

А. В. Фоменко¹, Я. Ю. Зеленов¹

¹ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, Российская Федерация

ВОПРОСЫ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ В ДОМЕНЕ WINDOWS: ТОКЕНЫ

Аннотация. Рассматривается проблема повышения защищённости корпоративных информационных систем при помощи внедрения двухфакторной аутентификации (2FA) на основе аппаратного токена RuToken в доменной среде Windows. Отмечены ключевые уязвимости традиционной парольной аутентификации, фишинг, перехват паролей и ошибки пользователей. Исследуется архитектура на основе открытых ключей (PKI), где закрытый ключ остаётся только на физическом носителе, а открытый хранится на компьютере пользователя. Произведён сравнительный анализ нескольких методов авторизации пользователей такие как парольная аутентификация (Password-only), SMS / Email OTP (One-Time Password), TOTP (Time-based One-Time Password), FIDO2 / WebAuthn, RuToken + PKI в следствии чего были выявлены их уязвимости и преимущества. Основными критериями сравнения являются уязвимость к фишинговой и к MITM (Man-in-the-Middle) атаке, зависимость от интернет-соединения, возможность централизованного управления и сложность развёртывания. Особое внимание уделяется практическому внедрению RuToken + PKI в доменной среде без доступа к интернет-соединению. Показана настройка Active Directory Certificate Services (AD CS), групповых политик, шаблонов сертификатов, после которых возможен вход в учётную запись пользователя при помощи смарт карты в виде RuToken. При этом выявлены базовые неудобства использования данной архитектуры в доменной среде. Зависимость от криптодрайверов, риск потери физического носителя или PIN-кода и др. Эксперимент был проведён на базе Windows Server 2025 и Windows 11, развёрнутых на виртуальной машине Oracle VirtualBox. Результатом является демонстрация эффективности PKI-подхода в доменной среде по сравнению с классическими уровнями защиты

Ключевые слова: двухфакторная аутентификация, RuToken, инфраструктура открытых ключей (PKI), Active Directory Certificate Services (AD CS), Windows-домен, информационная безопасность

Введение

Основной целью кибератак в нынешнее время в основном являются корпоративные информационные системы из-за большого количества сотрудников в организации, именно компрометация пользовательских данных является главной проблемой при атаке. Привычная парольная аутентификация демонстрирует низкую устойчивость к различным векторам атак. Фишинг, перехват трафика и другим. Поэтому внедрение надёжной защиты учётных данных пользователей становится необходимостью в наше время. Для увеличения надёжности по всему миру развиваются двухфакторные аутентификации (2FA) при помощи различных решений, особенно актуально проблема в изолированных от интернета сетях, в которых невозможна интеграция с облачными сервисами.

Объектом исследования выступают информационные системы, построенные на базе доменной архитектуры Windows с централизованным управлением через Active Directory. Предметом исследования являются архитектурные особенности и эффективность реализации двухфакторной аутентификации на основе аппаратных токенов RuToken в условиях отсутствия интернет-соединения.

Целью работы является проведение сравнительного анализа методов двухфакторной аутентификации и обоснование лидерства PKI-подхода с использованием RuToken в offline доменных средах.

Проблема надёжной аутентификации широко освещена в нормативных и научных источниках. NIST SP 800-63B [1] формализует требования к многофакторной аутентификации и выделяет phishing-resistant методы — FIDO2/WebAuthn и PKI на основе аппаратных токенов. Однако стандарт ориентирован на современные облачные среды и не рассматривает особенности их применения в изолированных Windows-доменах. Для повышения надёжности идентификации пользователей и устройств, в компании Google разрабатывают схемы двухэтапного подтверждения прав доступа к аккаунту [7], основанные на одноразовых паролях и технологии открытого ключа. В российской практике ГОСТ Р 57580.1–2017 [4]

закладывает основу для использования PKI с аппаратным хранением ключей, а документация Microsoft [5] и компании «Aktiv» [2] подтверждает техническую возможность интеграции RuToken в Active Directory. Практическую значимость требований ГОСТ Р 57580.1–2017 подтверждает исследование Гнездилова [6], демонстрирующее снижение инцидентов безопасности при внедрении аппаратной двухфакторной аутентификации. Особое внимание в отечественных исследованиях уделяется в работе Грекова В.С. и Уймина А.Г. [3] по созданию учебно-тренировочных сред.

Методология и критерии сравнения

Для оценки эффективности различных подходов к реализации двухфакторной аутентификации в условиях изолированной Windows-доменной среды был применён сравнительный анализ, основанный на шести ключевых критериях. В исследовании рассматриваются пять наиболее распространённых методов: парольная аутентификация, одноразовые пароли по SMS или электронной почте, временные одноразовые пароли (TOTP), FIDO2/WebAuthn и PKI-аутентификация на основе аппаратного токена RuToken. Выбор именно этих методов обусловлен их широким использованием в корпоративной среде, и различиями в архитектуре, что позволяет выявить сильные и слабые стороны каждого подхода.

Одним из основных критериев является устойчивость к фишинговой атаке. Фишинг-атаки остаются главным вектором компрометации учётных данных, поскольку пользователи вводят свои реквизиты на поддельных сайтах. Метод может считаться устойчивым к фишингу, только если злоумышленник не может повторно использовать полученные данные. Парольные и OTP-методы уязвимы, так как передаваемый ключ не привязан к домену. В отличие от них, FIDO2 и PKI на основе аппаратных токенов генерируют криптографическую подпись, привязанную к конкретному домену, что делает её бесполезной вне легитимного контекста.

Следующий и не наиболее важный критерий сравнения является защита от атак типа «человек посередине» (MITM). При перехвате сетевого трафика методы, передающие ключ в открытом виде или в виде динамического кода, теряют свою безопасность, особенно если используется незащищённое TLS-соединение. PKI и FIDO2 устойчивы к таким атакам, поскольку закрытый ключ никогда не покидает устройство, а протокол аутентификации основан на запрос-ответ механизме, гарантирующем уникальность каждого подключения.

В условиях изолированных сетей организаций, которые имеют зависимость от интернета и внешних сервисов. Такие решения, как SMS/Email OTP или облачные TOTP-сервисы, требуют постоянного подключения к внешним ресурсам, что делает их неприменимыми в изолированных от интернета сетях. Однако RuToken + PKI или локальный TOTP могут функционировать полностью автономно, что обеспечивает их жизнеспособность в offline-инфраструктуре.

Централизованное управление представляет собой критически важный критерий для корпоративных систем. Возможность настройки политик, отзыва доступа и принудительного применения правил через Active Directory является важным требованием в корпоративных средах. В нашем случае только парольная аутентификация и PKI на базе AD CS обеспечивают полную интеграцию с групповыми политиками и механизмами управления доменом. FIDO2, несмотря на высокую безопасность, в чистой Windows-доменной среде без Azure AD или сторонних систем не поддерживает аналогичного уровня централизации. Сложность развёртывания аутентификации имеет не менее главную роль в выборе метода. Парольная аутентификация требует минимальных усилий, тогда как внедрение PKI или FIDO2 предполагает настройку дополнительных компонентов, таких как центров сертификации, шаблонов, криптопровайдеров и политик безопасности. Несмотря на повышенную сложность развёртывания самого метода, это гарантия высокой степени защиты вашей системы.

Основным фактором безопасности является место и способ хранения закрытого ключа. Если ключ может быть извлечён из устройства в TOTP-приложениях, то система является уязвимой для атаки со стороны злоумышленника. В RuToken и FIDO2 закрытый ключ

Рубрика 2. Методы и системы защиты информации, информационная безопасность

генерируется и хранится в аппаратном защищённом элементе и является невыгружаемым, что соответствует требованиям современных стандартов.

Для количественной оценки эффективности методов была проведена оценка трудоёмкости внедрения и замер времени аутентификации в ходе эксперимента. Результаты сведены в таблицу 1.

Таблица 1 – Сравнительная оценка методов аутентификации

Метод	Время внедрения	Время входа	Стоимость внедрения	Риск отказа
Password-only	0 ч	3–5 сек	Бесплатно	Низкий (забывание пароля)
SMS/Email OTP	4–8 ч	15–30 сек	Средняя	Средний (задержки сети)
TOTP (App)	2–4 ч	10–15 сек	Бесплатно	Средний (рассинхронизация)
FIDO2/WebAuthn	8–12 ч	5–7 сек	Высокая	Низкий
RuToken + PKI	12–16 ч (AD CS + драйверы)	8–12 сек	Высокая	Низкий (ошибка PIN)

Экспериментальная часть

Сеть, состоящая из двух, устройств на основе Windows Server 2025 и Windows 11 является полностью изолированной от глобальной сети интернет. Перед началом исследования устанавливаем необходимое программное обеспечение для корректной работы RuToken. Для этого через официальный сайт скачиваем драйвер поддержки Рутокена 2.0, устанавливаем на обе машины.

Установка и настройка операционных систем на машины. На машине DC создаём домен, настраиваем сеть, устанавливаем AD CS, DNS. В домен вводим машину CLI, устанавливаем необходимое ПО для работы Рутокена (драйвер и криптосервис) на обе машины, без этой установки машины будут воспринимать токен как обычную флешку

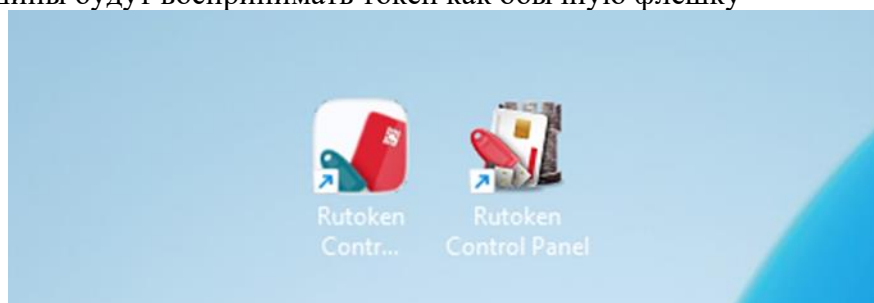


Рис. 1. ПО для Рутокена

Устанавливаем AD CS на машину DC с выбором типа Enterprise Root CA, обеспечивающего интеграцию с Active Directory и автоматическое распространение корневого сертификата на компьютеры домена. После установки выполнили начальную конфигурацию центра сертификации

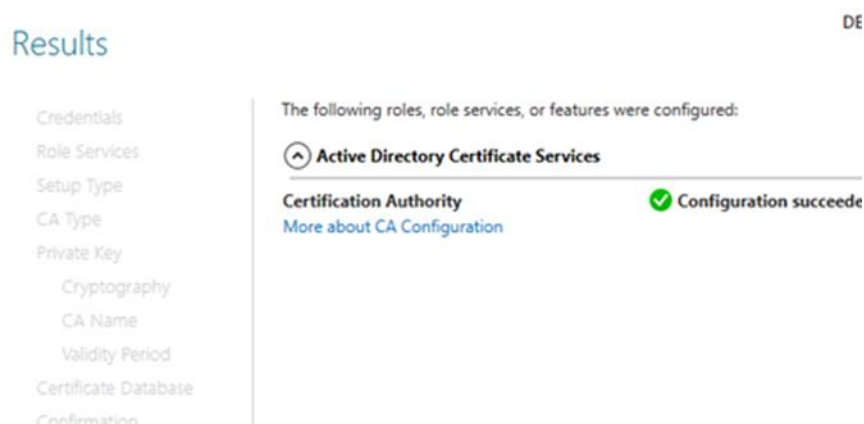


Рис. 2. Добавление AD CS

Создание и публикация пользовательского шаблон сертификата на основе стандартного шаблона «Smart Card User» под названием «Rutoken_Logon» с предоставленными разрешениями Enroll, Autoenroll. Важным этапом конфигурирования шаблона Rutoken_Logon

является настройка криптографических параметров на вкладке Cryptography. В поле Cryptography Service Provider выбран поставщик, соответствующий установленному драйверу Рутокен Aktiv Co. RuToken CSP для CAPI-совместимых приложений, что гарантирует генерацию закрытого ключа непосредственно в защищённой памяти аппаратного носителя и исключает возможность его экспорта в программное хранилище. Минимальная длина ключа установлена на уровне 2048 бит, алгоритм хеширования — SHA-256, что соответствует требованиям ГОСТ Р 57580.1–2017 [4] к стойкости ключевой информации в инфраструктуре открытых ключей. Дополнительно активирована опция Request must use a specific provider, исключающая выпуск сертификата с ключом, сгенерированным сторонним криптопровайдером. Данные настройки обеспечивают выполнение ключевого требования безопасной архитектуры PKI: закрытый ключ никогда не покидает аппаратный токен, а все криптографические операции выполняются внутри защищённого элемента Рутокен.

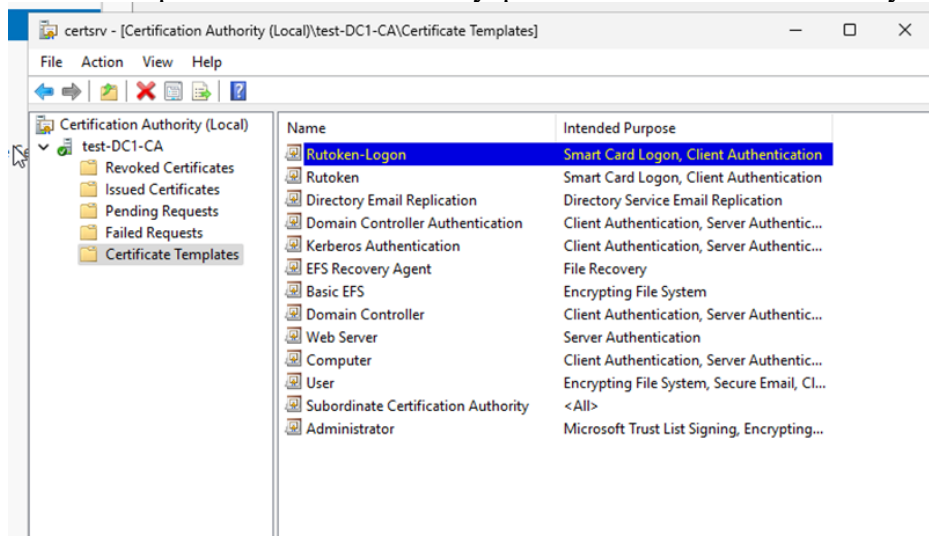


Рис. 3. Создание Rutoken_Logon

Для выпуска сертификатов пользователям домена, на клиентской машине через консоль MMC → Certificates (Current User) был запущен мастер Certificate Enrollment. Выбран целевой шаблон и инициирован запрос сертификата. После вставки токена и ввода PIN-кода, закрытый ключ создавался непосредственно на смарт-карте (токене), а полученный сертификат автоматически установился в соответствующее устройство. При успешной регистрации сертификат появлялся в хранилище Personal → Certificates, где можно было убедиться в наличии критических атрибутов «Smart Card Logon» и «Client Authentication»

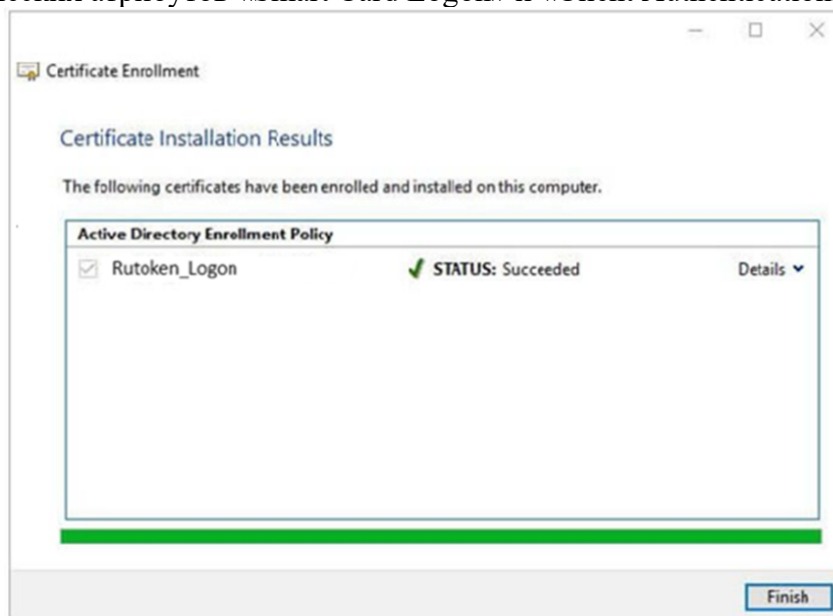


Рис. 4. Выпуск сертификатов Rutoken_Logon

Рубрика 2. Методы и системы защиты информации, информационная безопасность

После настройки групповых политик для пользователя домена при входе на CLI требуется вводить не только пароль, но также обязательным требованием является владение токеном, зарегистрированным на DC (контроллере домена)

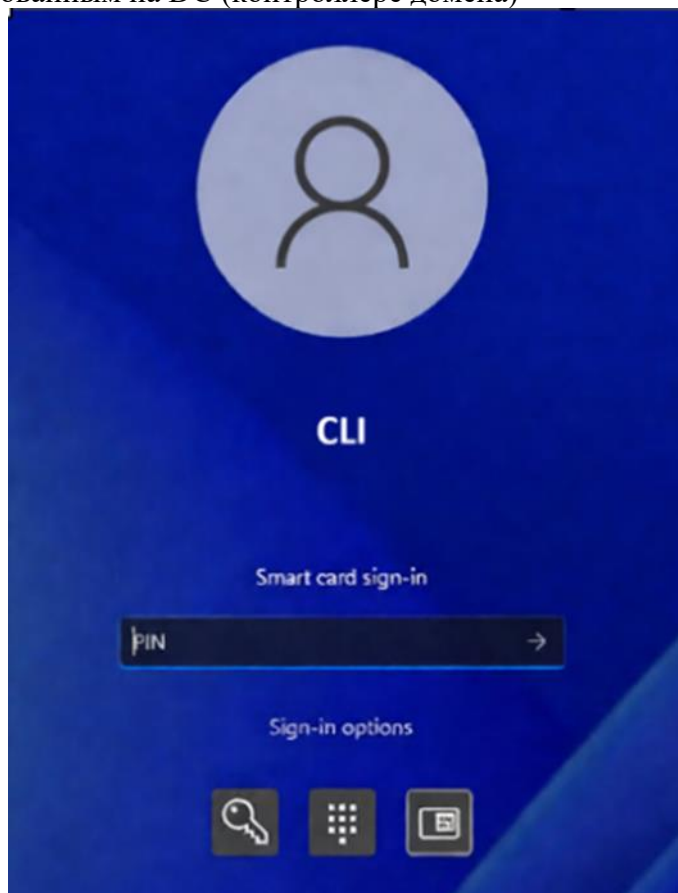


Рис. 5. Выпуск сертификатов Rutoken_Logon

Заключение

Таким образом анализ методов двухфакторной аутентификации показал, что в условиях изолированной Windows-доменной среде без доступа к интернет-соединению наиболее эффективным и безопасным решением является PKI-подход на основе аппаратного токена RuToken. В отличие от OTP-методов, уязвимых к фишингу и MITM-атакам, и FIDO2, RuToken обеспечивает высокий уровень защиты за счёт хранения невыгружаемого закрытого ключа на устройстве, полной совместимости с Active Directory и независимости от внешних сервисов. Экспериментальная верификация на основе Windows Server 2025 и Windows 11 подтвердила работоспособность решения, несмотря на операционные ограничения, связанные со сложностью развёртывания и зависимостью от криптодрайверов. В случаях, где приоритетом являются безопасность и возможность централизованного управления, данный подход представляет собой наиболее верное и практически применимое решение для защищённых информационных систем.

Библиографический список

1. NIST Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management [Electronic resource] (Специальная публикация NIST 800-63B Руководство по цифровой идентификации Аутентификация и управление жизненным циклом) // NIST Pages : official website. – Gaithersburg, 2020. – URL: <https://pages.nist.gov/800-63-3/sp800-63b.html> (date of access: 02.01.2026).
2. АО «Актив». РутOKEN : документация для разработчиков и администраторов [Электронный ресурс] // РутOKEN.ru : официальный сайт. – Москва. – URL: <https://dev.rutoken.ru> (дата обращения: 02.01.2026).
3. Греков, В. С., Уймин А. Г. Стратегии создания модели сети предприятия в рамках киберполигона для эффективной подготовки кадров в области кибербезопасности //

- Вестник кибербезопасности. – 2024. – № 3. – С. 45–58. // eLibrary.ru : научная электронная библиотека. – URL: <https://www.elibrary.ru/item.asp?id=80499001> (дата обращения: 04.01.2026).
4. ГОСТ Р 57580.1–2017. Информационная технология. Криптографическая защита информации. Инфраструктура открытых ключей: национальный стандарт Российской Федерации [Электронный ресурс]. – Москва: Стандартинформ, 2017. – URL: <https://regulhub.kaspersky.ru/upload/iblock/71a/k99732yk7w1rrz8d3yg3y4hwqzmg8bcw.pdf> (дата обращения: 04.01.2026).
 5. Smart Card Logon Architecture [Electronic resource] // Microsoft Learn : official documentation portal. – Redmond, 2025. – URL: <https://learn.microsoft.com/en-us/windows/security/identity-protection/smart-cards/smart-card-architecture> (date of access: 05.01.2026).
 6. Гнездилов, Р. Р. Многофакторная аутентификация и эффективность обеспечения безопасности информации при доступе к ресурсам телекоммуникационных сетей / Р. Р. Гнездилов // Гагаринские чтения - 2018 : Сборник тезисов докладов XLIV Международной молодёжной научной конференции, Москва-Ахтубинск-Байконур, 17–20 апреля 2018 года. Том 1. – Москва-Ахтубинск-Байконур: Московский авиационный институт (национальный исследовательский университет), 2018. – С. 193. – EDN XMKQST.
 7. Гроссе, Э. Многофакторная аутентификация / Э. Гроссе, М. Упадхаяй // Информационная безопасность. – 2013. – № 4. – С. 42–47. EDN: SDXTOH

References

1. NIST Special Publication 800-63B. (2020). Digital Identity Guidelines: Authentication and Lifecycle Management. National Institute of Standards and Technology, Gaithersburg. URL: <https://pages.nist.gov/800-63-3/sp800-63b.html> (date of access: 02.01.2026).
2. Aktiv JSC. Rutoken: Documentation for developers and administrators [Electronic resource]. Rutoken.ru: official website. Moscow. URL: <https://dev.rutoken.ru> (date of access: 02.01.2026).
3. Grekov, V. S., & Uymin, A. G. (2024). Strategies for creating an enterprise network model within a cyber range for effective cybersecurity personnel training. Vestnik kiberbezopasnosti, (3), 45–58. URL: <https://www.elibrary.ru/item.asp?id=80499001> (date of access: 04.01.2026).
4. GOST R 57580.1–2017. (2017). Information technology. Cryptographic information protection. Public key infrastructure: National standard of the Russian Federation. Moscow: Standartinform. URL: <https://regulhub.kaspersky.ru/upload/iblock/71a/k99732yk7w1rrz8d3yg3y4hwqzmg8bcw.pdf> (date of access: 04.01.2026).
5. Smart Card Logon Architecture [Electronic resource]. (2025). Microsoft Learn: official documentation portal. Redmond. URL: <https://learn.microsoft.com/en-us/windows/security/identity-protection/smart-cards/smart-card-architecture> (date of access: 05.01.2026).
6. Gnezdilov, R. R. (2018). Multifactor authentication and the efficiency of information security when accessing telecommunication network resources. In Gagarin Readings – 2018: Proceedings of the XLIV International Youth Scientific Conference, Moscow–Akhtubinsk–Baikonur, April 17–20, 2018 (Vol. 1, p. 193). Moscow–Akhtubinsk–Baikonur: Moscow Aviation Institute (National Research University). EDN XMKQST.
7. Grosse, E., & Upadhyay, M. (2013). Multifactor authentication. Informationsnaya bezopasnost, (4), 42–47. EDN SDXTOH.

Информация об авторах

Фоменко Артём Владимирович — студент 3-его курса, факультет КБ ТЭК, группы КИ-23-01 ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: 1studentnow1@gmail.com

Зеленов Ярослав Юрьевич — студент 3-его курса, факультет КБ ТЭК группы КИ-23-01 ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: mobzila567@gmail.com

Рубрика 2. Методы и системы защиты информации, информационная безопасность

TWO-FACTOR AUTHENTICATION ISSUES IN THE WINDOWS DOMAIN: TOKENS

Fomenko A. V.¹, Zelenov Ya. Yu.¹

¹National University of Oil and Gas «Gubkin University», Moscow, Russian Federation

Abstract. *This article examines the problem of increasing the security of corporate information systems by implementing two-factor authentication (2FA) based on the RuToken hardware token in a Windows domain environment. Key vulnerabilities of traditional password authentication, phishing, password interception, and user errors are highlighted. A public key infrastructure (PKI) architecture is explored, where the private key remains only on the physical medium, and the public key is stored on the user's computer. A comparative analysis of several user authorization methods, such as password authentication (Password-only), SMS / Email OTP (One-Time Password), TOTP (Time-based One-Time Password), FIDO2 / WebAuthn, and RuToken + PKI, is conducted, as a result of which their vulnerabilities and advantages are identified. The main comparison criteria are vulnerability to phishing and MITM (Man-in-the-Middle) attacks, dependence on an internet connection, the possibility of centralized management, and the complexity of deployment. Particular attention is given to the practical implementation of RuToken + PKI in a domain environment without internet access. The article demonstrates the configuration of Active Directory Certificate Services (AD CS), group policies, and certificate templates, which enable user account login using a RuToken smart card. The article identifies the challenges of using this architecture in a domain environment, including dependence on cryptographic drivers, the risk of losing the physical drive or PIN, and more. The experiment was conducted using Windows Server 2025 and Windows 11, deployed on an Oracle VirtualBox virtual machine. The result demonstrates the effectiveness of the PKI approach in a domain environment compared to traditional security levels.*

Keywords: *two-factor authentication, RuToken, public key infrastructure (PKI), Active Directory Certificate Services (AD CS), Windows domain, information security*

Information about the authors

Artem Vladimirovich Fomenko, third-year student, Faculty of Design Bureau of Fuel and Energy Complex, group KI-23-01, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: 1studentnow1@gmail.com

Yaroslav Yuryevich Zelenov, third-year student, Faculty of Design Bureau of Fuel and Energy Complex, group KI-23-01, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: mobzila567@gmail.com