Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

AD CS: корпоративный PKI, который переживёт смену админов

Двухуровневая иерархия, шаблоны, автоэнроллмент и CRL — как мы это строим в офисе до 50 PM

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Сертификаты в офисе появляются стихийно: самоподписанный TLS на 1С-веб, ЦС прямо на контроллере домена, CRL, который никто не публикует. Пока всё работает, проблемы не видно. Но в момент, когда истекает корневой сертификат или перестаёт открываться URL из CDP, разом отваливаются Wi-Fi 802.1X, VPN, RD Gateway, внутренние порталы и почта — и починить это за час нельзя.

Почему это важно бизнесу

- Истёкший корневой сертификат гасит Wi-Fi, VPN и внутренние порталы одновременно: встаёт вся компания, а не один сервис
- Недоступный CDP-адрес превращает валидный сертификат в отвергнутый — клиент не может проверить отзыв и рвёт соединение
- ЦС на контроллере домена нельзя переименовать и нельзя понизить: любая миграция DC упирается в пересборку всей PKI
- Слабые привязки сертификата к учётной записи: с 11.02.2025 KDC работает в полном применении и такой вход отклоняет
- Публичные сертификаты на каждый внутренний сервис — постоянный расход и ручное продление в десятках мест

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

20 / 10 / 2

лет: срок Root CA, Issuing CA и наш потолок для конечных сертификатов пользователей и машин

наш стандарт

8 ч

таймер автоэнроллмента: старт системы или вход, обновление GPO и далее каждые 8 часов

по докам AD CS

80%

срока жизни — раньше этого порога автопродление не стартует, renewal period сдвигает позже

по докам AD CS

09.09.2025

с этого обновления параметр StrongCertificateBindingEnforcement KDC больше не читает

KB5014754

26 нед

CRLPeriod=Weeks и CRLPeriodUnits=26 у офлайнового Root; у Issuing — Days/7 и delta 1 день

наш стандарт

ML-DSA-87

постквантовый провайдер ЦС в Windows Server 2025: KeyLength 20736 бит, HashAlgorithm NoHash

по докам AD CS, KB5087539

РЕАЛИЗАЦИЯ 1 ИЗ 3

Разворачиваем офлайновый Root и доменный Issuing

Что настраиваем

Офис 40-50 PM, один домен AD, два ESXi: BM Root CA 2 vCPU / 4 ГБ / 60 ГБ вне домена и Issuing CA 4 vCPU / 8 ГБ / 100 ГБ SSD

Как мы это делаем

1. До установки роли кладём C:\Windows\CAPolicy.inf, секция [certsrv_server]: RenewalKeyLength=4096, RenewalValidityPeriod=Years и Units=20, CRLPeriod=Weeks и Units=26
2. Install-AdcsCertificationAuthority -CAType StandaloneRootCA -KeyLength 4096 -HashAlgorithmName SHA256 -ValidityPeriod Years, провайдер RSA#Microsoft Software KSP
3. certutil -setreg CA\CRLPublicationURLs и CA\CACertPublicationURLs: локальный путь плюс http://pki.<домен>/CertEnroll/; LDAP-записи у Root нет — он вне домена
4. Issuing — EnterpriseSubordinateCA с -OutputCertRequestFile и LoadDefaultTemplates=0 в своём CAPolicy.inf; .req на Root: certreq -submit, назад certutil -installcert
5. Root гасим: адаптер отключён, снапшот и Backup-CARoleService с паролем в два разных хранилища, приватный ключ BM не покидает

РЕЗУЛЬТАТ

Компрометация Issuing лечится отзывом его сертификата и выпуском нового за час — без замены корня на каждом устройстве. Корневой ключ физически вне сети почти весь год, а цепочка доверия раздаётся по домену групповыми политиками автоматически.

КЛЮЧЕВОЙ НЮАНС

CAPolicy.inf читается только при установке роли и перевыпуске сертификата ЦС, а LoadDefaultTemplates=0 действует лишь на Enterprise CA: забыли — встроенные шаблоны опубликуются, снимать вручную.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Собираем свои шаблоны и включаем автоэнроллмент через GPO

Что настраиваем

Домен с отдельными OU под серверы, станции и людей: TLS для 1С-веб и RD Gateway, Computer под 802.1X, Code Signing под PowerShell

Как мы это делаем

1. Встроенные не трогаем: в certtmpl.msc делаем Duplicate Template с совместимостью Windows Server 2012 R2 (версия 4, ключи CNG/KSP) и именем вида ITF-Computer-2026
2. Subject Name: для компьютеров Build from AD → DNS name, для пользователей CN плюс UPN; Supply in the request — только где нужен и с manager approval
3. Security: убираем Authenticated Users, целевой группе даём Read + Enroll + Autoenroll. Публикуем: Add-CATemplate -Name ITF-Computer-2026, сверяем Get-CATemplate
4. GPO ITF-PKI-Autoenroll на OU: Public Key Policies → Certificate Services Client - Auto-Enrollment = Enabled, обе галки обновления; то же в User Configuration
5. Приёмка на клиенте: gpupdate /force, certutil -pulse и certutil -user -pulse, certutil -store My, certutil -verify -urlfetch на выгруженном .cer

РЕЗУЛЬТАТ

Новая машина получает сертификат в момент ввода в домен, продление уходит автоматически после 80% срока жизни. Ручная выдача остаётся только для wildcard и внешних устройств, где мы сознательно оставили одобрение оператором.

КЛЮЧЕВОЙ НЮАНС

Autoenroll в ACL шаблона без Enroll не работает вовсе. А Authenticated Users с правом Enroll на шаблоне с EKU аутентификации — прямой путь к выпуску сертификата на чужую учётную запись.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Публикуем CRL и AIA, закрываем требование строгих привязок

Что настраиваем

Инфраструктура с 802.1X на NPS, RD Gateway и S/MIME; контроллеры домена уже переведены в полное применение строгих привязок

Как мы это делаем

1. Сайт IIS pki.<домен> раздаёт каталог CertEnroll; appcmd set config /section:requestfiltering /allowDoubleEscaping:true, иначе delta-CRL с плюсом уходит в 404
2. У Issuing в CRLPublicationURLs три записи: файл, http://pki.<домен>/CertEnroll/ и ldap:///CN=%7%8,CN=%2,CN=CDP,...; в CACertPublicationURLs — файл, http и LDAP
3. certutil -setreg CA\CRLPeriod Days и CRLPeriodUnits 7, CRLDeltaPeriodUnits 1, CRLOverlapPeriod с запасом; далее Restart-Service certsvc и certutil -crl
4. Сверяем наличие SID-расширения 1.3.6.1.4.1.311.25.2 в выпущенных сертификатах и собираем события KDC 39, 40 и 41 с контроллеров домена
5. Где сертификат без SID, ставим строгую привязку altSecurityIdentities: X509IssuerSerialNumber, X509SKI или X509SHA1PublicKey; слабые X509RFC822 не берём

РЕЗУЛЬТАТ

Аутентификация по сертификатам переживает переход контроллеров в полное применение без массовых отказов Wi-Fi и VPN, а любой клиент проверяет отзыв двумя путями — по HTTP и по LDAP, даже если один из них временно недоступен.

КЛЮЧЕВОЙ НЮАНС

Откатиться в режим совместимости больше нельзя: значение StrongCertificateBindingEnforcement в ветке Kdc после обновления от 09.09.2025 не действует. Слабые привязки надо было заменить заранее.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **ЦС поставили на контроллер домена**
  Имя ЦС намертво привязано к имени сервера: понизить или переименовать такой DC уже нельзя, миграция превращается в пересборку всей иерархии.

- ✕ **Забытый или недоступный CDP**
  URL из расширения CRL Distribution Point не открывается с клиента — проверить отзыв невозможно, и валидный сертификат отвергается.

- ✕ **Правят встроенные шаблоны**
  В шаблонах версии 1 меняются только права доступа, и удалить их нельзя. Работаем исключительно с дубликатами со своим префиксом в имени.

- ✕ **Authenticated Users на шаблоне**
  Право Enroll у всех на шаблоне с EKU аутентификации позволяет получить сертификат на произвольную учётку. Оставляем только целевую группу.

- ✕ **Включён EDITF_ATTRIBUTESUBJECTALTNAME2**
  Флаг разрешает подставлять свой SAN в любой шаблон. Снимаем: certutil -setreg policy\EditFlags -EDITF_ATTRIBUTESUBJECTALTNAME2 и перезапуск certsvc.

- ✕ **IIS без allowDoubleEscaping**
  Delta-CRL вида CAName+.crl отдаётся как 404, проверка отзыва падает по таймауту, и построение цепочки молча ломается на части клиентов.

- ✕ **Root никогда не включают**
  CRL корня тоже имеет срок. Пропустили публикацию — вся иерархия считается недоверенной, включая полностью живой Issuing CA.

- ✕ **Снапшот вместо бэкапа ЦС**
  Нужен Backup-CARoleService с паролем плюс экспорт ветки реестра CertSvc в отдельное хранилище; восстановление проверяем на тестовой ВМ.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Один Enterprise CA, но на отдельной ВМ, а не на контроллере домена
- CDP и AIA по HTTP на внутреннем имени pki.<домен> плюс запись в LDAP
- Только свои шаблоны-дубликаты, встроенные на ЦС не публикуем
- Backup-CARoleService по расписанию и экспорт ветки реестра CertSvc

НОРМАЛЬНО

- Двухуровневая схема: офлайновый Standalone Root плюс Enterprise Issuing
- RSA 4096 / SHA-256 на ЦС, 2048 на конечных, срок листа не больше 2 лет
- Автоэнроллмент GPO на OU компьютеров и пользователей, обе галки обновления
- Ежедневная проверка цепочки и CRL: certutil -verify -urlfetch по расписанию

ХОРОШО

- Online Responder (OCSP) и delta CRL раз в сутки для парка от 300 устройств
- Разделение ролей: Manage CA и Issue and Manage Certificates у разных людей
- Аудит ЦС: certutil -setreg CA\AuditFilter 127 и сбор событий в Zabbix или SIEM
- Пилот ML-DSA на WS2025 с KB5087539 — отдельной постквантовой иерархией

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] CAPolicy.inf лежит в C:\Windows до установки роли, у Issuing в нём LoadDefaultTemplates=0
- [ ] Root CA выключен, адаптер отключён, снапшот и бэкап ключа в двух разных хранилищах
- [ ] certutil -verify -urlfetch на свежем сертификате проходит без ошибок по CDP и AIA
- [ ] В CRLPublicationURLs есть и HTTP, и LDAP; сайт pki отдаёт файлы с allowDoubleEscaping
- [ ] Все рабочие шаблоны — дубликаты с префиксом организации, Authenticated Users из ACL убраны
- [ ] GPO автоэнроллмента привязана к OU компьютеров и пользователей, certutil -pulse отрабатывает
- [ ] В выпущенных сертификатах присутствует SID-расширение 1.3.6.1.4.1.311.25.2
- [ ] На контроллерах домена нет событий KDC 39, 40 и 41 за последние 30 суток
- [ ] В календаре: публикация CRL корня и перевыпуск Issuing за полгода до истечения
- [ ] Backup-CARoleService идёт по расписанию, восстановление проверено на тестовой ВМ

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 двухуровневую AD CS: офлайновый Root, Issuing, CDP и AIA, шаблоны, автоэнроллмент
- Переводим самодельные ЦС и самоподписанные сертификаты на управляемую иерархию без простоя сервисов
- Готовим домен к строгим привязкам KDC: аудит SID-расширения, событий 39/40/41, altSecurityIdentities
- Настраиваем 802.1X на NPS, TLS для 1С-веб и RD Gateway, подпись PowerShell и S/MIME на своих шаблонах
- Регламент обслуживания: мониторинг CRL, бэкап ЦС, перевыпуск Issuing, документация и передача админу

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 What is Active Directory Certificate Services in Windows Server (learn.microsoft.com — 2026)

02 Certificate template concepts in Windows Server (learn.microsoft.com — 2026)

03 Prepare the CAPolicy.inf File (learn.microsoft.com — 2025)

04 Configure a certification authority to use ML-DSA in Windows Server (learn.microsoft.com — 2026)

05 What is ML-DSA support in AD CS (learn.microsoft.com — 2026)

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

07 certutil — Windows Commands reference (learn.microsoft.com — 2026)

08 Шаблон ITfresh: паспорт PKI и чек-лист сдачи иерархии (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.