Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Корпоративный PKI на AD CS: двухуровневый ЦС без сюрпризов

Offline Root CA + Enterprise Issuing CA: шаблоны, автоэнроллмент, отзыв и защита от эскалаций

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Внутренние сервисы (1С веб-клиент, порталы, RDS) живут на самоподписанных сертификатах, Wi-Fi — на общем пароле, VPN — на логине. Уволенный сотрудник сохраняет доступ, браузеры пугают пользователей, а единственный онлайн Enterprise Root CA — точка полной компрометации домена. Мы разворачиваем двухуровневый PKI на AD CS: офлайн-корень, автоэнроллмент, управляемый отзыв.

Почему это важно бизнесу

- Общий Wi-Fi/VPN-пароль не отзывается при увольнении — бывший сотрудник заходит в сеть месяцами
- Компрометация онлайн корневого ключа = переустановка доверия на всех машинах и простой сервисов
- Коммерческие сертификаты на 10+ внутренних имён — постоянные расходы, свой CA входит в Windows Server
- Просроченный сертификат Issuing CA кладёт разом 802.1X, VPN и HTTPS — авария на весь офис
- Красные предупреждения браузера приучают людей нажимать «Продолжить» — фишинг проходит без сопротивления

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

RSA 4096

Ключ офлайн Root CA, SHA-256, срок сертификата 20 лет — перевыпуск корня раз в десятилетие

наш стандарт, KSP Windows Server

26 нед.

CRLPeriod офлайн-корня + CRLOverlap 4 недели: включаем Root-виртуалку дважды в год только ради…

по докам AD CS (certutil -setreg)

8 ч

Внутренний таймер автоэнроллмента (плюс старт/логон); при внедрении форсируем certutil -pulse,…

по докам Microsoft, autoenrollment

80%

Порог автопродления: клиент перевыпускает сертификат по достижении 80% срока — «протухания» на…

по докам Microsoft, autoenrollment

Full

Enforcement KB5014754 на DC: только сертификаты с SID-расширением; с 09.2025 откат в Compatibi…

KB5014754, enforcement с 02.2025

1 нед.+1 д.

Base CRL и Delta CRL на Issuing CA — быстрый отзыв без ручной публикации; плюс OCSP для 802.1X

наш стандарт для Issuing CA

РЕАЛИЗАЦИЯ 1 ИЗ 3

Офлайн Root CA и публикация цепочки доверия

Что настраиваем

Изолированная ВМ вне домена (Hyper-V/ESXi), Windows Server 2022/2025 Standard, роль ADCS-Cert-Authority

Как мы это делаем

1. Готовим CAPolicy.inf (RenewalKeyLength=4096, отключаем default CDP/AIA в корневом сертификате), ставим роль: Install-AdcsCertificationAuthority -CAType StandaloneRo…
2. Криптография параметрами командлета: -CryptoProviderName "RSA#Microsoft Software Key Storage Provider" -KeyLength 4096 -HashAlgorithmName SHA256 -ValidityPeriod Yea…
3. certutil -setreg ca\CRLPeriod "Weeks" + CRLPeriodUnits 26, CRLOverlapPeriodUnits 4, CRLDeltaPeriodUnits 0, ValidityPeriodUnits 10 (Years) — рестарт certsvc, certuti…
4. Публикуем корень с доменной станции: certutil -dspublish -f RootCA.crt RootCA плюс корневой CRL — клиенты забирают доверие из AD-контейнера автоматически, без ручно…
5. Отключаем vNIC, гасим ВМ, экспорт образа в офлайн-хранилище; в календарь эксплуатации — включение раз в 26 недель на публикацию CRL

РЕЗУЛЬТАТ

Корневой ключ физически недосягаем из сети: компрометация любого онлайн-узла не рушит иерархию. Отзыв скомпрометированного Issuing CA — штатная операция корнем, а не перестройка доверия на всех машинах и устройствах.

КЛЮЧЕВОЙ НЮАНС

CRLPeriodUnits корня обязан переживать интервал включений машины с запасом (overlap 4 недели), иначе просроченный корневой CRL молча валит проверку цепочки у всех клиентов разом.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Issuing CA, шаблоны и автоэнроллмент через GPO

Что настраиваем

Доменный Windows Server 2022/2025, роли ADCS-Cert-Authority + ADCS-Web-Enrollment, вся выдача конечных сертификатов

Как мы это делаем

1. Install-AdcsCertificationAuthority -CAType EnterpriseSubordinateCA → CSR на флешке подписываем корнем (certreq -submit / -retrieve), certutil -installCert
2. Встроенные шаблоны не публикуем: в certtmpl.msc дублируем Computer/User/Web Server в свои V2+ (ITF-Computer 2 года, ITF-User 1 год), криптопровайдер KSP, SHA256
3. Security шаблонов: точечные группы с Read+Enroll+Autoenroll; Autoenroll — только на шаблоны массового автовыпуска, Web Server выдаём по Enroll с одобрением
4. GPO «PKI-Autoenrollment» на OU: Public Key Policies → Certificate Services Client — Auto-Enrollment = Enabled, обе галки renew/update; проверка: gpupdate /force + c…
5. Публикация шаблона на CA: Add-CATemplate -Name "ITF-Computer"; контроль выдачи — certutil -store My и журнал CertificateServicesClient-Lifecycle-System/Operational

РЕЗУЛЬТАТ

Сертификаты на компьютеры и пользователей выпускаются и продлеваются без участия инженера: новая машина в домене получает сертификат в первый 8-часовой цикл, продление на 80% срока исключает массовые «протухания» парка.

КЛЮЧЕВОЙ НЮАНС

Автоэнроллмент — это три условия одновременно: права Autoenroll на шаблоне, шаблон опубликован на CA, GPO включена на правильной OU. Отсутствие любого из трёх — тихий отказ без ошибок на клиенте.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Отзыв, CDP/OCSP и защита CA от эскалации привилегий

Что настраиваем

Issuing CA + IIS-узел pki.<домен> для CDP/AIA, Online Responder, контроллеры домена (strong mapping)

Как мы это делаем

1. CRLPublicationURLs/CACertPublicationURLs: первым HTTP (http://pki.corp…/CertEnroll/), вторым LDAP — недоменные и мобильные клиенты достают CRL без LDAP
2. Issuing CA: Base CRL 1 неделя + Delta 1 день; для Wi-Fi/VPN поднимаем Online Responder (ADCS-Online-Cert) — ревокация видна за минуты, не за сутки
3. Проверяем и держим выключенным флаг EDITF_ATTRIBUTESUBJECTALTNAME2 (certutil -getreg policy\EditFlags) — иначе любой заявитель дописывает чужой UPN в SAN
4. Включаем аудит CA: certutil -setreg CA\AuditFilter 127 + Object Access в GPO; на DC подтверждаем Full Enforcement (StrongCertificateBindingEnforcement=2), ловим соб…
5. Регламент: certutil -revoke <serial> при увольнении в день отключения учётки → certutil -crl; еженедельный Backup-CARoleService -Path … -Password в защищённое храни…

РЕЗУЛЬТАТ

Отзыв реально работает: уволенный не проходит EAP-TLS уже после ближайшей публикации Delta CRL/ответа OCSP. CA перестаёт быть каналом эскалации до администратора домена, а восстановление после сбоя — из свежего бэкапа ключей и базы.

КЛЮЧЕВОЙ НЮАНС

pkiview.msc — первый инструмент диагностики: он показывает просроченные CRL и битые CDP/AIA по всей иерархии до того, как пользователи начнут жаловаться на «неработающий Wi-Fi».

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Enterprise Root CA онлайн в домене**
  Одноуровневая схема ставится за час, но корневой ключ живёт на доменном сервере. Мы строим только двухуровневую: Standalone-корень офлайн, выдаёт лиш…
- ✕ **Включён EDITF_ATTRIBUTESUBJECTALTNAME2**
  Флаг разрешает заявителю дописать произвольный SAN (чужой UPN) в любой запрос. Проверяем certutil -getreg policy\EditFlags и держим бит выключенным;…
- ✕ **«Supply in the request» + Client Authentica…**
  Шаблон с subject от заявителя и EKU аутентификации — выпуск сертификата за любого пользователя. Subject строим из AD; где ручной subject неизбежен —…
- ✕ **Короткий CRL у офлайн-корня**
  CRLPeriod 1 неделя заставляет включать изолированную машину еженедельно — её перестают включать, CRL истекает, цепочка падает у всех. Закладываем 26…
- ✕ **CDP только LDAP**
  Недоменные ноутбуки, смартфоны и сетевое оборудование не умеют ldap:///. Первой ссылкой в CDP/AIA всегда публикуем HTTP на выделенном имени pki.<доме…
- ✕ **Сертификат есть — учётку отключили**
  Disable учётки не гасит EAP-TLS: ноутбук ходит в Wi-Fi по живому сертификату. В регламент увольнения вшиваем certutil -revoke + внеочередную публикац…
- ✕ **Сертификаты без SID-расширения**
  DC в Full Enforcement (KB5014754, обязателен с 02.2025, откат убран с 09.2025) отклоняет сертификаты без szOID_NTDS_CA_SECURITY_EXT. Старые перевыпус…
- ✕ **Бэкап сервера без ключей CA**
  Снапшот ОС не спасает без ключевой пары и базы. Еженедельно Backup-CARoleService (ключ+БД) плюс экспорт ветки реестра CertSvc\Configuration — иначе в…

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Двухуровневая иерархия: офлайн Standalone Root (RSA 4096) + доменный Issuing CA
- Свои дубликаты шаблонов вместо встроенных, KSP + SHA256, точечные группы Enroll
- CDP/AIA по HTTP на pki.<домен>, base CRL Issuing CA — 1 неделя
- Корень и CRL опубликованы в AD через certutil -dspublish

НОРМАЛЬНО

- Автоэнроллмент GPO на компьютеры и пользователей с автопродлением на 80% срока
- Delta CRL 1 день + регламент certutil -revoke в чек-листе увольнения
- Аудит CA (AuditFilter 127) и еженедельный Backup-CARoleService в защищённое хранилище
- Контроль EditFlags и прав на шаблонах после каждого изменения PKI

ХОРОШО

- OCSP Online Responder для 802.1X/VPN — отзыв виден за минуты
- EAP-TLS на NPS: Wi-Fi и VPN только по сертификатам, без общих паролей
- Full Enforcement KB5014754 на всех DC подтверждён, мониторинг событий KDC 39/41
- pkiview.msc + алертинг на сроки CRL и сертификата Issuing CA (за 6-12 мес. до конца)

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Корневой CA физически офлайн и вне домена, а его образ лежит в офлайн-хранилище?
- [ ] В календаре эксплуатации стоит включение Root CA на публикацию CRL до истечения overlap-окна?
- [ ] Встроенные шаблоны сняты с публикации, выдача идёт только по вашим дубликатам с точечными группами?
- [ ] Флаг EDITF_ATTRIBUTESUBJECTALTNAME2 проверен и выключен на каждом Issuing CA?
- [ ] Есть ли шаблоны, где заявитель сам задаёт Subject/SAN и при этом нет одобрения менеджером CA?
- [ ] Отзыв сертификата включён в процедуру увольнения и публикуется CRL в тот же день?
- [ ] Первая ссылка CDP/AIA — HTTP, и она открывается с недоменного устройства?
- [ ] Бэкап CA содержит ключевую пару и базу (Backup-CARoleService), а не только снапшот ОС?
- [ ] Все сертификаты перевыпущены с SID-расширением — DC в Full Enforcement их принимают без событий 39/41?
- [ ] Известна дата истечения сертификата Issuing CA и назначен ответственный за перевыпуск заранее?

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).

- Проектируем и разворачиваем двухуровневый AD CS под ключ: офлайн-корень, Issuing CA, CDP/AIA, OCSP — за 5-10 дней
- Переводим Wi-Fi и VPN на EAP-TLS по сертификатам: шаблоны, автоэнроллмент, NPS/RADIUS, профили клиентов
- Аудитим существующий PKI: права шаблонов, EditFlags, сроки CRL, соответствие strong mapping KB5014754
- Встраиваем PKI в эксплуатацию: регламент отзыва при увольнении, бэкап CA, мониторинг сроков и алертинг
- Мигрируем с одноуровневого онлайн Root CA на безопасную иерархию без остановки сервисов

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 PKI design considerations using AD CS in Windows Server (learn.microsoft.com — 2025)

02 Install-AdcsCertificationAuthority (ADCSDeployment) (learn.microsoft.com — 2025)

03 Certificate Autoenrollment / Troubleshooting Autoenrollment (learn.microsoft.com — 2024)

04 Prepare the CAPolicy.inf File (Server Certificates Guide) (learn.microsoft.com — 2025)

05 KB5014754: Certificate-based authentication changes on DC (support.microsoft.com — 2025)

06 Наш шаблон certutil -setreg для офлайн Root CA (26w CRL) (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.