PROTECTIMUS

# Technical Overview

Version 1.0.3 EN
dated 14 November 2020

# Contents

# Solution Overview

Authentication based only on one factor – the password – cannot be considered reliable enough for systems with a high level of security requirements. Using several factors in the authentication system simultaneously significantly increases the system's level of protection against unauthorized access.

Many companies offer their solutions for implementing multifactor authentication, but their problem is that they are bureaucratic monsters with all the predictable consequences: poor communication and subpar service; cumbersome, inconvenient and inflexible products; unavailability of the current information and lack of means to obtain it promptly. Besides, these companies are monopolists; they bill their customers for huge amounts after completing the stage of negotiations with each client, without publically disclosing their prices.

Protectimus aims to offer the best solution in the sphere of two-factor authentication in terms of price and ease of use and ensure a high level of quality and system reliability.

The product developed will allow:

- **Customers** to build more secure services based on the product in a simple and affordable way, regardless of the company's size
- **Customers' users** to securely protect their accounts from unauthorized access

Protectimus offers a comprehensive solution that includes both an authentication system and a wide range of software and hardware tokens.

The authentication system can function both as a separate application installed on a customer's servers and as a cloud service providing a SaaS solution. Protectimus has already taken care of the stable and failure-free operation of its system.

Protectimus solves the problem of two-factor authentication at all levels. Each customer will be able to find a solution that best meets all their requirements.

# System Features

The Protectimus platform supports a wide range of OS (from Linux, FreeBSD to any version of Windows).

The system supports the current and older versions of these popular browsers:
Google Chrome, Mozilla Firefox, Internet Explorer.

All the system's components support the existing software development standards, as well as the OATH standards for OTP authentication, which makes it possible to use third-party manufacturers' or competitors' tokens in Protectimus.

Protectimus ensures the operation of several copies of the application that are not connected with each other in different geographic zones near a customer's users. Also, there is a possibility to have several nodes working for one large-scale customer with users located in various parts of the world.

## Algorithms Used to Generate One-Time Passwords

The following algorithms are used to generate one-time passwords:

- 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

They were developed by the Initiative For Open Authentication (OATH) group with the aim of standardizing authentication methods. These algorithms were thoroughly tested and proven reliable; they have become the standard in the field of two-factor authentication.

# Technology Stack

| # | 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 |

# Software Quality Attributes

In the process of software development, the following was used:

- Standard mechanisms and libraries
- Java Programming Style Guidelines (Java™ Coding Style Guide)
- DRY (Don’t Repeat Yourself) and DIE (Duplication Is Evil) principles
- Test Driven Development (TDD)

## Solution Architecture

Protectimus is based on the best SOA, MVC, RESTful, and other practices. Let's look at the overall solution architecture presented in Figure 1 below.

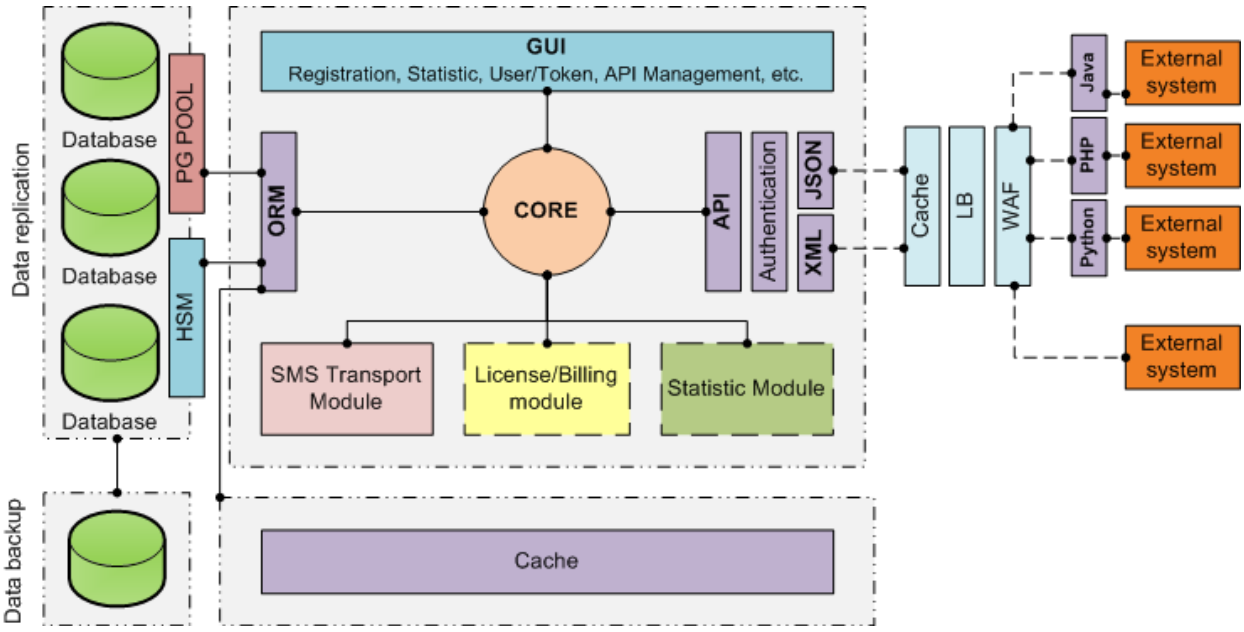



Figure 1. Overall Solution Architecture

To ensure reliable and uninterrupted operation, the system is deployed in a cluster of high-performance servers. The hardware Load Balancer is responsible for distributing and balancing the workload between the servers. The Monitoring System continuously monitors the state of the infrastructure and notifies Protectimus administrators of possible threats and emergencies.

The Hardware Security Module ensures secure storage of cryptographic information.

It is difficult to overestimate the value of the data stored in our system. We must prevent any data loss and provide a data recovery mechanism in the event of any possible failure or force majeure. That is why data backup and data replication are used.

Protectimus "holds" 10 backups: one for each day of the week, as well as backups that are two weeks, one month, and three months old, which allows "rolling back" in time far enough in the event of any data loss. Backups are stored on separate servers.

A common problem with all backups is that they always lag behind in time. In the event of a fatal failure of the primary server, restoring the system will only be possible with some "rolling back" in time; solving this problem is the task of the replication system — replicating

data changes from the database's main server on one or several dependent servers. The primary server is called the master server, and dependent servers are called replicas.
The data changes that occur on the master server are replicated on the replicas (but not vice versa). Therefore, data modification requests (INSERT, UPDATE, DELETE, etc.) are performed only on the master server, and data reading requests can be performed both on the replicas and the master server.
Replication is performed by means of binary logs kept on the master server. All requests resulting in database changes are saved and stored in them. These logs are sent to the replicas, and the requests stored are executed, starting at a certain position. During replication, it is only the queries resulting in database changes that are transmitted, not the modified data.
Thus, the use of backup and replication ensures enhanced system stability and data integrity.

To improve performance, optimization is used at various levels:

- On the client side: caching at the browser level, minimizing resources (HTML, CSS, and JavaScript), image optimization, CSS sprites, etc.;
- On the server side: caching (Memcached), static content processing optimization (Nginx), application server setting optimization, load balancing, etc.;
- On the database end: database setting optimization, use of indexes, partitioning.

The system is managed through a graphical user interface developed on the basis of Twitter Bootstrap, which provides adequate content display in different browsers and on different devices.

The interaction between Protectimus and the customers' systems is performed through the RESTful API; data is transmitted in the XML or JSON format. To facilitate the integration processes, libraries in Java, Python, and PHP were developed. The API documentation is available on the Protectimus website in the Documentation section.

The certified authentication module allows using any tokens that operate based on the standard OATH algorithms – HOTP, TOTP and OCRA - in Protectimus. The SMS delivery module will provide one-time passwords for those users that do not want to or cannot use other types of tokens.

# Integration with Protectimus

To integrate Protectimus into your project, you can use these two methods:

1. Integration using the API. For integration through the API, we provide a set of auxiliary libraries for the following programming languages: Java, Python, and PHP. If there is no client for your programming language, you can use detailed descriptions of all the API methods using this link.
2. Integration using the IFrame widget for user authentication.

User authentication is always performed for a specific resource; therefore, a user must be assigned to the resource to which this user should have access. If a user is not assigned to a resource, this user will have no access to this resource. The method of assigning a user to a resource depends on the authentication method selected. Protectimus supports several user authentication methods:

1. **User authentication with a static password.** This method requires that a user should have a password, and that this user should be assigned to the resource for which authentication is performed.

**Note:** Protectimus will ensure secure storage of your users' passwords and will not use them for any purpose other than their intended purpose. You can find detailed information about this on the PRIVACY POLICY page. You can find information on how to securely transmit and use your users' passwords in Protectimus in the documentation on our API.

2. **User authentication with a one-time password.** This method requires that a user should have a token, and that this user should be assigned to a resource WITH this token. This method will not work if a user and a token are assigned to a resource separately from each other.
3. **User authentication with a static password and a one-time password.** It is a combination of the two methods described above. A user must be assigned to a resource WITH a token. This user must have a password. If a user's token is deactivated, OTP authentication will not be performed, in which case only this user's static password and this user's compliance with the filters' requirements, if any, will be authenticated.
4. **Token authentication on a resource.** This method allows you not to assign a token to any specific user, but simply to verify the validity of a one-time password generated by the token. This method requires that a token should be assigned to a resource.

**Note:** During authentication, it is verified, among other things, whether or not a request meets the requirements of the filters on this resource.

**Note:** If a user's authentication is not successful because this user enters an incorrect OTP, the value of the counter of failed authentication attempts for this token will be increased. When the threshold of failed authentication attempts for the specified resource is exceeded, a token will be locked. A token can be unlocked either through the web interface or through the API (the Editing Token method). If a user's authentication is successful, the counter of failed authentication attempts is reset to zero if it has not exceeded the allowable limit for this resource, and if this user has not yet been blocked.

# Tokens Used in Protectimus

You can use different types of tokens to generate one-time passwords.

## Hardware Tokens

Hardware tokens are devices intended specially for generating OTPs. They are typically small and can be used as a keychain. We offer the following hardware token models: Protectimus TWO, Protectimus SLIM NFC, and Protectimus FLEX. Let’s look at these tokens in more detail.

**Protectimus TWO** are classic hardware TOTP tokens. High-strength and water-resistant. Protectimus TWO tokens are produced with pre-installed secret keys that can't be reprogrammed.

Protectimus TWO

High-strength, water-resistant hardware OTP tokens

**Key features:**

- Algorithms: TOTP (RFC 6238); SHA-1, SHA-256 (optional)
- Produced with pre-installed secret keys
- Full water resistance – class IP68
- One-time password lifetime – 30 seconds, 60 seconds (optional)
- 6-digit display, 8-digit display (optional)

**The best choice for:**

- Corporate use with Protectimus multi-factor authentication service.
- Corporate use if you can add the secret keys to the authentication system you use.


**Protectimus Slim NFC** are programmable hardware TOTP tokens in a credit card format. Thes OTP tokens can be reprogrammed using the Protectimus TOTP Burner application for Android phones with NFC support. The user can assign a new seed (secret key) an unlimited number of times and can select the desired lifetime for generated OTPs: 30 or 60 seconds. The programmable Protectimus Slim mini token is the most reliable, practical, and convenient solution for two-factor authentication.


Protectimus Slim NFC

Programmable security tokens – hardware alternative to Google Auth and other 2FA apps

**Key features:**

- Available in 2 form-factors: standard bank card and mini
- Algorithms: TOTP (RFC 6238); SHA-1, SHA-256 (optional)
- Supports 16- to 32-character long secret keys (Base32)
- Can be programmed over NFC (Android smartphone is required)

**The best choice for:**

- Corporate use with Google Authenticator based authentication systems as well as Microsoft Azure MFA, Office365, Duo, Okta, etc.
- Personal use with Google, Dropbox, GitHub, Kickstarter, Mailchimp, Microsoft, Facebook, many cryptocurrency exchanges, etc.

**Protectimus FLEX** are programmable hardware TOTP tokens in a key fob format. Unlike traditional TOTP hardware tokens, whose secret keys can't be changed, you can add a new secret key to the Protectimus Flex OTP token over NFC. This makes it possible to connect the OTP device to any site that supports two-factor authentication. The only requirement is that the secret key be no longer than 32 Base32 characters.

Protectimus Flex

Programmable hardware TOTP token in a key fob format

**Key features:**

- Algorithms: TOTP (RFC 6238); SHA-1
- Can be programmed over NFC (Android smartphone is required)
- Supports 16- to 32-character long secret keys (Base32)
- One-time password lifetime – 30 seconds or 60 seconds (can be set when programming the token)
- 6-digit display with the one-time password lifetime and battery life indicators
- Time synchronization feature

**The best choice for:**

- Corporate use with Protectimus multi-factor authentication service; Google Authenticator based authentication systems; as well as Microsoft Azure MFA, Office365, Duo, Okta, etc.
- Personal use with PayPal, Google, Dropbox, GitHub, Kickstarter, Mailchimp, Microsoft, Facebook, Twitter, many cryptocurrency exchanges, etc.

## Software Tokens

**Protectimus SMART** is an application from Protectimus used to generate OTPs; it can be installed on Android and iOS. The application has no connection with the server, which eliminates the risk of any unauthorized impact on the authentication system by means of taking over the communications channel.
Protectimus SMART allows customers to save money on the implementation of two-factor authentication and allows users to simplify its use. You can create several tokens in the application, which allows working with different independent systems with two-factor authentication using one device.

Protectimus SMART OTP

Free two-factor authentication application for iOS and Android with PIN and backup

**Key features:**

- Algorithms: HOTP (RFC 4226), TOTP (RFC 6238), OCRA (RFC 6287); SHA-1, SHA-256 (coming soon), and SHA-512 (coming soon)
- Customized OTP length: 6 or 8 characters
- CWYS function support (data signing)
- Cloud backup (coming soon)
- Push notifications (coming soon)
- PIN or fingerprint protection (coming soon)
- Available in English and Russian
- Multiple tokens can be created on one device
- Available for free for iOS and Android

**The best choice for:**

- Personal use with any website that supports 2-factor authentication.
- Corporate use with Protectimus or any other two-factor authentication service.

# SMS and Email Tokens

One-time passwords will be sent to the phone number or the email address specified. Using such tokens simplifies interaction with users; users are not required to perform any additional actions, and they can be located in various parts of the solar system.

Users are already familiar with the practice of confirming their identity with codes received by phone, which means that you will not have to train them or explain why it is necessary.
When SMS tokens are used, a fee is charged for the services of message delivery operators. We do everything possible to lower this fee and make this instrument even more convenient and affordable for you.

Protectimus SMS

One-time passwords delivery via SMS messages

**Key features:**

- Algorithms: HOTP (RFC 4226)
- CWYS function support (data signing)
- No additional user instructions are necessary
- You can connect your own SMS provider if you use Protectimus service on-premises

**The best choice for:**

- Corporate use with Protectimus multi-factor authentication service.


You can use email tokens free of charge; besides, it is the most simplified protection method because access to an email inbox is typically protected with a password. It is important to understand that the level of protection provided by this token is lower than that of other types of tokens if the same password is used to access email and the protected resource.

Protectimus Mail

Free one-time passwords delivery via email

**Key features:**

- Algorithms: HOTP (RFC 4226)
- CWYS function support (data signing)
- No additional user instructions are necessary
- Free delivery of any messages and notification in addition to one-time passwords

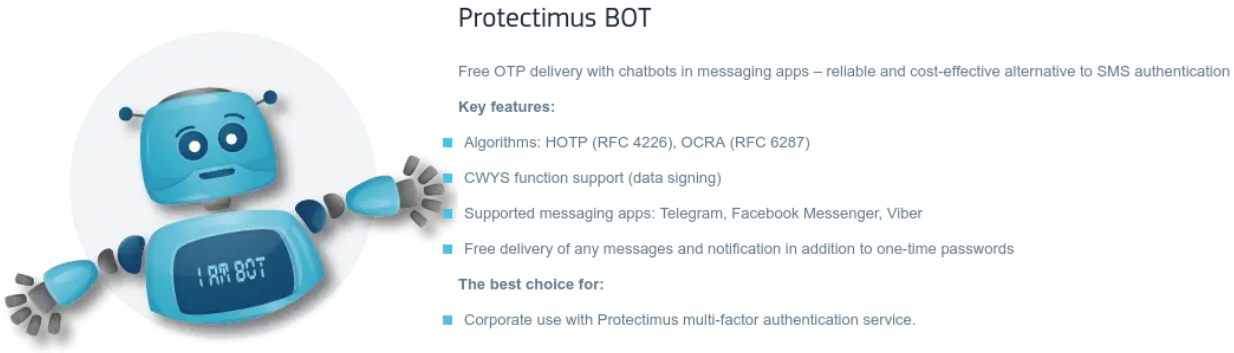
**The best choice for:**

- Corporate use with Protectimus multi-factor authentication service.

# Protectimus Bot

One-time password delivery in messaging apps is easy, secure and free. The service is already available on Telegram, Viber and Facebook Messenger. It's time to say no to outdated and insecure SMS authentication. Connect to the Protectimus chatbot in your messaging app to receive one-time passwords and important notifications without the risk of having messages intercepted.

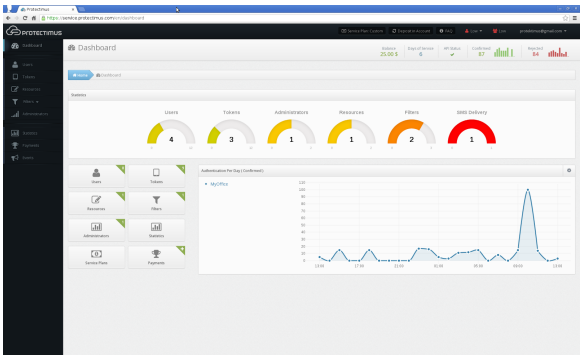
It's the most convenient method for receiving one-time passwords. There's no more need to pay SMS providers, buy hardware OTP tokens, or ask your users to install extra OTP generator apps. Users need only add the ProtectimusBot chatbot to their usual messaging app. And after a quick, 15-second setup process, they will receive one-time passwords and other important messages.



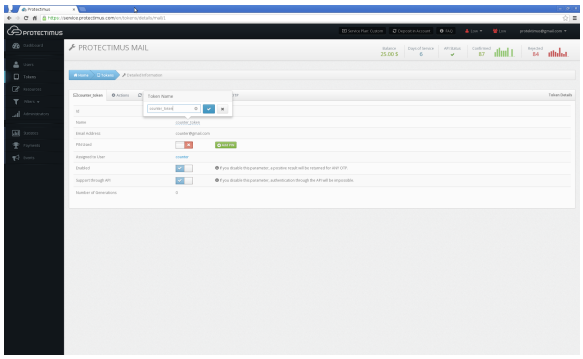
# Graphical User Interface

The graphical user interface is built on the basis of the Tapestry 5.3 framework with the use of Bootstrap, jQuery, AJAX, and JavaScript. Below you can see several screenshots from the Protectimus system.

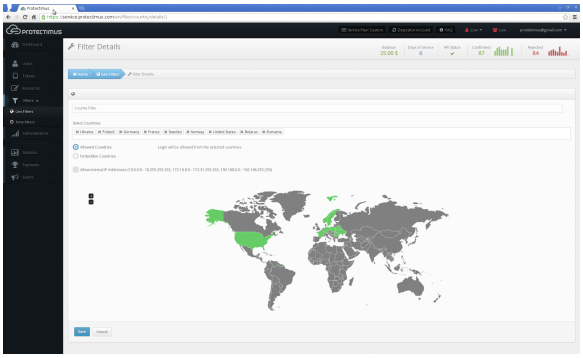
### Control Panel



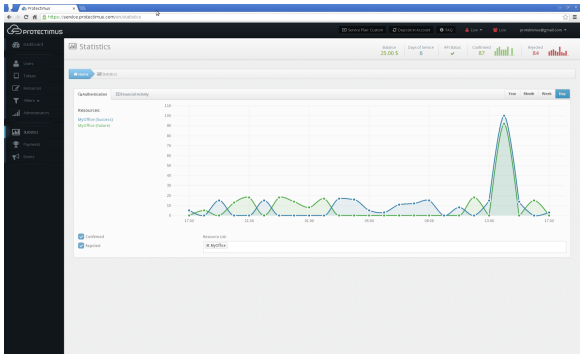
### Editing Token Details



### Geo Filters



### Statistics



Special priority is given to users' convenience; any action can be performed in a maximum of three clicks. Most operations are performed via an AJAX request, which increases the speed of the system's operation. Prompts and recommendations allow quickly familiarizing oneself with the system and the way it operates.

## Contacts

Technical questions, software distribution, and any help:

support@protectimus.com

Partnership, sales, business opportunities:

sales@protectimus.com

Call us:

Ireland +353 1 563 2165

United Kingdom: +44 20 3808 7124

USA: +1 786 796 66 64

Ukraine: +38 057 706 21 24

Russia: +7 499 677 16 34

## Corporate Information

Protectimus Limited

Carrick House

49 Fitzwilliam Square

Dublin 02, N578

Ireland