**УДК 004.056.55**

***Никулин И. А.***
***Студент кафедры прикладной информатики***
***и информационных технологий***
***НИУ «БелГУ», 4 курс (Белгород, Россия)***
***Научный руководитель: Гахова Н.Н.***
***доцент кафедры прикладной информатики***
***и информационных технологий***
***НИУ «БелГУ», (Белгород, Россия)***
***Nikulin I. A.***
***Student of the Department of Applied Informatics***
***and Information Technology***
***NRU "BelSU", 4rd year (Belgorod, Russia)***
***Scientific supervisor: Gahova N.N.***
***docent of the Department of Applied Informatics***
***and Information Technology***
***NRU "BelGU", (Belgorod, Russia)***

# ТЕХНОЛОГИЯ ПРОЦЕССА ПРОЕКТИРОВАНИЯ И РЕАЛИЗАЦИИ ПОДСИСТЕМЫ PRIVATE STATE TOKENS API

# TECHNOLOGY OF DESIGN AND IMPLEMENTATION PROCESS OF THE PRIVATE STATE TOKENS API SUBSYSTEM

*Аннотация: В статье описывается процесс проектирования и реализации подсистемы анонимной аутентификации, основанной на протоколе Trust Tokens и API Private State Tokens. Представлены основные компоненты системы, включая генерацию криптографических ключей, выпуск и погашение анонимных токенов. Рассматриваются особенности интеграции с библиотекой OpenSSL, а также типы методов аутентификации, предусмотренные протоколом. Разработка направлена на обеспечение*

*конфиденциальности пользователей без использования традиционных идентификаторов, что особенно актуально в современных условиях защиты персональных данных.*

*The article presents the design and implementation of an anonymous authentication subsystem based on the Trust Tokens protocol and the Private State Tokens API. The main components of the system are described, including cryptographic key generation, token issuance, and redemption. The integration with the OpenSSL library is discussed, as well as the various authentication methods supported by the protocol. The development aims to ensure user privacy without relying on traditional identifiers, which is particularly relevant in today's data protection landscape.*

*Ключевые слова: анонимная аутентификация, Trust Tokens, Private State Tokens API, OpenSSL, криптография, конфиденциальность, безопасность, WebAuth, Privacy Sandbox.*

*Keywords: anonymous authentication, Trust Tokens, Private State Tokens API, OpenSSL, cryptography, privacy, security, WebAuth, Privacy Sandbox*

Современные веб-приложения сталкиваются с необходимостью предоставления персонализированного контента без нарушения конфиденциальности пользователя. Традиционные методы аутентификации, такие как cookie-файлы, fingerprinting или сторонние идентификаторы, всё чаще подвергаются критике за избыточное раскрытие информации о пользователе и отсутствие прозрачности. Эти подходы не соответствуют современным требованиям к приватности и становятся всё менее приемлемыми в условиях усиливающегося регулирования (например, GDPR, ePrivacy).

В этом контексте протокол Trust Tokens и API Private State Tokens, разработанные в рамках инициативы Privacy Sandbox, предлагают перспективный подход к анонимной аутентификации. Настоящая работа

посвящена разработке подсистемы, реализующей данный протокол в программной среде [1].

В основе архитектуры разрабатываемой подсистемы лежат несколько ключевых компонентов. Первый из них – механизм генерации криптографических ключей, который обеспечивает создание необходимых пар приватного и публичного ключей. Эти ключи в дальнейшем используются для выпуска и валидации анонимных токенов.

Криптографические методы инкапсулируются в специальной структуре, которая абстрагирует выбор конкретного алгоритма. На этапе инициализации разработчики определили перечисление, содержащее поддерживаемые типы методов, включая экспериментальные и производственные версии. В зависимости от выбранного типа инициализируется соответствующий объект, связанный с реализациями из криптографической библиотеки OpenSSL.

Вторым важным компонентом является объект-эмитент, отвечающий за выпуск и управление токенами. При его создании указывается допустимый размер пакета токенов (batch size), а также связывается ранее выбранный криптографический метод. Эмитенту назначается один или несколько публичных ключей, а также устанавливается ключ, используемый для шифрования служебных метаданных. Добавление ключей и установка параметров выполняются через специализированные методы интерфейса.

Процесс выпуска токенов начинается с получения от клиента запроса, который проходит валидацию. После этого на его основе формируются токены, подписываются приватным ключом и возвращаются клиенту. При последующем использовании клиент направляет токен обратно серверу, где происходит его погашение – проверка подлинности и извлечение анонимных аттрибутов. При этом не используются какие-либо персональные идентификаторы пользователя, такие как cookies или IP-адреса, что обеспечивает высокий уровень конфиденциальности.

Важным аспектом реализации является обработка ошибок, возникающих при инициализации методов, генерации ключей и работе с API. Для этого были заранее определены типовые исключения, сопровождающие каждую критическую операцию. Это позволило обеспечить устойчивость системы при сбоях на этапах криптографических вычислений и взаимодействия с внешними библиотеками [2].

Подсистема была успешно интегрирована в существующую инфраструктуру авторизации и продемонстрировала свою эффективность. Использование анонимных токенов позволило реализовать проверку подлинности без сохранения пользовательских идентификаторов, что значительно снижает риск нарушения конфиденциальности.

Таким образом, Trust Tokens и Private State Tokens API доказали свою состоятельность как технологическая база для построения защищённых и этичных механизмов идентификации в современных веб-приложениях.

**Использованные источники:**

1. Уайт Р. Криптография и безопасность в компьютерных сетях – Москва: 4-е издание, 2011. – 992 с.

2. Браун Э. Современные протоколы веб-безопасности – Санкт-Петербург: 4-е издание, 2019. – 416 с.