УДК [004.056+003.26](075.8)

Студ. А.А. Орлов
Науч. рук. проф. П.П. Урбанович
(Кафедра информационных систем и технологий, БГТУ)

МОДУЛЬ АУТЕНТИФИКАЦИИ И АВТОРИЗАЦИИ ПОЛЬЗОВАТЕЛЯ ПРИ ДОСТУПЕ К WEB-РЕСУРСАМ

Аутентификация и авторизация играют важную роль в решении проблемы защиты информационных ресурсов [1, 2]. Реализация процедур аутентификации и авторизации пользователя в web-приложениях – трудоёмкий процесс, необходимый в большинстве продуктов. В среде .NET наиболее популярной библиотекой, решающей данные задачи, является *Identity*. Библиотека предоставляет гибкий интерфейс для конфигурации системы аутентификации и авторизации, но имеет ряд ограничений:

– по умолчанию не поддерживает модель полномочий для авторизации пользователей;

– роли глобальны, сложно реализовать системы, где область действия роли ограничена.

Данные ограничения могут быть устранены благодаря гибкой базовой структуре сущностей, добавляемых библиотекой, но для этого требуется дополнительные действия со стороны разработчика. Разработанный модуль создает аналогичную систему на основе модели доступа RBAC (Role-BasedAccessControl) [3] с изоляцией контекстов ролей.

Реализованный модуль имеет ряд особенностей:

– расширяет модель доступа RBAC с использованием полномочий для авторизации пользователей;

– позволяет определить изолированные контексты ролей, определяющие границы действия роли;

– пользователь может быть ассоциирован со множеством ролей, но обладает единственной ролью в рамках контекста;

– в связи с тем, что ко множеству контекстов может получить доступ один и тот же пользователь, прошедший аутентификацию на уровне приложения, существует 2 типа «гостевых» ролей: гостевая роль для пользователей, прошедших процедуру аутентификации, но не получивших роль в рамках контекста и гостевая роль для пользователей, не прошедших процедуру аутентификации.

Для реализации такой модели доступа используется сущность «шаблон», которая определяет набор привилегий для контекстов ролей на основе шаблона. Позволяет реализовать многоуровневые при-

ложения с наборами изолированных сложных ресурсов, например: система управления проектами (создание новых проектов, просмотр общей статистики проектов и т.д.) и проект (управление задачами проекта).

Шаблоны могут быть сконфигурированы при помощи класса-конфигуратора, реализуемого разработчиком. Класс наследуется от базового класса конфигурации и позволяет описать необходимый набор полномочий и базовых ролей, добавляемых при создании контекста роли на основе указанного шаблона. Конфигурация таким способом не является обязательным шагом в интеграции модуля. При необходимости могут быть использованы любые другие средства (заполнение базы данных SQL-скриптом или импорт данных).

Созданные модулем сущности связаны с базой данных при помощи фреймворка *Entity Framework Core* 6. Логическая схема данных модуля представлена на рис. 1.

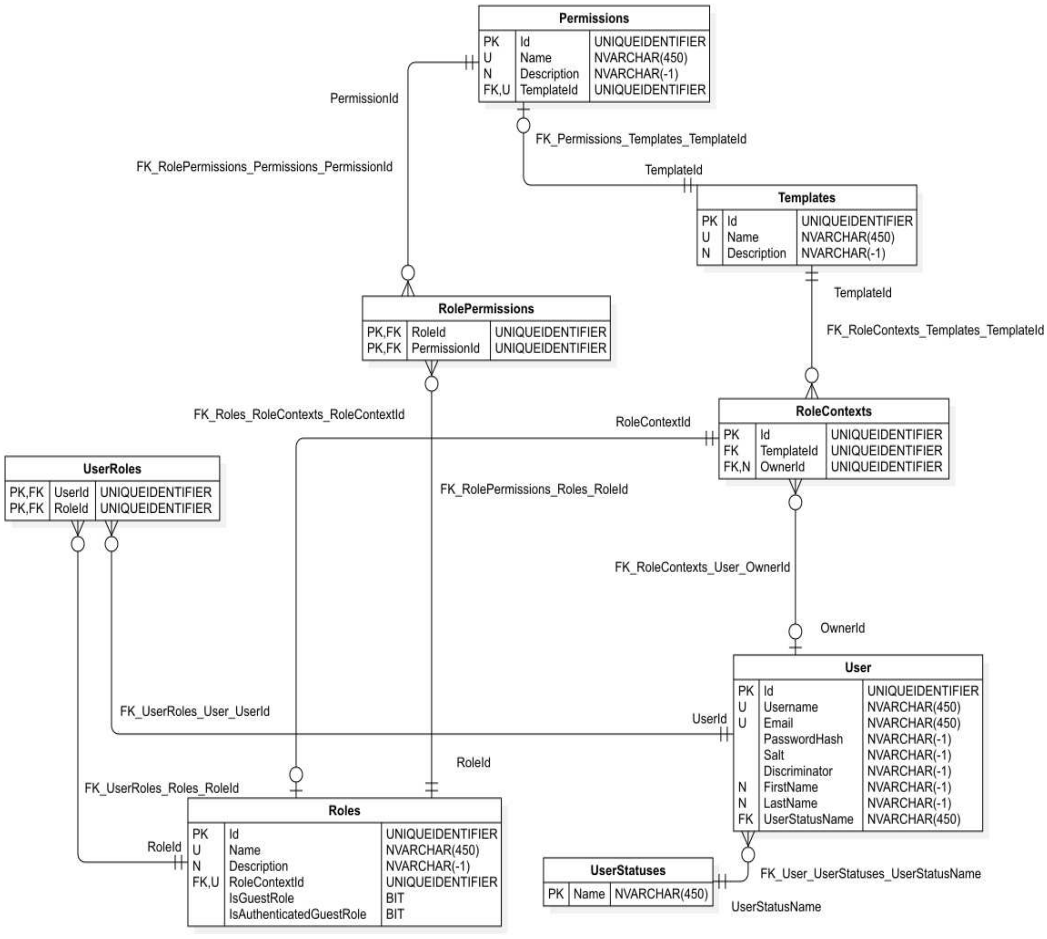

Рисунок 1 – Логическая схема данных модуля

В модуль входит набор из 4 библиотек, включая библиотеку для создания и декодирования токенов стандарта JWT [4] с возможностью добавления электронной цифровой подписи и её верификации. Биб-

лиотека поддерживает добавление новых стратегий создания и верификации подписи. Все библиотеки могут быть опубликованы в виде nuget-пакета и добавлены в проект из репозитория.

Созданный модуль, будучи интегрированным в приложение, позволяет динамически создавать новые роли и устанавливать для них полномочия (рис. 2), а также назначать данные роли пользователям. Все эти действия ограничены в рамках контекста.

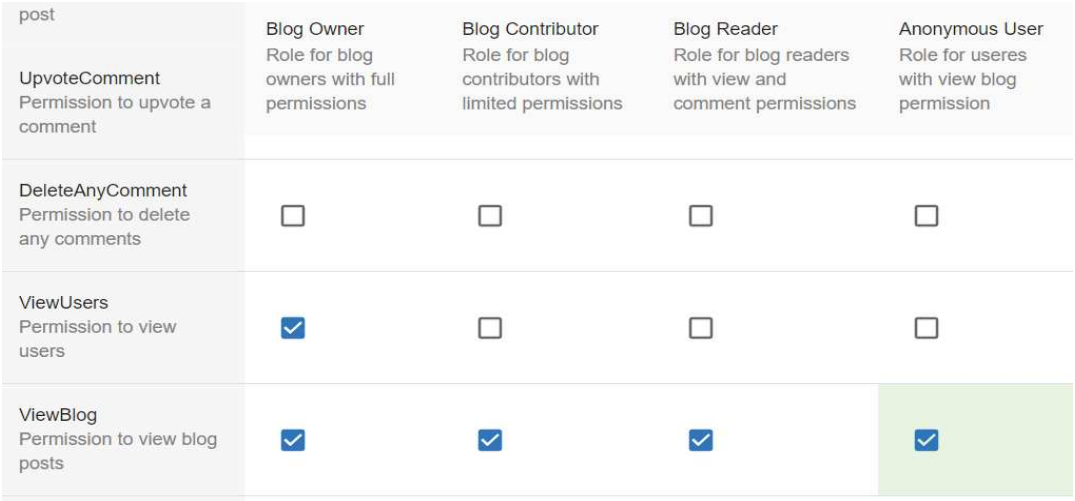

Рисунок 2 – Назначение полномочий ролям в приложении с интегрированным модулем

Разработанный модуль подходит для приложений с требованием к разграничению доступа при помощи полномочий с изолированными контекстами и может быть просто сконфигурирован при помощи созданных инструментов. Аналогичные задачи решаются при помощи других моделей доступа, однако различные модели доступа предоставляют различный баланс между гибкостью и сложностью конфигурации.

ЛИТЕРАТУРА

1. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие. – Минск: БГТУ, 2016. – 220 с.

2. Урбанович, П. П. Компьютерные сети и сетевые технологии: учеб. пособие для студ. технических спец. / П. П. Урбанович, Д. М. Романенко. – Минск : БГТУ, 2022. – 608 с.

3. Role-BasedAccessControl [Электронный ресурс]. – Режим доступа: https://auth0.com/docs/manage-users/access-control/rbac. – Дата доступа: 15.02.2023.

4. RFC 7519: JSON Web Token(JWT) [Электронный ресурс]. – Режим доступа: https://www.rfc-editor.org/rfc/rfc7519. – Дата доступа: 15.02.2023.