РАЗРАБОТКА И РЕАЛИЗАЦИЯ RESTFUL API ДЛЯ КОНТРОЛЯ ДОСТУПА НА ОСНОВЕ МОДЕЛИ ORBAC В ОРГАНИЗАЦИЯХ. НА ПРИМЕРЕ ГЛАВНОГО УПРАВЛЕНИЯ КАЗНАЧЕЙСТВА И ГОСУДАРСТВЕННОГО УЧЕТА (DGTCP) В РЕСПУБЛИКЕ БЕНИН

Муаль Мутуама Нда Бьенвеню
Аспирант, Российский Университет Дружбы Народов
bmouale@mail.ru
Самбьену Кувиммиту Калеб
Орловский Государственный Университет имени И. С. Тургенева
Куаме Гнабро Йанник
Аспирант, Российский Университет Дружбы Народов

Аннотация. Безопасность информационных систем сегодня особенно важна. В том числе, когда общественные и частные компании находятся в постоянной реорганизации, расширении или совершенствовании своей информационной системы (ИС), с целью улучшения эффективности. Это есть случай DGTCP, когда администрация государственной политики в правительстве Бенина участвует в процессе реструктуризации в соответствии с функциональными требованиями для улучшения качества предлагаемых услуг. Эта реорганизация имеет значительное влияние на ее информационную систему. Действительно, процедуры стали более сложными, и обеспечение безопасности ИТ-системы становится очень важной проблемой. В этой статье мы предлагаем внедрение системы контроля доступа на основе модели OrBAC для усиления безопасности этой правительственной организации. Эта система будет рассматриваться как политика безопасности, и будет реализована как RESTFull API, позволяющая существующим или будущим бизнес-приложения имеет доступ к ресурсам организации. Имитационные тесты были выполнены, чтобы убедиться, что система работает так, как задумано.

Ключевые слова: Контроль доступа, OrBAC, веб-API, политика безопасности, безопасность, DGTCP.

DESIGN AND IMPLEMENTATION OF A RESTFUL API FOR ACCESS CONTROL BASED ON THE ORBAC MODEL IN AN ORGANIZATION. CASE: MAIN DEPARTMENT OF THE TREASURY AND STATE ACCOUNTING (DGTCP) IN THE REPUBLIC OF BENIN

Mouale Moutouama N'dah Bienvenue
Sambienou Kouwimmitou Caleb
Kouame Gnabro Yannick

Summary. Information systems security is particularly important today as public and private companies are in constant reorganization, expansion or enhancement of their information system in order to be more efficient. For example, the head office of task (DGTCP), a strategic public administration in the Benin government's policy, is engaged in a process of restructuring it to meet functional requirements in order to improve the quality of the offered services. This reorganization has a significant impact on the information system. Indeed, the procedures have become more complex and ensuring IT system security has become a very important issue.

In this dissertation, we proposed implementation of an access control system based on the Organization Based Access Control (OrBAC) model to strengthen the security of this (government) organization. This system will consider the organization's security policy and will be implemented as a RESTFull API, allowing existing or future business applications to access the organization's resources depending on the employees' rights and context. Simulation tests have been performed to ensure that the system is working as intended.

Keywords: Access control, OrBAC, Web API, security policy, security, DGTCP.

Введение

Сегодня компьютерные системы занимают важное место в компаниях, администрациях и повседневной жизни людей. Это явление было вызвано, среди прочего, быстрым развитием информационных и коммуникационных технологий. Зависимость от этих взаимосвязанных систем в различных аспектах жизни, и их повсеместного распространения, дает много преимуществ. В общем, через обмен информацией и доступ к ней [5], а также, в частности, через средства связи к быстрому и недорогому совместному использованию вычислительных ресурсов и ресурсов хранения большой ёмкости (облачное копирование).

Чтобы воспользоваться этими преимуществами для максимального увеличения производительности и эффективности в достижении своих целей, компании проводят организационные изменения, в ходе которых создается несколько иерархических уровней, несколько назначений разделены и состоят из нескольких актёров.

Эта реорганизация оказывает влияние на информационную систему, которая является очень ценным активом, и чьё эффективное управление данными имеет первостепенное значение. Таким образом, конфиденциальные данные, процессы, инфраструктуры информационной системы компании подвергаются злонамеренным действиям, характер и способ вторжения которых постоянно меняются.

Целью данной статьи является разработка и внедрение системы контроля доступа на основе модели OrBAC в соответствии с политикой безопасности DGTCP и непосредственно доступа ко всем бизнес-приложениям (существующим и/или будущим) указанной организации независимо от их местоположения в информационной системе и/или языка программирования, используемого в их проекте.

Для решения поставленной задачи мы представили моделирование системы, а также выбор различных инструментов, используемых для реализации указанной системы.

В первом разделе мы более подробно представим модули, которые составляют систему контроля доступа и систему администрирования, их реализации, а также технологии, которые были применены. Во втором мы представим серию тестов и экспериментов, которые были выполнены, чтобы убедиться, что система работает правильно. И в последнем разделе будет проведено заключение полученных результатов.

Система обозначения

API: интерфейс прикладного программирования
DGTCP: главное управление казначейства и государственного учета
PGT: казначей общего казначейства
HTTP: протокол передачи гипертекста
JSON: нотация объектов JavaScript
JWT: JSON Web Token
OrBAC: управление контролем доступа в организации
RBAC: управление ролями и доступами
WWW: всемирная паутина сети
UML: унифицированный язык моделирования

Используемая технология

Для реализации наших систем мы прибегли к определенным технологиям, которые являются:

Spring Загрузочный (Spring Boot)

Spring — это бесплатный фреймворк (Framework) для разработки и определения инфраструктуры приложений Java, и облегчает разработку и тестирование. Он предлагает Spring Boot, модульный подход для быстрого и эффективного создания API веб-сервисов. В нескольких строках кода с (очень) небольшим проектом Maven или Gradle мы получаем непосредственно исполняемый файл.jar. Все включено, в том числе кирпичи веб-сервера, которые нам нужны. Можно очень легко использовать необходимые фреймворки (например, Hibernate или любой кирпич классической Spring). Spring Boot обеспечивает мощность сервера приложений, сохраняя только то, что вам действительно нужно. Сериализация JSON работает изначально, а маршрутизация на основе аннотаций очень проста в обращении. Spring Boot является частью одной из лучших фреймворков для разработки веб-приложений в целом, и веб-API частным образом. Более того, его сообщество растет из года в год.

MySQL

MySQL — самая популярная в мире база данных с открытым исходным кодом. Благодаря своей производительности, надежности и простоте использования, MySQL зарекомендовал себя как очевидный выбор базы данных для веб-приложений. Эта база данных существует под несколькими типы лицензий, более эффективными. В нашем случае, мы выбрали бесплатную лицензию. Выбор MySQL был мотивирован его простыми свойствами в реализации, такие, как репликация и распределение нагрузки.

Таблица 1. Архитектурные ограничения bscakoAPI

Свойства	Детали/Значения
Архитектура	Клиент-Сервер
Протокол	HTTP
Формат запросов и ответ	JSON
Сессия	Да
Аутентификация	Через токен [2.2.1.1]

Реализация

В общем, моделируемая система основана на модели Model; Просмотр; Контроллер (MVC).

Система контроля доступа (bscakoAPI)

Мы начали с наблюдения, что DGTCP — это организация, которая уже имеет много бизнес-приложений, и не собирается останавливаться на достигнутом. Таким образом, чтобы стандартизировать данные, которые будут обрабатываться различными системами и бизнес-приложениями, мы решили, что система контроля доступа имеет форму RESTFull API и называется bscakoAPI. Система bscakoAPI состоит из двух основных модулей, а именно модуля аутентификации и модуля контроля доступа. Он предоставляет интерфейс для каждого модуля, которые его составляют.

bscakoAPI представляет архитектурные ограничения, которые указаны в следующей таблице:

Модуль аутентификации

Модуль аутентификации — это модуль, который позволяет пользователю аутентифицироваться в приложении через bscakoAPI (обратите внимание, что сам API является приложением организации). Аутентификация осуществляется через два уровня безопасности, где информация инкапсулирована в заголовке HTTP-запроса:

Ключ приложения. Это ключ, который идентифицирует уникальное приложение в системе. Его структура — это структура JWT, и он предоставляется администратором безопасности после обращения к приложению. Он встроен в заголовок ключа любого запроса к системе контроля доступа.

Учетные данные для входа — Это данные аутентификации пользователя. Они обычно состоят из:

- Имя пользователя / адрес электронной почты и пароль. Эти элементы часто кодируются в заголовке Авторизации с базовым механизмом аутентификации.
- Ключ аутентификации, сгенерированный bscakoAPI по запросу пользователя. Этот ключ часто кодируется в заголовке авторизации с помощью механизма аутентификации Носитель.

Этот модуль предоставляет интерфейс, который может использоваться всеми бизнес-приложениями в организации.

Модуль контроля доступа

Это сердце этой системы. Он позволяет проверить доступ к ресурсам пользователя в соответствии со своими прерогативами и задачами, ранее определенными из политики организации, и ранее предоставленными администратором безопасности. Этот модуль использует модуль аутентификации. Он предоставляет интерфейс, используемый всеми бизнес-приложениями организации.

Система администрирования bscakoAPI

Система администрирования bscakoAPI была смоделирована для того, чтобы облегчить задачу администратора безопасности в его функциях. Это основной инструмент или приложение любого администратора безопасности для хорошего управления политикой безопасности, а также для конфигурации систем управления доступом и аутентификации организации. Настоящая система состоит из двух основных модулей, а именно модуля администрирования безопасности и модуля MotOrBAC.

Модуль администрирования безопасности

Это сердце системы администрирования безопасности. Он отвечает за управление ссылками на бизнес-приложения, на пользователей организации и назначение им привилегий для аутентификации в бизнес-приложениях. Он использует модуль MotOrBAC и интерфейсы, созданные в bscakoAPI.

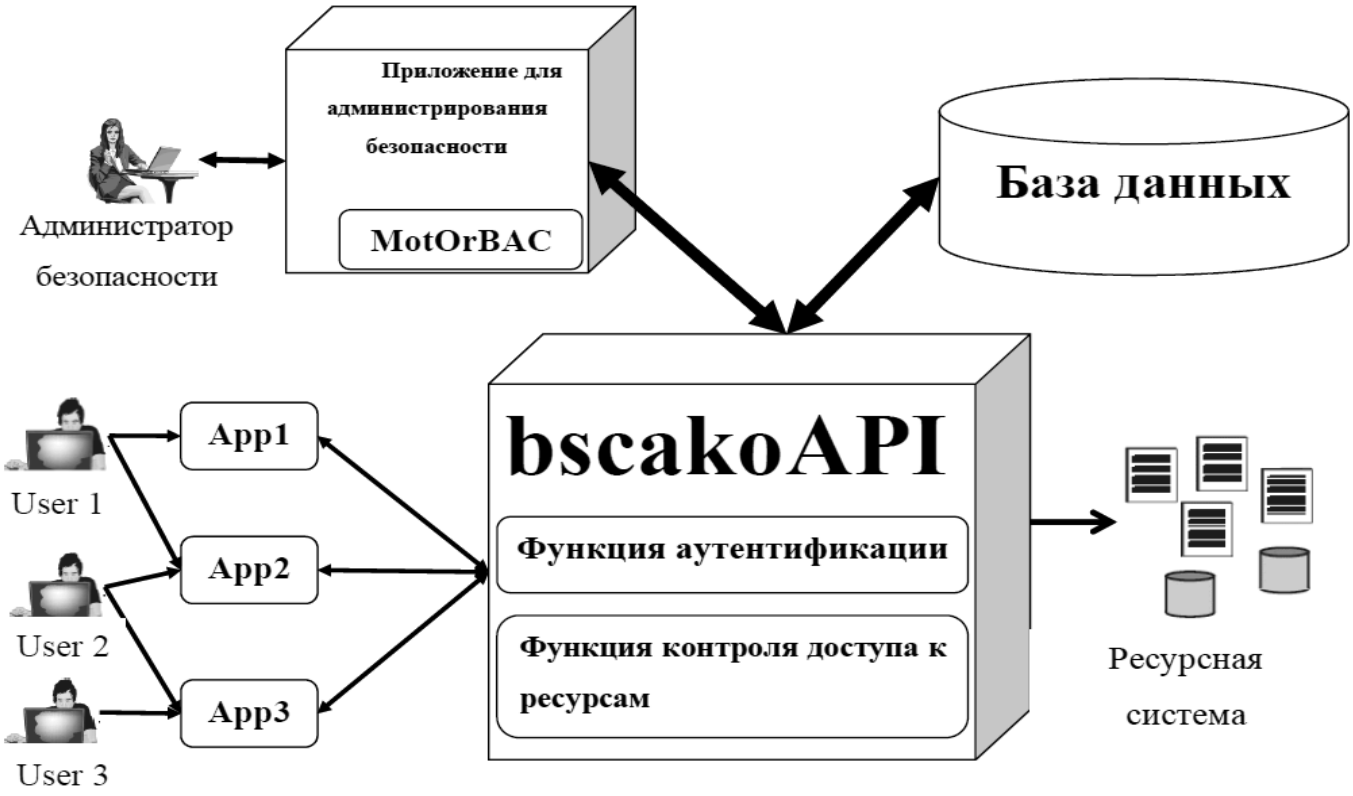

Рис. 1. Общая архитектура всей системы

Модуль MotOrBAC

Инструмент администрирования содержит последнюю версию MotOrBAC [2]. Этот модуль обеспечивает выполнение MotOrBAC, позволяя администратору безопасности управлять политикой безопасности организации.

Заключение

В этом разделе, мы представили различные модули, которые составляют систему контроля доступа. Администрация создана внутри организации «DGTCP».

Общий вид всей системы выглядит следующим образом (рис. 1)

В оставшейся части нашей работы мы представим серию тестов и экспериментов, которые были сделаны чтобы убедиться, что система работает правильно. И в последнем разделе будет проведено заключение полученных результатов.

Эксперименты и анализ Особенности bscakoAPI

После развертывания bscakoAPI и его инструментов администрирования, администратор безопасности приступает к настройке систем контроля доступа и аутентификации в соответствии с руководством пользователя. В этом разделе мы познакомимся с рабочим интерфейсом некоторых пользователей при использовании системы контроля доступа, настроенной для этой цели администратором безопасности в соответствии с руководством пользователя. Мы разрабатываем политики безопасности DGTCP, и предоставляем эту политику безопасности на уровне системы контроля доступа, после аутентификации администратора безопасности с помощью инструмента администрирования.

В рамках наших тестов мы представим сценарий обработки и выплаты зарплат и пенсий PGT. Мы считаем номинальным случай, где расходы (мандат и платежное поручение) рассматриваются с оплатой на счетчиках DGTCP и выплатой пенсий.

Описание

Зарплаты поступают к верификаторам, они выполняют обработку (проверяют и противодействуют удержаниям). Затем эти зарплаты (ценные бумаги) направляются в отдел контроля регулярности, который проверяет и передает их генеральному плательщику для получения разрешения на оплату. Кассовые чеки (части оплаты зарплат) передаются кассиру, действительному кассиру,

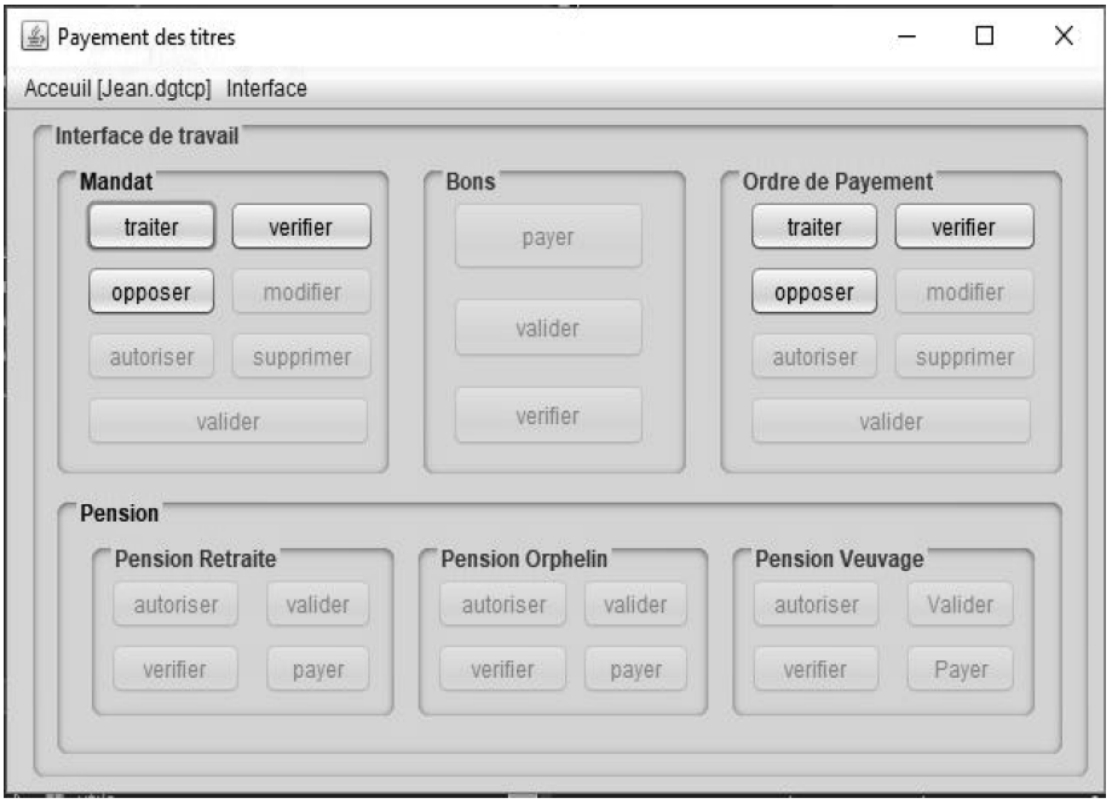

Рис. 2. Задачи аудитора(верификатора) в PGT в рабочее время (с 8:00 до 13:00 и с 15:00 до 19:00).

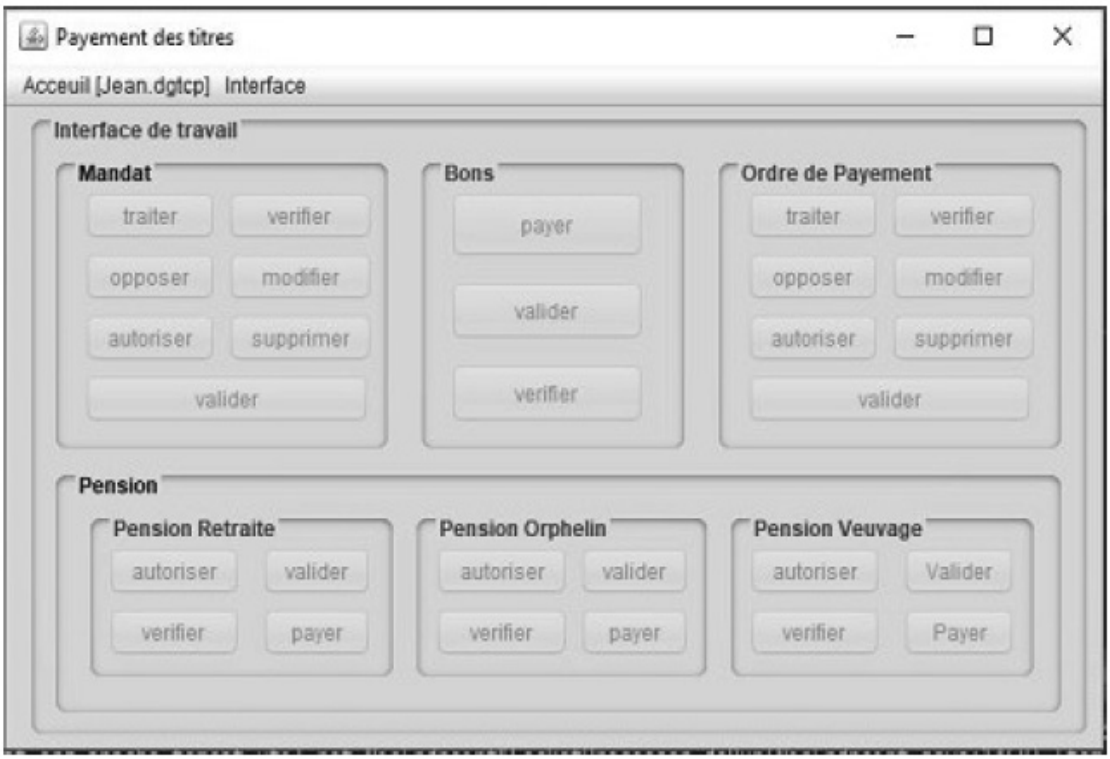

Рис. 3. Обязанности аудитора(верификатора) в PGT вне рабочего времени.

Рис. 4. Задачи Главного Регулярного Управления в PGT.

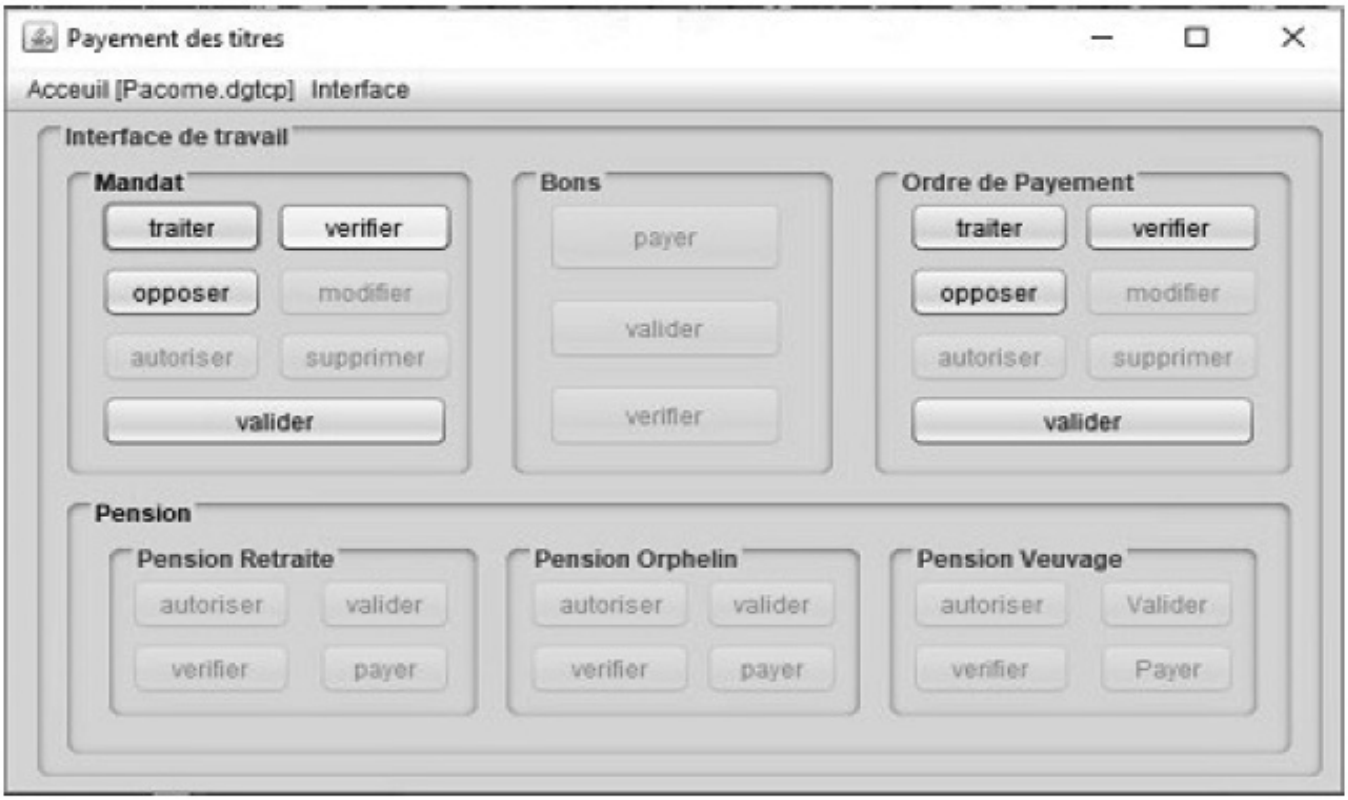

Рис. 5. Задачи Главного Регулярного Управления в PGT в случае чрезвычайной ситуации.

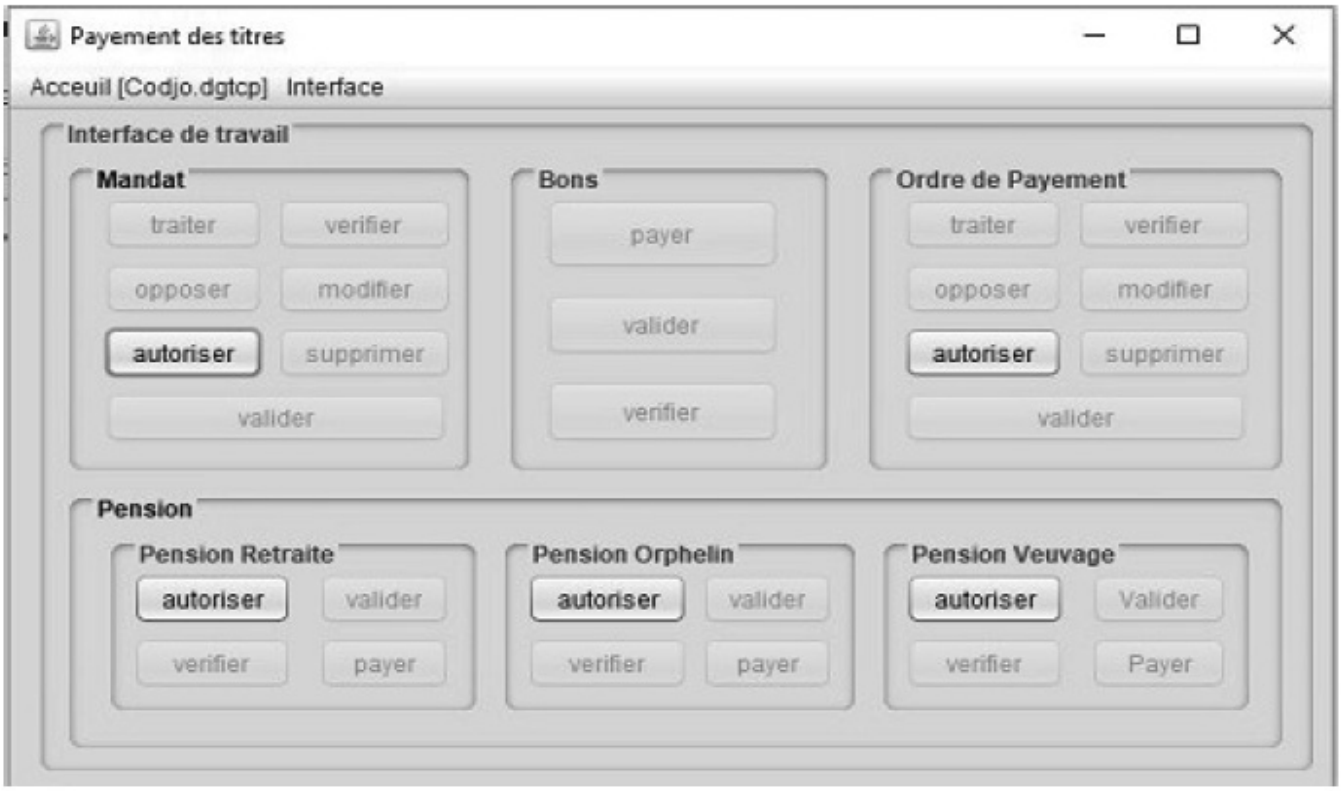

Рис. 6. Задачи главного плательщика в PGT.

и делают их доступными на уровне кассира для эффективной оплаты. В случае пенсий, генеральный кассир разрешает платеж действительному кассиру, и делает их доступными на прилавках.

Бизнес-приложение «Оплата зарплат (ценных бумаг)» было специально разработано, и может рассматриваться как модель для будущих разработок бизнес-приложений любой организации. Приложение объединяет различные задачи сотрудников организации или под организации в одном графическом интерфейсе.

Учитывая придуманный выше сценарий, этот интерфейс объединяет все задачи пользователей, которые вмешиваются в процесс обработки и выплаты зарплат (ценных бумаг) и пенсий.

Результаты будут представлены по ролям.

Аудитор(верификатор) в PGT (рис. 2, 3).

Анализ: Аудиторы(верификаторы) в PGT при обработке зарплат (ценных бумаг) могут выполнять только проверки, возражения и обработки ордеров и / или платежных поручений. Эти задачи выполняются только в рабочее время (с 8 до 13 часов и с 15 до 19 часов).

Главный регулярный контроль PGT (рис. 4, 5):

Анализ: Главное управление по контролю за соблюдением нормативных требований регулярно выполняет задачи проверки мандата и / или платежного поручения. В случае возникновения чрезвычайной ситуации, к его первоначальным прерогативам добавляются такие, как проверка, возражение и подтверждение мандата и / или порядка оплаты.

Генеральный плательщик (рис. 6).

Анализ: главный плательщик авторизует денежные переводы, платежные поручения и пенсии для оплаты.

Главный кассир (рис. 7, 8).

Анализ: Главный кассир по умолчанию имеет обязательство (обозначенное звездочкой (*) на графическом интерфейсе) проверять ваучеры. Но каждые 28–31 месяца (пенсионного периода) он имеет обязательство утвердить пенсии (выход на пенсию, сиротство и вдовство).

Кассир (рис. 9, 10)

Анализ: Кассир проводит проверку и оплату кассовых сертификатов и пенсий только в часы работы кассы (с 8 до 11 и с 15 до 17h).

Рис. 7. Задачи главного кассира в PGT.

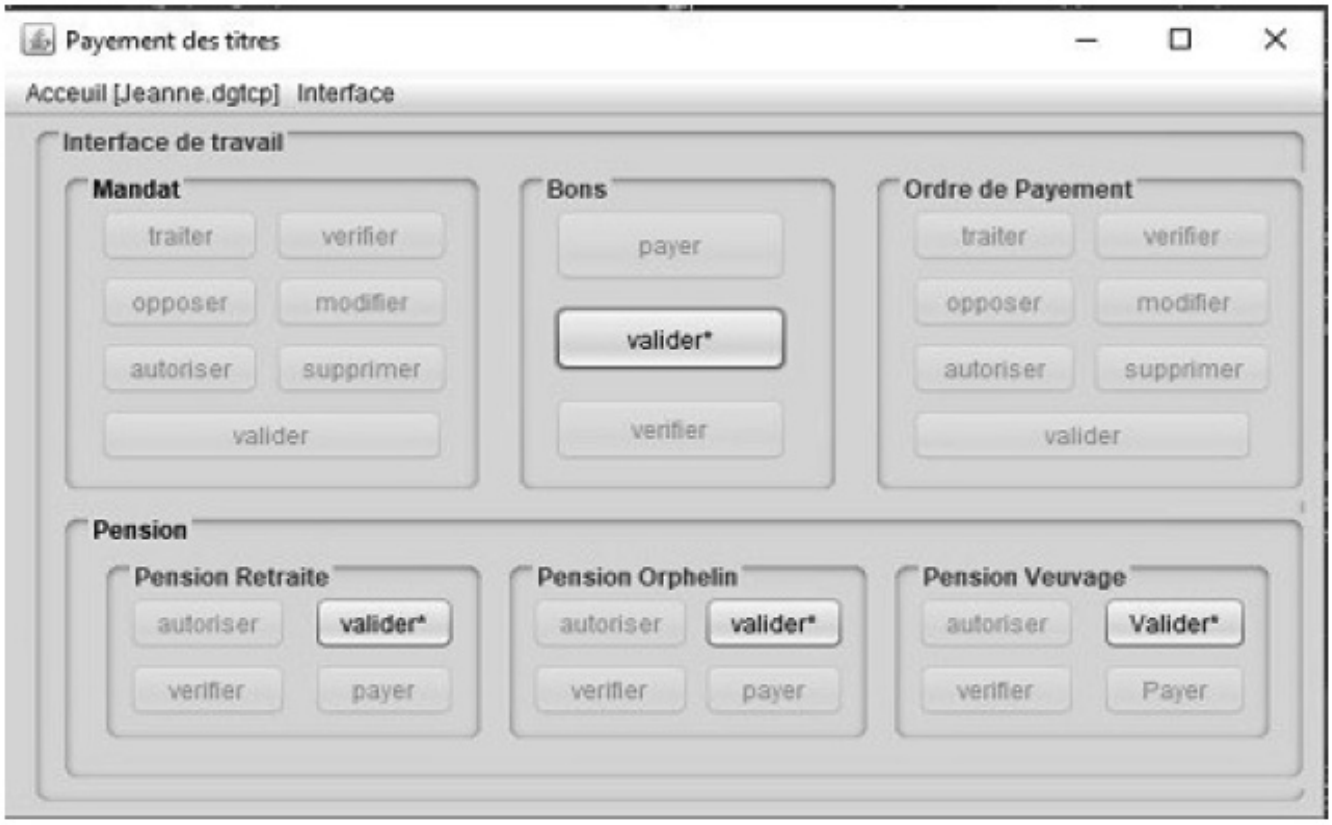

Рис. 8. Задачи главного кассира в PGT в течение пенсионного периода (с 28 до 31 месяца).

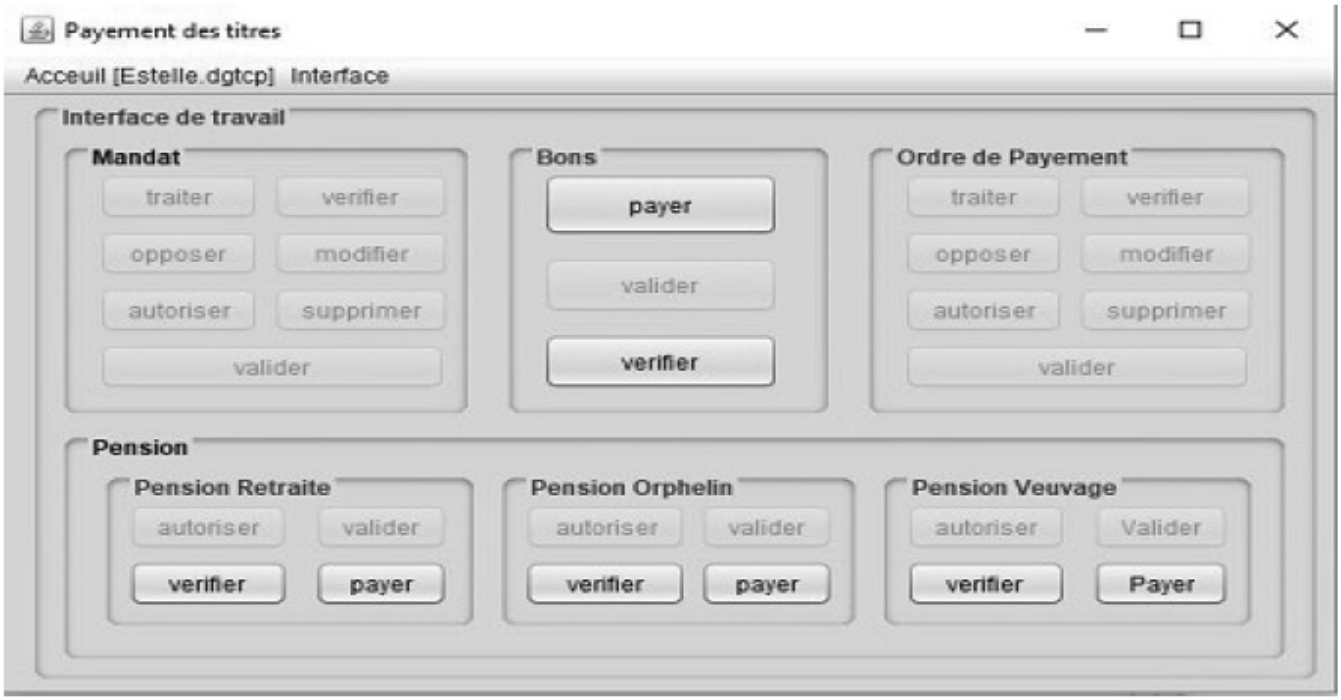

Рис. 9. Обязанности кассира в PGT в рабочее время кассы (с 8:00 до 11:00 и с 15:00 до 17:00).

Рис. 10. Обязанности кассира в PGT вне рабочего времени кассы.

Таблица 2. Результаты теста производительности.

Функции	Среднее время обработки (в мс)	Актеры
Идентификация	822	Всех
Реализация политики безопасности	5000	Администратор безопасности
Ссылки на бизнес-приложения	890	Администратор безопасности
Присвоение привилегий	834	Администратор безопасности
Доступность ресурса	915	Всех

Производительность bscakoAPI

Тесты производительности bscakoAPI, выполненные с помощью программного обеспечения «postman», записаны в следующей таблице:

Обсуждение

В нашем исследовании мы отметили, что система контроля доступа обеспечивает более элементарный контроль доступности ресурсов в организации. Система контроля доступа bscakoAPI — это удобное, спроектированное, разработанное и развернутое решение, которое обеспечивает и гарантирует пользователям доступ к ресурсам в соответствии с их прерогативами, которые определены политикой безопасности организации. Кроме того, с одной стороны, результаты каждой роли согласуются с их прерогативами.

С другой стороны, они показывают нам, что когда политика безопасности четко определена и сделана доступной на уровне контроля доступа bscakoAPI, и что бизнес-приложения имеют хорошие ссылки, то эти бизнес-приложения получают доступ только к тем ресурсам, которые предназначены в соответствии с контекстом и аутентифицированными пользователями. Пользователи при этом не могут превзойти прерогативы, назначенные им со времен политики безопасности.

Короче говоря, введение в действие bscakoAPI, как описано выше, принесет много пользы для любой организации. Действительно, анализ наших результатов показал, что:

- Каждый сотрудник имеет доступ по существу, и исключительно к тем ресурсам, которые необходимы для выполнения его задач;
- Система контроля доступа bscakoAPI учитывает всю политику безопасности организации, которая разработана и развернута ее администратором безопасности.
- Система аутентификации bscakoAPI обеспечивает единый вход для пользователей приложений в соответствии с конфигурацией, установленной администратором безопасности.
- Наконец, системы аутентификации и контроля доступа bscakoAPI могут использоваться любым приложением или информационной системой благодаря мощному механизму REST.

ЛИТЕРАТУРА

1. DENAKPO M. Vincent. Architecture de médiation des données dédiées à l'édition des statistiques pour le trésor public. Master's thesis, Institut de Mathématiques et de Sciences Physiques, Porto-Novo (Bénin), 2009.
2. Fabien Autrel. MotOrbac. http://motorbac.sourceforge.net/.
3. KELOME T Patrick. réalisation d'un prototype de l'annuaire GSM. Master's thesis, Institut de Mathématiques et de Sciences Physiques, Porto-Novo (Bénin), 2009.
4. Patrick Rodolphe BOKO. Le Système d'Information de la DGTCP: élaboration d'une politique de sécurité basée sur le modèle Or-BAC pour la nouvelle organisation. Master's thesis, Institut deFormation et de Recherche en Informatique (IFRI-UAC), 2017.
5. Yves Deswarte et Sébastien Gambs. Cyber-attaques et cyber-defenses: problématique et évolution. Revue de l'électricité et de l'électronique (REE), (2):23–35, juin 2012