Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Passkey в офисе: убираем пароли для 60 сотрудников

Наша методология passwordless: Keycloak 26.6, FIDO2-токены, WHfB, PIV-логон, 1С через OIDC

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Пароль остаётся единственным барьером к почте, банк-клиенту и 1С: фишинговая копия домена, подстановка кредов из старых утечек, стикер с «Winter2026!» на мониторе. Мы убираем сам секрет: подпись WebAuthn считается только для своего RP ID и origin, приватный ключ не покидает TPM или токен, вместо ввода пароля — локальное подтверждение PIN или биометрией.

Почему это важно бизнесу

- Фишинг перестаёт работать: браузер отдаёт подпись только своему RP ID, поддельный домен ответа от ключа не получит.
- Сброс паролей уходит из работы админа: нет «забыл пароль» — нет блокировок УЗ и простоя бухгалтерии в день сдачи отчётности.
- Вход одним касанием вместо пароля и кода TOTP: на 60 сотрудниках это десятки минут рабочего времени в день по нашим замерам.
- Утечка базы IdP теряет смысл: на сервере только публичный ключ и AAGUID, приватный ключ не покидает TPM или токен.
- Аудит доказуем: в УЗ виден AAGUID и метка каждого ключа, событие входа фиксирует, каким credential вошёл сотрудник.

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

26.4

Passkeys в Keycloak официально поддержаны с 26.4.0; с 23.0.0 это было preview

keycloak.org, Release Notes 26.4 (2025)

100

Discoverable credentials на токен: 100 на прошивке 5.7 против 25 на 5.5/5.6

docs.yubico.com, YubiKey Tech Manual, fw 5.7

8

Минимальный FIDO2-PIN на прошивке 5.7 — 8 символов; в WHfB без политики хватает 6

docs.yubico.com, FIDO Specifics, fw 5.7

direct

Attestation Conveyance = direct плюс Acceptable AAGUIDs: в контур входят только наши модели

keycloak.org, Server Administration Guide

09.2025

С обновлений 09.2025 StrongCertificateBindingEnforcement не поддерживается — KDC в Enforcement

support.microsoft.com, KB5014754

24H2

С Windows 11 24H2 при включённом VBS параметры PIN Expiration и History не работают

learn.microsoft.com, WHfB policy settings

РЕАЛИЗАЦИЯ 1 ИЗ 3

IdP: Keycloak как единая точка входа

Что настраиваем

Keycloak 26.6.4 в Docker за nginx, realm corp, ~60 УЗ из AD через LDAP-федерацию с Edit mode = READ_ONLY

Как мы это делаем

1. Authentication → Policies → Webauthn Passwordless Policy: Relying Party ID = корневой домен, Discoverable credential = required, User Verification = required.
2. Там же Attestation Conveyance = direct, Acceptable AAGUIDs — только закупленные модели, Avoid Same Authenticator Registration = On, Create Timeout = 60.
3. Attestation проверяется лишь при наличии сертификатов вендора в truststore Keycloak (conf/truststores, --truststore-paths), иначе регистрация падает.
4. Passkeys включаем в той же политике, в browser flow добавляем authenticator «Conditional - credential», пароль из основного flow убираем.
5. Realm settings → Events: Save events = On, Expiration = 90 дней, admin events с representation, listener jboss-logging → stdout → SIEM; Brute force detection = On.

РЕЗУЛЬТАТ

Все OIDC/SAML-приложения (вики, helpdesk, VPN, файловое облако) пускают по ключу и не держат собственных паролей. Пароль остаётся только у break-glass-учётки в сейфе, и любой её вход даёт алерт в SIEM.

КЛЮЧЕВОЙ НЮАНС

Смена RP ID обнуляет все ключи: фиксируем его на неизменном корневом домене, а поддомены и мобильные клиенты добавляем в Extra Origins, иначе нужна перерегистрация.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Рабочие станции: WHfB и PIV-логон по токену

Что настраиваем

Windows 11 24H2 в домене AD, GPO ITF-WHfB с фильтром по security-группе, шаблон Smartcard Logon на нашем CA

Как мы это делаем

1. Computer Configuration → Administrative Templates → Windows Components → Windows Hello for Business: Use Windows Hello for Business = Enabled.
2. Там же Use a hardware security device = Enabled с исключением TPM 1.2: машины без TPM 2.0 не провижинятся и уходят в отдельный список.
3. System → PIN Complexity: Minimum PIN length = 8, Expiration = 0, History = 0 — с 24H2 при VBS эти два параметра всё равно не применяются.
4. Токен как смарт-карта: шаблон Smartcard Logon (EKU 1.3.6.1.4.1.311.20.2.2), сертификат в PIV-слоте 9a, ключ генерируется на токене, minidriver на клиенте.
5. Сертификаты выпускаем с SID-расширением 1.3.6.1.4.1.311.25.2: KDC работает только в Full Enforcement и слабые сопоставления отклоняет.

РЕЗУЛЬТАТ

Вход в ОС — PIN, отпечаток или касание токена. В RDP-сессии WebAuthn-запросы уходят на локальный токен (redirectwebauthn:i:1 плюс GPO «Do not allow WebAuthn redirection» = Disabled), поэтому веб-сервисы в терминале логинятся тем же ключом.

КЛЮЧЕВОЙ НЮАНС

Сначала инвентаризация TPM и сборок, потом раскатка: машины без TPM 2.0 и на EOL-сборках выпадают из WHfB, для них остаётся только логон по токену как по смарт-карте.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Legacy и 1С: не оставляем пароли «как есть»

Что настраиваем

1С:Предприятие 8.3.27, RDS-фермы, SMB- и FTP-шары, банк-клиент на КриптоПро, админ-доступ по SSH

Как мы это делаем

1. 1С: аутентификация OpenID Connect настраивается в default.vrd, ключ сопоставления — e-mail пользователя ИБ (КлючиСопоставленияПользователя), провайдер Keycloak.
2. После перехода на 8.3.25+ обязательно ТиИ с пунктом «Прочее»: без него нет индексов под сопоставление по e-mail и вход по токену тормозит.
3. Что не умеет OIDC — за nginx auth_request с oauth2-proxy: бэкенд отвечает только после passkey-сессии в realm.
4. SSH: ключи ed25519-sk, созданные ssh-keygen -O resident -O verify-required; в sshd PasswordAuthentication no и KbdInteractiveAuthentication no.
5. Банк-клиент и КриптоПро оставляем на своей схеме: доступ по IP-whitelist и VPN, вход в который уже по ключу; пароли в менеджере, разлочка passkey.

РЕЗУЛЬТАТ

Пароль как фактор остаётся только там, где его физически нельзя убрать, и всегда за двумя контурами: сетевым (VPN плюс whitelist) и сессией IdP на ключе. Число парольных точек входа держим в реестре и сокращаем на каждом квартальном аудите.

КЛЮЧЕВОЙ НЮАНС

Инвентаризация приложений важнее закупки токенов: сначала перечень «умеет OIDC/SAML — закрывается прокси — остаётся на пароле», иначе на середине проекта находится сервис с целым парольным контуром.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **RP ID выбран по поддомену**
  Смена или переезд поддомена = все passkey недействительны. RP ID фиксируем на корневом домене, поддомены вносим в Extra Origins.

- ✕ **Один ключ на сотрудника**
  Потеря = остановка работы и очное восстановление. Выдаём два ключа, регистрируем оба в день выдачи, резервный храним в сейфе.

- ✕ **Attestation включён, а truststore пуст**
  Без direct список Acceptable AAGUIDs не проверяется, а с direct без сертификатов вендора в conf/truststores регистрация ключа падает.

- ✕ **Синхронизируемые passkey**
  Ключ уезжает в личный аккаунт и живёт после увольнения. Требуем device-bound: attestation плюс фильтр по AAGUID в политике realm.

- ✕ **Забыли про break-glass**
  IdP недоступен, пароли выключены — входа нет. Держим офлайн-учётку с длинным паролем в сейфе и алерт в SIEM на её использование.

- ✕ **Сертификаты без SID-расширения**
  KDC уже в Full Enforcement: без 1.3.6.1.4.1.311.25.2 или strong-мэппинга в altSecurityIdentities логон по токену отклоняется.

- ✕ **PIN-ротация как у паролей**
  С Windows 11 24H2 при VBS Expiration и History не применяются — политика молча не работает. Ставим 0 и растим длину PIN до 8.

- ✕ **Нет логирования регистраций**
  Регистрация нового ключа — критичное событие. Пишем admin events realm в SIEM и разбираем каждую внеплановую регистрацию passkey.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Passkey вторым фактором для почты, VPN и админ-панелей, пароль пока остаётся
- По два FIDO2-токена на сотрудника, оба зарегистрированы в день выдачи
- PIN не короче 8 символов, TOTP оставляем только как аварийный резерв
- События входа IdP хранятся 90 дней и выгружаются в SIEM

НОРМАЛЬНО

- Keycloak 26.4+: Webauthn Passwordless Policy, пароль убран из основного flow
- WHfB на всех ПК с TPM 2.0, GPO нацелен фильтром по security-группе
- Attestation = direct, Acceptable AAGUIDs — только корпоративные модели
- sshd без пароля: ed25519-sk с -O resident -O verify-required

ХОРОШО

- Внутренние сервисы за OIDC/SAML, legacy — за nginx auth_request и oauth2-proxy
- PIV-логон в Windows, сертификаты с SID-расширением, KDC в Full Enforcement
- redirectwebauthn:i:1 в RDP, чтобы в терминале работал тот же токен
- Квартальный аудит: два ключа на человека, отзыв в день увольнения

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] RP ID зафиксирован на корневом домене, поддомены и мобильные клиенты внесены в Extra Origins?
- [ ] Discoverable credential = required и User Verification = required в Webauthn Passwordless Policy?
- [ ] Attestation = direct, список AAGUID ограничен, сертификаты вендора лежат в truststore Keycloak?
- [ ] У каждого сотрудника два ключа, резервный хранится отдельно от рабочего?
- [ ] Пароль убран из основного browser flow, а не просто «не используется» сотрудниками?
- [ ] Есть офлайн break-glass-учётка, доступ к /admin по IP-allow-list и алерт в SIEM?
- [ ] TPM 2.0 проверен на всех ПК, GPO WHfB нацелен фильтром по security-группе?
- [ ] Выдаваемые сертификаты содержат SID-расширение 1.3.6.1.4.1.311.25.2?
- [ ] Регистрация и отзыв passkey логируются и разбираются как инцидент?
- [ ] Описан порядок при потере ключа: отзыв, временный доступ, срок выдачи нового?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Инвентаризируем приложения: что уходит на OIDC/SAML, что через прокси, что остаётся на пароле.
- Разворачиваем Keycloak 26.4+: Webauthn Passwordless Policy, LDAP-федерация из AD, события в SIEM.
- Готовим GPO WHfB и PIV-логон: аудит TPM, шаблон Smartcard Logon, SID-расширение в сертификатах.
- Выдаём и регистрируем по два токена на человека, обучаем микрогруппами, ведём реестр серийников.
- На абонентке: отзыв при увольнении, замена при потере, обновления IdP, квартальный аудит выдачи.

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 Server Administration Guide — WebAuthn, attestation, Passkeys (keycloak.org — 26.x)

02 Release Notes 26.4 — поддержка passkeys и Conditional UI (keycloak.org — 2025)

03 Windows Hello for Business policy settings (learn.microsoft.com — 2026)

04 KB5014754 — certificate-based authentication на DC (support.microsoft.com — 2025)

05 Configure WebAuthn redirection over RDP (learn.microsoft.com — 2026)

06 YubiKey Technical Manual — FIDO Specifics, firmware 5.7 (docs.yubico.com — 5.7)

07 ssh-keygen(1) — FIDO-ключи, resident и verify-required (man.openbsd.org — 2026)

08 OpenID Connect аутентификация платформы 1С (v8.1c.ru — 8.3.27)

09 Web Authentication (WebAuthn) Level 3 (w3.org — 2025)

Основано на официальной документации продуктов и нашей практике внедрения.