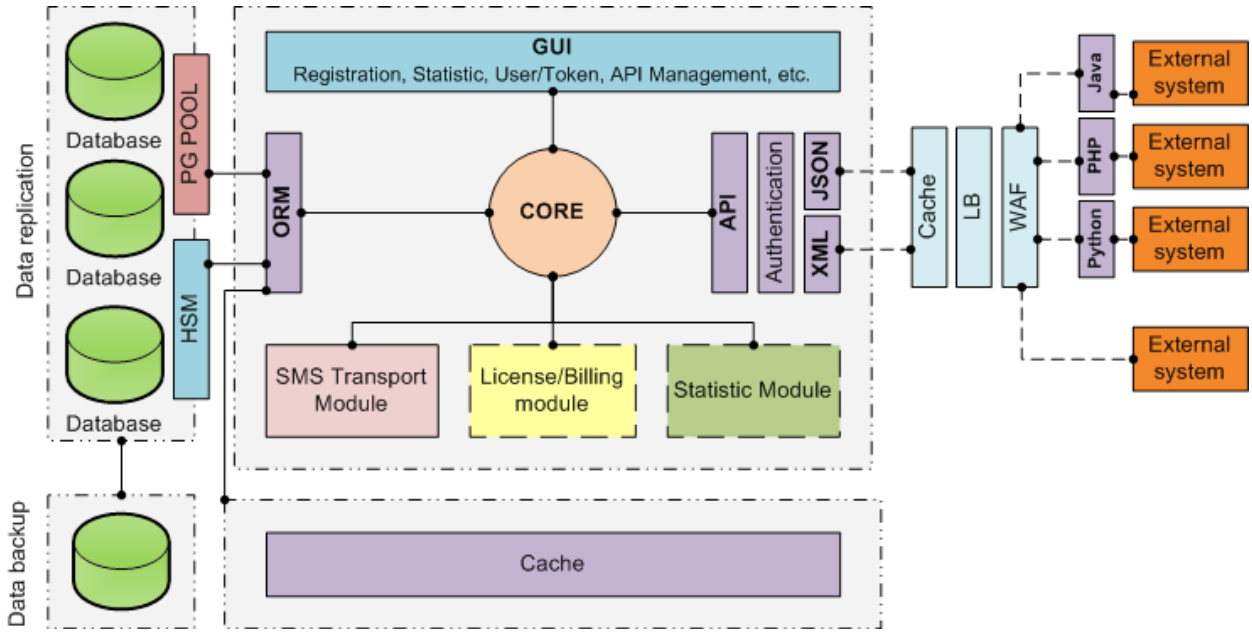


Рисунок 1. Общая архитектура решения

Для обеспечения надежной и бесперебойной работы система развернута в кластере высокопроизводительных серверов. Распределением нагрузки между ними занимается аппаратный Load Balancer. Система мониторинга постоянно отслеживает состояние инфраструктуры и уведомляет администраторов Protectimus о возможных угрозах и критических ситуациях.

Hardware Security Module обеспечивает надежное хранение криптографической информации.

Ценность данных в нашей системе сложно переоценить. Мы обязаны предотвратить потерю данных, а также предусмотреть механизм восстановления данных в случае сбоев или при возникновении форс-мажорных ситуаций. Именно поэтому используется резервное копирование (бэкапы) и репликация данных.

Protectimus «держит» 10 бэкапов: по одному на каждый день недели, а также бэкапы двухнедельной, месячной и квартальной давности, что позволяет достаточно глубоко «откатиться» в случае утраты каких-либо данных. Хранятся бэкапы на отдельных серверах.

Общая проблема с любыми бэкапами в том, что они всегда отстают. В случае фатального сбоя основного сервера восстановить систему можно будет только с некоторым «откатом» по времени, для устранения этой проблемы предназначена система репликации — тиражирование изменений

данных с главного сервера БД на одном или нескольких зависимых серверах. Главный сервер называется мастером, а зависимые — репликами.
Изменения данных, происходящие на мастере, повторяются на репликах (но не наоборот). Поэтому запросы на изменение данных (INSERT, UPDATE, DELETE и т. д.) выполняются только на мастере, а запросы на чтение данных могут выполняться как на репликах, так и на мастере.
Репликация производится при помощи бинарных логов, ведущихся на мастере. В них сохраняются все запросы, приводящие к изменениям в БД. Эти логи передаются на реплики и сохраненные запросы выполняются, начиная с определенной позиции. При репликации передаются не сами измененные данные, а только запросы, вызывающие изменения.
Таким образом, использование резервного копирования и репликация данных обеспечивают повышенную устойчивость системы и сохранность данных.

Для повышения производительности используется оптимизация на различных уровнях:

- на стороне клиента: кэширование на уровне браузера, минимизация ресурсов (HTML, CSS, and JavaScript), оптимизация изображений, CSS-спрайты и др.;
- на стороне сервера: кеширование (Memcached), оптимизация обработки статического контента (Nginx), оптимизация настроек сервера приложений, балансировка нагрузки и др.;
- на стороне базы данных: оптимизация настроек базы, использование индексов, партиционирование.

Управление системой осуществляется через графический интерфейс пользователя, созданный на базе Twitter Bootstrap, что обеспечивает адекватное отображение контента в различных браузерах и на различных устройствах.

Взаимодействие между Protectimus и системами клиентов осуществляется посредством RESTful API, данные передаются в формате XML или JSON. Для облегчения процессов интеграции разработаны библиотеки на Java, Python, PHP. Документация по API доступна на сайте Protectimus в разделе “Материалы”.

Сертифицированный модуль аутентификации позволяет использовать в Protectimus любые токены, работающие по стандартным алгоритмам OATH: HOTP, TOTP, OCRA. А модуль доставки SMS обеспечит одноразовыми паролями тех, кто не желает или не может использовать другие виды токенов.

Интеграция с Protectimus

Для интеграции Protectimus в свой проект Вы можете воспользоваться двумя путями:

1. Интеграция через API. Для интеграции через API мы предоставляем набор вспомогательных библиотек для следующих языков программирования: Java, Python и PHP. Если же для Вашего языка программирования клиент еще не предложен, Вы можете использовать полное описание всех методов API, доступное по данной ссылке.
2. Использование IFrame-виджета для аутентификации пользователей.

Аутентификация пользователя всегда проводится для определенного ресурса, следовательно пользователь должен быть назначен на ресурс, к которому он должен иметь доступ. Если пользователь не назначен на ресурс, то пользователь не имеет к нему доступа. Способ назначения пользователя на ресурс зависит от выбранного способа аутентификации. Protectimus поддерживает несколько способов аутентифицировать пользователя:

1. **Аутентификация пользователя по статическому паролю.** Для работы этого метода у пользователя должен быть задан пароль и пользователь должен быть назначен на ресурс, для которого выполняется проверка.

Обратите внимание: Protectimus принимает все меры по обеспечению безопасного хранения паролей Ваших пользователей и никогда не будет использовать их в целях, отличных от их прямого предназначения. Больше информации по данному вопросы Вы найдете на странице PRIVACY POLICY. Информацию о том, как безопасно передать и использовать пароли Ваших пользователей в Protectimus смотрите в документации к нашему API.

2. **Аутентификация пользователя по одноразовому паролю.** Для этого у пользователя должен быть токен и пользователь должен быть назначен на ресурс ВМЕСТЕ с токеном. Назначение на ресурс отдельно пользователя и отдельно токена будет неправильным для работы этого метода.
3. **Аутентификация пользователя по статическому и одноразовому паролю.** Является комбинацией двух вышеописанных методов. Пользователь должен быть назначен на ресурс ВМЕСТЕ с токеном. У пользователя должен быть задан пароль. Если токен пользователя будет отключен, то проверка OTP выполняться не будет, в таком случае будет проверен только статический пароль и проходит ли пользователь фильтры, если они существуют.
4. **Аутентификация токена на ресурсе.** Этот способ позволяет не привязывать токен к какому-то конкретному пользователю и просто проверять валидность сгенерированного одноразового пароля. При использовании этого способа токен должен быть назначен на ресурс.

Обратите внимание: При аутентификации, кроме прочего, выполняется проверка: удовлетворяет ли запрос требованиям фильтров, установленных на данном ресурсе.

Токены, используемые в Protectimus

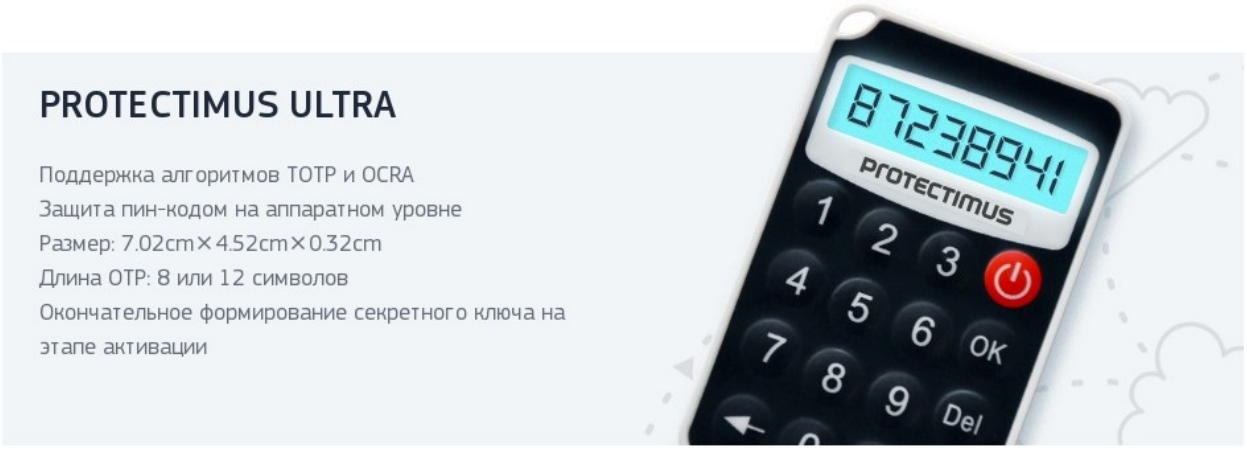
Для получения одноразового пароля Вы можете использовать разные виды токенов.

Физические токены

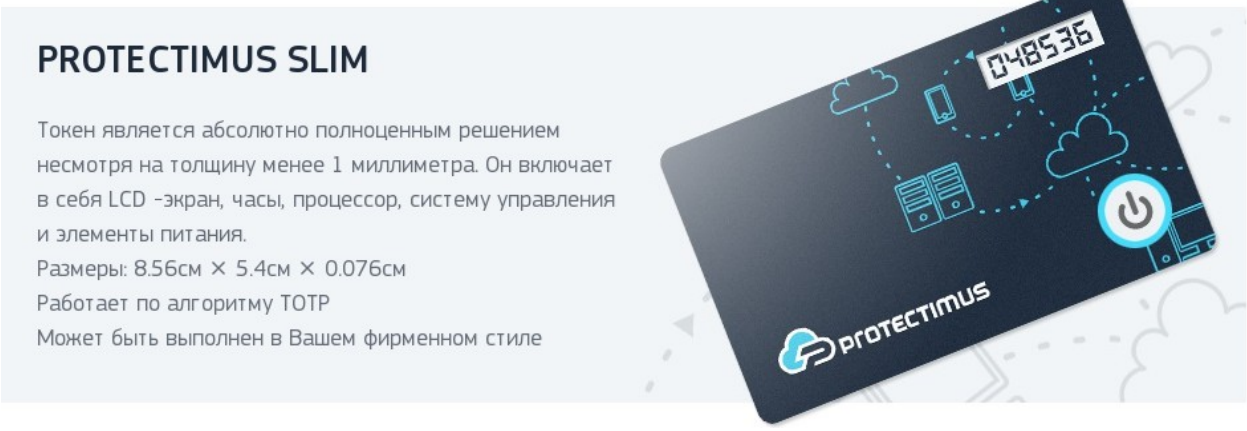
Физические токены - устройства специально предназначены для генерации OTP. Имеют небольшой размер, могут быть использованы в качестве брелока. К ним относятся следующие модели токенов: Protectimus ONE, Protectimus ULTRA, Protectimus SLIM. Рассмотрим эти токены ближе.

Токены Protectimus ONE являются базовым решением, подходящим большинству пользователей, которым нужны физические токены.

Для обеспечения наибольшей защиты стоит использовать токены Protectimus ULTRA, они работают по алгоритму OCRA - сервер показывает число-вопрос, пользователь вводит его в токен и на основании этого токен генерирует ответный OTP. Особенность данного токена в том, что секретный ключ окончательно формируется в процессе активации токена пользователем или сотрудником клиента.



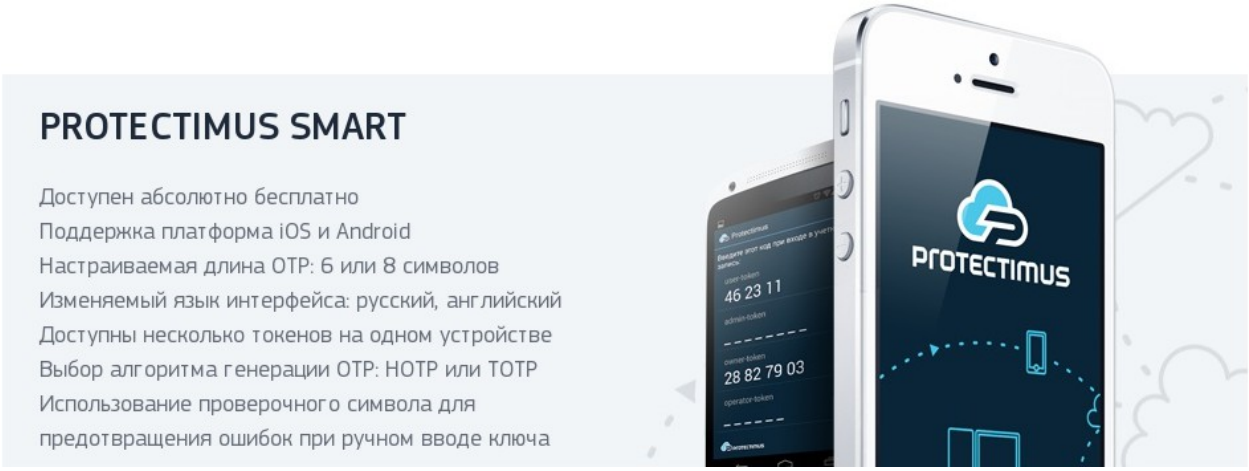
Токен SLIM имеет размеры обычной банковской карты, в том числе и толщину. За счет этого его использование становится более удобным, а сам токен может быть выполнен в Вашем фирменном стиле.



Программные токены

Protectimus SMART - приложение от Protectimus для генерации OTP, может быть установлено на Android и iOS. Приложение не имеет связи с сервером, что исключает возможность влиять на систему аутентификации путем перехвата канала связи.

Protectimus SMART позволяет клиентам экономить на внедрении двухфакторной аутентификации, а пользователям - облегчить ее использование. В приложении можно создавать несколько токенов, что позволит работать с разными независимыми системами двухфакторной аутентификации с использованием одного устройства.

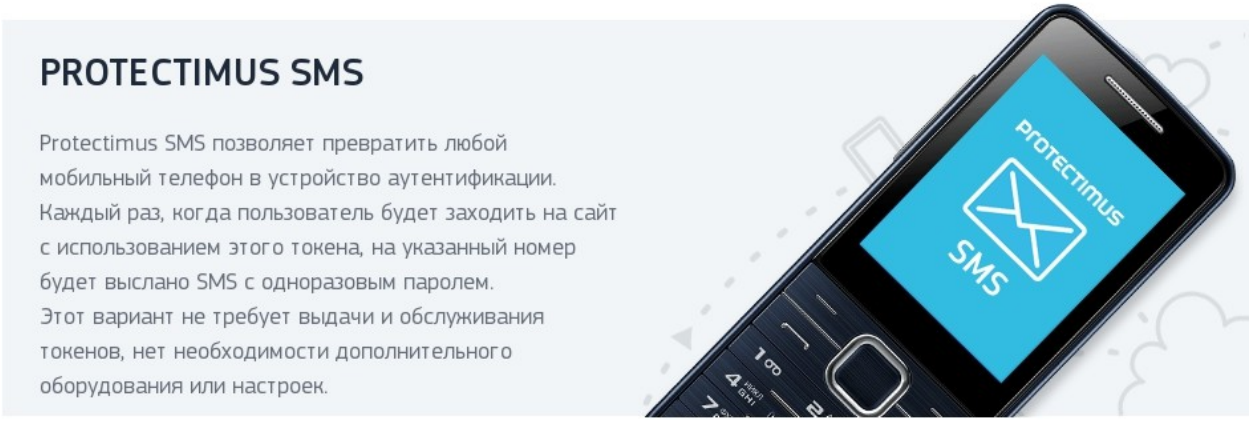


SMS и e-mail токены

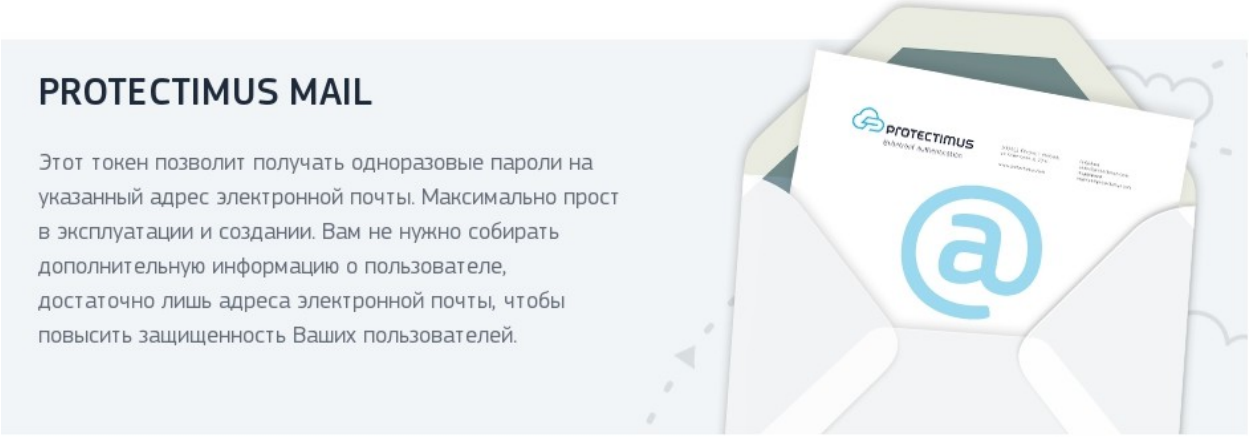
Одноразовые пароли будут приходить на указанный номер телефона или адрес электронной почты. Использование таких токенов максимально упрощает взаимодействие с пользователями, им не нужно выполнять никаких дополнительных действий и они могут быть расположены в любых уголках солнечной системы.

Пользователи уже давно знакомы с практикой подтверждения своей личности с помощью кодов, которые приходят на телефон, а это значит, что Вам не нужно будет обучать их и рассказывать для чего это нужно.

При использовании SMS-токенов взимается плата за услуги операторов по доставке сообщений. Мы делаем все возможное, чтобы уменьшить цену и сделать этот инструмент еще более удобным и доступным для Вас.



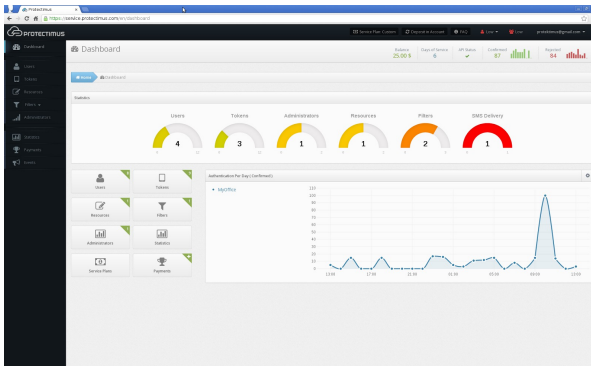
Использование e-mail токенов абсолютно бесплатно, но в то же время это максимально упрощенный вариант защиты, так как доступ к почтовому ящику чаще всего защищен знанием пароля. Следует понимать, что уровень защиты таким токеном ниже, чем у других токенов, особенно, если используется один и тот же пароль для входа в почту и защищаемый ресурс.



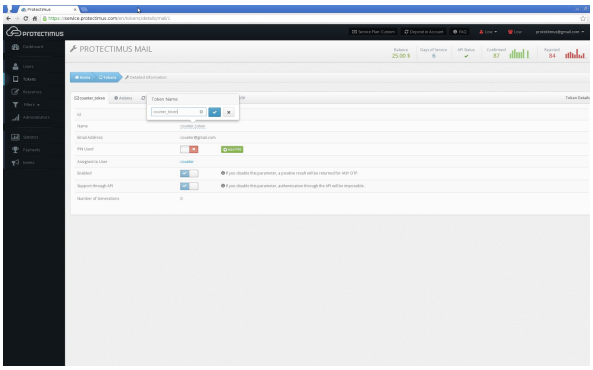
Графический интерфейс пользователя

Графический интерфейс пользователя построен на базе фреймворка Tapestry 5.3 с использованием Bootstrap, jQuery, AJAX, JavaScript. Далее представлено несколько скриншотов системы Protectimus.

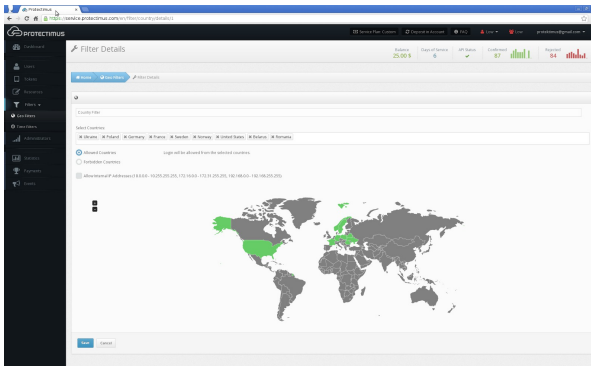
Панель управления



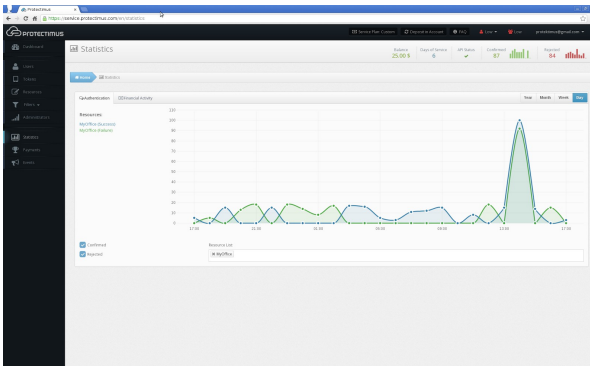
Редактирование информации о токене



Гео-фильтры



Статистика



Удобству пользователей уделено особое внимание, любое действие находится на расстоянии не более трех кликов. Большинство операций выполняется через AJAX-запрос, что повышает скорость работы системы. А наличие подсказок и рекомендаций позволяет быстрее познакомиться с системой и понять как она работает.

Контактная информация

Наши службы

Потенциальное партнерство, продажи:

sales@protectimus.com

Проблемы, вопросы, обратная связь:

support@protectimus.com

Корпоративная информация

Protectimus Solutions LLP

Телефон: +38(057) 751 62 34