

ОБЫЧНО НЕ ВИДНЫ...

КОМПЛЕКСНЫЙ ПОДХОД В УПРАВЛЕНИИ ЖИЗНЕННЫМ ЦИКЛОМ ТЕХНОЛОГИЧЕСКИХ СЕРТИФИКАТОВ SSL/TLS И СОПРОВОЖДЕНИИ ИОК RSA



Константин ЛЕОНТЬЕВ
ведущий архитектор и управляющий партнёр
ООО «Клируэй Текнолоджис» (Clearway Integration)

1. ПОЧЕМУ ТЕМА УПРАВЛЕНИЯ ЖИЗНЕННЫМ ЦИКЛОМ ТЕХНОЛОГИЧЕСКИХ СЕРТИФИКАТОВ АКТУАЛЬНА И ВАЖНА?

Когда мы говорим с бизнесом о цифровых сертификатах, на ум сразу

приходят сертификаты разнообразных электронных подписей, пользовательские токены и шифрование пользовательских данных. И все давно уже привыкли к этому пониманию и задачам, которые решает бизнес с использованием сертификатов. Данная статья посвящена менее

известной, но не менее актуальной сегодня теме управления **технологическими сертификатами**, которые пользователям или бизнесу обычно не видны. Исключением являются случаи, когда вовремя не продлён сертификат одного из публичных веб-сайтов, в результате пользователи при входе на сайт видят в браузере яркое и заметное предупреждение о небезопасном веб-сервере (некоторые такие примеры на слуху — Microsoft, Google, Telegram и другие).

Однако руководителям направлений ИТ и ИБ крупных компаний в своей профессиональной жизни приходится сталкиваться с гораздо более серьёзными проблемами, свя-

SSL/TLS-сертификатов с одного года до 6 месяцев, а в будущем даже ещё короче — до 3 месяцев. В то же время аварии и нештатные ситуации, вызванные несвоевременным обновлением даже одного сертификата, могут обходиться бизнесу в десятки и сотни миллионов рублей.

Не стоит на месте и внутрикорпоративная инфраструктура: в ней появляются внутренние, ориентированные на сотрудников, подрядчиков и партнёров корпоративные веб-сервисы и приложения, частные облачные платформы, интеграционные сервисы и шины данных, построенные на веб-технологиях, контейнерных средах Kubernetes/OpenShift и других технологиях, нуждающихся в сертификатах. Активно развиваются внутренние и внешние интеграционные шины и шлюзы API, реализованные на базе семейства протоколов HTTP. Вся эта инфраструктура требует непрерывного выпуска и применения технологических сертификатов всё в большем и большем количестве. В одной из организаций, в которых мы некоторое время назад внедрили решение по автоматизации выпуска технологических сертификатов в середине 2010-х годов количество таких сертификатов составляло всего несколько тысяч в год. Сегодня же в этой организации в год выпускается, обновляется и используется несколько миллионов технологических сертификатов.

Отдельно необходимо отметить, что для инфраструктуры современных корпоративных приложений сертификаты используются не только при шифровании трафика, но, прежде всего, как инструмент идентификации и проверки подлинности клиента и сервера друг для друга (mutual TLS — mTLS), что даёт приложениям более безопасный аналог логины и пароля для авторизации.

В связи с тем, что мы исключили из предмета рассмотрения настоящей статьи все другие типы сертификатов, кроме технологических — следует сделать важное уточнение: далее в тексте будут рассматри-

ваться сертификаты x.509 с алгоритмами шифрования RSA. Такое ограничение понятно и объясняется тем, что большинство современных библиотек кода и информационных систем ещё не в полной мере в рамках семейства протоколов SSL/TLS и IPSec поддерживают сертификаты и криптографию ГОСТ. Безусловно, ГОСТ SSL/TLS получает все более широкое распространение, но чаще пока применяется на каналобразующем оборудовании. Нас же в первую очередь интересует взаимодействие микро-сервисов, приложений и интеграционных шин.

2. КРАТКИЙ ОБЗОР ТРАДИЦИОННЫХ ПОДХОДОВ И ТЕХНОЛОГИЙ

Для общего контекста вспомним, что Инфраструктура Открытых Ключей (ИОК или PKI) — это не только непосредственно Удостоверяющий Центр, а ещё и вся та технологическая инфраструктура сопровождающая УЦ и обеспечивающая взаимодействие с ним. Инструменты и технические решения, которые предлагают нам традиционные Инфраструктуры Открытых Ключей (ИОК, PKI) для решения, описанной в предыдущем разделе задачи, на самом деле весьма ограниченные и, мягко скажем, недостаточно универсальные. Но прежде, чем дать краткий обзор этих средств давайте всё же перечислим сами задачи.

К основным задачам, стоящим перед современной ИОК, предназначенной для выпуска технологических сертификатов, относятся:

1. Формирование подходящей потребителю ключевой пары и её безопасное хранение.
2. Формирование соответствующего потребностям потребителя запроса CSR, сбор сведений о потребителе.
3. Проверка запроса сертификата (CSR) на соответствие ряду требований ИБ.
4. Доставка запроса (CSR) до удостоверяющего центра.
5. Выпуск сертификата непосредственно на УЦ.
6. Доставка подписанного УЦ сертификата до системы-потребителя.

занными с технологическими сертификатами, когда виновником сбоев в работе критически важных бизнес-процессов оказывается просроченный сертификат.

Каких-то пять-десять лет назад, когда использование протоколов SSL/TLS в сети Интернет было ещё рекомендательным, самоподписанные сертификаты — нормой, а очень длительные сроки действия SSL-сертификатов не вызывали ни у кого беспокойства, мы вообще не думали о том, что просроченный сертификат может стать какой-то заметной проблемой.

Сейчас же, под действием растущих угроз и числа уязвимостей, всё стремительно меняется, в том числе ужесточаются общепринятые нормы безопасности в сети Интернет. Некоторые крупные корпорации, влияющие на стандарты Интернет, уже предлагают увеличить длину ключей и сократить сроки действия

7. Установка сертификата в нужное хранилище системы-потребителя.

8. Информирование и конфигурирование системы-потребителя о новом сертификате.

9. Своевременная замена устаревшего сертификата в системе-потребителе на обновлённый с выполнением всех шагов 1–8.

10. Обеспечение необходимого уровня надёжности и производительности ИОК (поддержка миллионов и десятков миллионов сертификатов) для выполнения задач 1–9.

Кроме перечисленных выше задач, есть ещё ряд задач ИОК, о которых часто забывают, но они от того не становятся менее значимыми:

1. Поддержание и распространение актуального списка(ов) доверенных корневых и промежуточных УЦ в рамках всей организации.

2. Поддержание и распространение актуального списка(ов) отозванных сертификатов в рамках всей организации.

3. Логирование не только фактов выпуска, но и фактов доставки и установки готовых сертификатов.

4. Мониторинг доступности ИОК, её отдельных компонентов и главной её функции — выпуска сертификатов.

5. Независимый мониторинг срока истечения выпущенных сертификатов и своевременное уведомление владельцев об этом.

6. Мониторинг и анализ интенсивности выпуска сертификатов различных типов, выявление пиковых нагрузок.

7. Обеспечение функции Личного Кабинета (одного окна) для пользователей сертификатов.

8. Механизмы оперативного отзыва сертификатов и удаления связанного с ними ключевого материала.

9. Учет технологических окон при выполнении обновления сертификатов.

10. Учет требований безопасности по обращению ключевого материала и защите приватных ключей.

11. В случае использования внешних сертификатов (сертификатов, полученных от УЦ за пределами своей организации), отслеживание не только их сроков действия, но и фактов их отзыва.

12. Инвентаризация фактически используемых сертификатов: сетевым сканированием и поиском в хранилищах ОС/Приложений.

13. Балансировка нагрузки и автоматическое переключение между несколькими однотипными УЦ.

14. Сквозной поиск в единой базе всех используемых сертификатов и предоставление необходимых расширенных сведений о сертификатах в другие автоматизированные системы.

15. Резервное копирование и восстановление ИОК и отдельных её компонентов.

16. Контроль за исполнением регулярных и однократных задач по обслуживанию ИОК.

17. Поддержка сложно сегментированных сетевыми экранами сетей.

18. Проверка актуальности версий установленных крипто-провайдеров и крипто-библиотек.

19. Обеспечение жизненного цикла короткоживущих сертификатов (сроком действия до 14 дней) — востребованы в Kubernetes ISTIO Service Mesh, сценариях Network Access Control/Network Access Protection при использовании 802.1x и IPSec, сценариях подтверждения онлайн транзакций и т.п.

20. Поддержка и динамический выбор УЦ от разных производителей.

В крупных организациях все перечисленные действия требуют автоматизации именно из-за большого количества систем и необходимых им сертификатов. При этом крайне желательно, чтобы эта автоматизация была централизованной и управлялась по общим правилам и стандартам под контролем ролевой модели доступа к функциям управления.

Теперь давайте попробуем оценить как традиционные ИОК и связанные с ними технологии позволяют решать перечисленные выше задачи. Начнем с наиболее очевидной и важной части ИОК — с Удостоверяющих Центров. Тут большинство традиционных решений обеспечивает выполнение основных задач: 3 и 5, частично 9 и 10. Из вспомогательных задач ИОК чаще всего оказываются решёнными 2, частично 3, 4, 6, 7, 8, 10 и 14, обыч-

но решена также задача 15. Теперь посмотрим, какие распространенные технологии позволяют расширить функционал традиционных УЦ:

♦ **SCEP** (в реализации Microsoft: сервис NDES) — протокол, описанный в RFC 8894 и обеспечивающий простой механизм запроса и выпуска сертификатов для доверенных сетевых устройств (роутеры, маршрутизаторы, МФУ и т.п.). Также часто этот протокол используется в связке с Mobile Device Management-системами для формирования и распространения сертификатов и списка доверенных УЦ на мобильные устройства пользователей.

♦ **CMP и EST** — группа протоколов (RFC 9480, RFC 5785), разработанных консорциумом вендоров во главе с Verisign, цель которых — заменить SCEP и обеспечить гибкие функции генерации ключевых пар, выпуска и отзыва сертификатов, восстановления и распространения ключей. Поддерживается в основном библиотеками для разработчиков и пакетом OpenSSL v3.

♦ **ACMEv2** — протокол, описанный в RFC 8555, разработанный командой Internet Security Research Group для проекта Let's Encrypt и использующий агента CertBot на Python или библиотеки для множества разнообразных языков программирования. Основан на принципе подтверждения владения DNS-именем доменов и зон с использованием асимметричных ключей в TXT-записях DNS-зон и автоматизирующий выпуск сертификатов SSL/TLS для полного доменного имени сервера или зоны с wildcard-поддоменами.

♦ **Microsoft Enterprise PKI** — семейство проприетарных технологий для ИОК, встроенных в ОС Windows, службу каталогов Microsoft Active Directory и API-вызовов к УЦ Microsoft CA, основанных на стеке протоколов Microsoft RPC. Позволяет автоматизировать процесс распространения доверенных корневых сертификатов (в составе Active Directory GPO), выпуск и обновление клиентских и технологических сертификатов для приложений и серверов, разрабатываемых корпорацией Microsoft.

♦ Системы автоматизации и мониторинга, нацеленные на ИОК, но при этом требующие тщательной настройки и развития.

3. ОБЪЕКТИВНЫЕ ОГРАНИЧЕНИЯ И РИСКИ СУЩЕСТВУЮЩИХ ТЕХНОЛОГИЙ

Если бы эти решения были универсальными, то необходимости в данной статье вероятно бы не было, но перечисленные в предыдущей главе решения не универсальны. Давайте разберём их наиболее существенные ограничения и проблемы.

SCEP — это в первую очередь не сервис или продукт, а протокол, поэтому его должны поддерживать как минимум потребители сертификатов и сам УЦ. Если с точки зрения УЦ проблем с поддержкой этого протокола нет — таких УЦ много, то при пристальном изучении поддержки со стороны клиентов оказывается, что не такое уж и большое разнообразие клиентов поддерживают этот протокол и ещё меньшее количество корректно пользуются всеми его возможностями и делают это безопасно. Например, многие клиенты произведённого в Китае оборудования не поддерживают обновление списка доверенных корневых и выпускающих УЦ по протоколу SCEP. Также очень многие клиенты специфическим образом нацелены именно на проприетарную реализацию SCEP от Microsoft (сервис NDES) в связке с Microsoft Active Directory. Наиболее активно используемыми SCEP устройствами являются те, которые недоступны или ограничены в России в рамках стратегии импортозамещения и действующих санкций. К таким устройствам относится сетевое оборудование Cisco и устройства Apple на базе iOS и её деривативов. Также надо отметить, что протокол SCEP не позволяет понять, успешно ли был выпущен и доставлен сертификат до конечного потребителя, у него нет механизмов, позволяющих контролировать своевременное обновление сертификатов, и нет средств для проксирования или применения в сегментированных корпоративных сетях. Наконец, в протоколе SCEP от-

сутствуют механизмы полноценного контроля доверия клиенту и содержанию его запроса на выпуск сертификата. Если клиент захочет выпустить сертификат с неподходящим для него Common Name или Subject Alternative Name, то только УЦ в режиме ручной проверки запросов и ручного выпуска сертификатов может предотвратить такой сценарий. Поэтому SCEP подходит только для абсолютно доверенных потребителей, самостоятельно проверяющих и формирующих запросы на сертификаты, и потому не позволяет полноценно автоматизировать весь процесс выпуска.

CMP и **EST** — эти протоколы, к сожалению, реализованы в очень ограниченном наборе проприетарных зарубежных продуктов из недружественных стран, например: EJBCA от шведско-американской компании Keyfactor, Nexus Certificate Manager от европейской Nexus Group, некоторые продукты американской компании Entrust, УЦ от финской INSTA и ряд облачных УЦ. Помимо того, что эти продукты и их производители не могут быть использованы в России, в основном их реализация ограничивается серверным функционалом и поддержкой именно протоколов, а потому полноценного контроля за выпускаемыми сертификатами и их применением на конечных ОС потребителей всё равно не обеспечивается, также нет важных механизмов мониторинга сроков действия сертификатов и ключей. В итоге это требует полноценного проекта по разработке и реализации клиентского функционала в применении к конкретным информационным системам и потребителям.

ACMEv2 — этот протокол ориентирован на один-единственный, хотя и важный сценарий выпуска SSL/TLS-сертификатов, а именно на выпуск сертификатов для классических web-серверов и web-сервисов с уникальным доменным именем, которые представлены в Интернет-пространстве мировой инфраструктуры DNS. При этом право получения сертификата с конкретным Subject Name/Subject Alternative Name имеет только такой клиент, который вла-

деет закрытым ключом (паролем), соответствующим публичной TXT-записи в текущем DNS-пространстве. Из этого сразу вытекают и очевидные ограничения и риски протокола: как лучше передать ключ клиенту и хранить его в безопасности, кто и как контролирует и актуализирует TXT-записи в DNS. Как при этом разделить публичную в сети Интернет и внутреннюю корпоративную инфраструктуру DNS и направить запросы к разным серверам ACME. Как бороться со спуфингом и «отравлением» кеша DNS, особенно в корпоративных сетях (по сути, без внедрения стандарта DNSSEC или его альтернативы Secure Dynamic DNS updates в Microsoft Active Directory защититься от получения злоумышленниками «ваших» сертификатов невозможно). ACME — это такой же протокол, и в нем нет специальных механизмов контроля факта установки и гарантии обновления сертификата информационной системы — потребителя.

Microsoft Enterprise PKI — пожалуй, наиболее функционально полное решение из всех описанных выше, однако оно обладает существенным недостатком: оно ориентировано только на стек продуктов корпорации Microsoft. И хотя существуют простые и понятные механизмы интеграции со сторонними решениями (тот же SCEP и поддержка форматов PKCS#), в таких сценариях существенная часть функционала становится недоступной. Например, без работы потребителя сертификатов на ОС Windows и в инфраструктуре Microsoft Active Directory, а также использования Групповых Политик Active Directory (GPO) у вас не получится распространять информацию о доступных УЦ, о корпоративных шаблонах и сертификатах, которые эти УЦ могут по этим шаблонам выпускать, едином корпоративном списке доверенных сертификатов, обеспечить автоматический перевыпуск устаревающих сертификатов (auto enrollment). Все эти механизмы реализованы поверх семейства сетевых протоколов Microsoft RPC, использование которых в сети Интернет, да и в корпоративных сетях, крайне рискованно. Также Microsoft RPC

плохо работает в сегментированных межсетевыми экранами сетях, поскольку устанавливает несколько разнонаправленных TCP-соединений. Надо отметить, что в рамках Microsoft Enterprise PKI нет и средств мониторинга и контроля как самой ИОК, так и подтверждения успешных фактов обновления списка доверенных сертификатов и собственно результатов выпуска сертификатов. Нет и автоматизации установки обновлённых сертификатов в конечную систему потребителя — это тоже делается чаще всего вручную.

При выборе решения по автоматизации управления технологическими сертификатами следует, кроме прочего, сформулировать общие вопросы ко всем технологиям и продуктам:

Все ли ваши корпоративные потребители сертификатов в корпоративной сети нативно поддерживают ту или иную технологию или протокол?

◆ Насколько сложно обеспечить поддержку протокола или технологии вашими потребителями сертификатов?

◆ Есть ли механизмы контроля результатов выпуска и обновления сертификата на целевой системе потребителей сертификатов?

◆ Есть ли механизмы мониторинга и своевременного оповещения об окончании срока действия сертификата для конкретной системы и её владельца?

◆ Есть ли механизмы балансировки и отказоустойчивости у технологии/протокола для повышения надёжности всего процесса автоматического выпуска и обновления сертификатов?

◆ Поддерживается ли балансировка нагрузки на несколько экземпляров однотипных УЦ?

◆ Есть ли механизмы дополнительной проверки запросов на выпуск сертификата, позволяющие понять, какой клиент запрашивает выпуск и насколько ему допустимо выпускать такой сертификат?

◆ В случае сбоя или отказа решения или технологии автоматического выпуска сертификатов, какие временные меры можно предпринять для обеспечения работоспособности систем потребителей?

◆ Поддерживает ли протокол, технология или продукт другие типы криптографических алгоритмов, в частности криптографические алгоритмы семейства ГОСТ?

При рассмотрении всех этих вопросов выясняются некоторые очень специфические моменты, особенно для современных контейнерных сред на базе **Kubernetes** или брокера сообщений **Apache Kafka**. Перечислять все нюансы обеспечения сертификатами SSL/TLS информационных систем и приложения — занятие долгое и неблагодарное для одной статьи, но давайте хотя бы кратко обозначим наиболее очевидные и заметные проблемы прикладных систем — потребителей сертификатов:

◆ Большинство приложений и систем после выпуска или обновления сертификата требуют выполнения специфических команд и действий, которые позволяют им начать использовать новый сертификат. Такие команды обычно выполняются с использованием данных из нового сертификата и должны быть выполнены полностью автоматически;

◆ Доставка, установка и обновление доверенных корневых сертификатов и полной цепочки сертификатов доверенных выпускающих УЦ в соответствующие хранилища;

◆ Обновление сертификатов в Java-приложениях и поддержание актуального списка доверенных УЦ для JVM — сложность состоит в том, что Java-приложения выполняются в JVM и используют специальное хранилище доверенных сертификатов, автоматическое размещение сертификатов в котором требует дополнительных шагов в сценарии обновления;

◆ Корректное автоматическое обновление сертификатов для распределённых кластеров СУБД, таких как etcd, PostgreSQL или брокеров сообщений Apache Kafka — сложность этой задачи состоит в скоординированном обновлении сертификатов и доверия к ним на разных узлах кластеров в такой последовательности, при которой узлы кластера будут сохранять доверие друг к другу. В противном случае кластер начнёт «терять» узлы и кворум, что приведёт к отказу;

◆ Обновление сертификатов для кластеров Kubernetes требует разработки специализированного компонента — оператора, который реализует специальные шаги и поддерживает специфические API-вызовы для выпуска и обновления сертификатов в Ingress и Egress контроллерах;

◆ Обновление сертификатов envoy-proxy в среде ISTIO Service Mesh на кластерах Kubernetes — особая сложность этой задачи состоит не только в том, чтобы заменить встроенный сервис выпуска сертификатов ISTIO Citadel, но и в том, чтобы обеспечить резервирование и высокую производительность самого процесса выпуска сертификатов. Перевыпуск при каждом рестарте pod-ов продиктован тем, что envoy не сохраняет свой закрытый ключ и сертификат. Производительность же нужна вследствие того, что рестарты pod-ов обычно массовые — перезапускаются целые namespaces и даже кластеры в результате чего за короткое время порядка 10–20 секунд стартуют тысячи pod-ов;

◆ Выпуск сертификатов для системных сервисов и приложений Microsoft, таких как контроллеры домена Active Directory, почтовые службы Exchange, сервера IIS, также требует особых специфических подходов по заполнению расширений EKU и правильному указанию SAN в сертификатах.

4. ДОСТУПНОСТЬ РАЗЛИЧНЫХ ТЕХНИЧЕСКИХ РЕШЕНИЙ В УСЛОВИЯХ САНКЦИЙ И ИМПОРТОЗАМЕЩЕНИЯ

Наверное, этот раздел будет самым коротким в статье — все известные автору имевшиеся продукты и решения по автоматическому управлению технологическими сертификатами в настоящий момент либо подлежат импортозамещению, либо вовсе недоступны для использования в России. Из чего следует очевидный вывод: такое решение должно быть создано в России и интегрироваться с российскими ОС, СУБД, системами резервного копирования, виртуализации и ПО с открытым исходным кодом. Критически важно в переход-

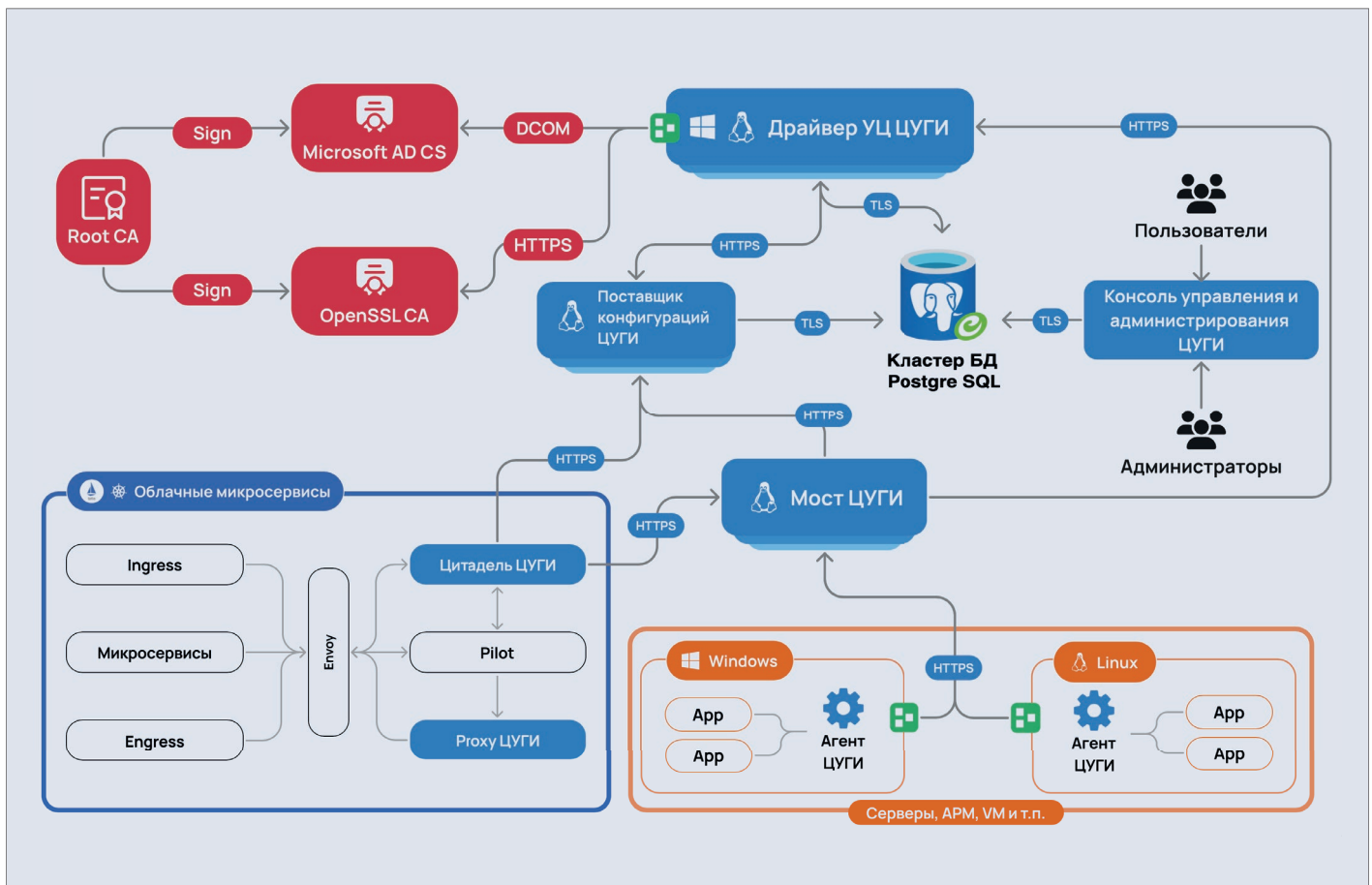


Рисунок 1. Этот компонент обеспечивает автоматизацию выпуска, доставки и установки сертификатов

ный период, пока программные продукты западных вендоров, таких как Microsoft, Cisco, Oracle и прочих, будут сосуществовать в организациях с новыми импортозамещенными продуктами и технологиями, обеспечить работоспособность и совместимость и тех, и других.

5. ОПЫТ ПО КОМПЛЕКСНОМУ ИМПОРТОЗАМЕЩЕНИЮ ИОК

В завершение статьи перейдем к краткому обзору нашего опыта внедрения системы ЦУГИ (Централизованное Управление Гетерогенными Инфраструктурами — в реестре отечественного ПО № 13033), которая в итоге позволяет решить все из перечисленных выше задач технологической ИОК и обеспечить безболезненный переход от инфраструктуры Microsoft Active Directory Certificate Services на технологические УЦ RSA на базе OpenSSL или УЦ российских производителей.

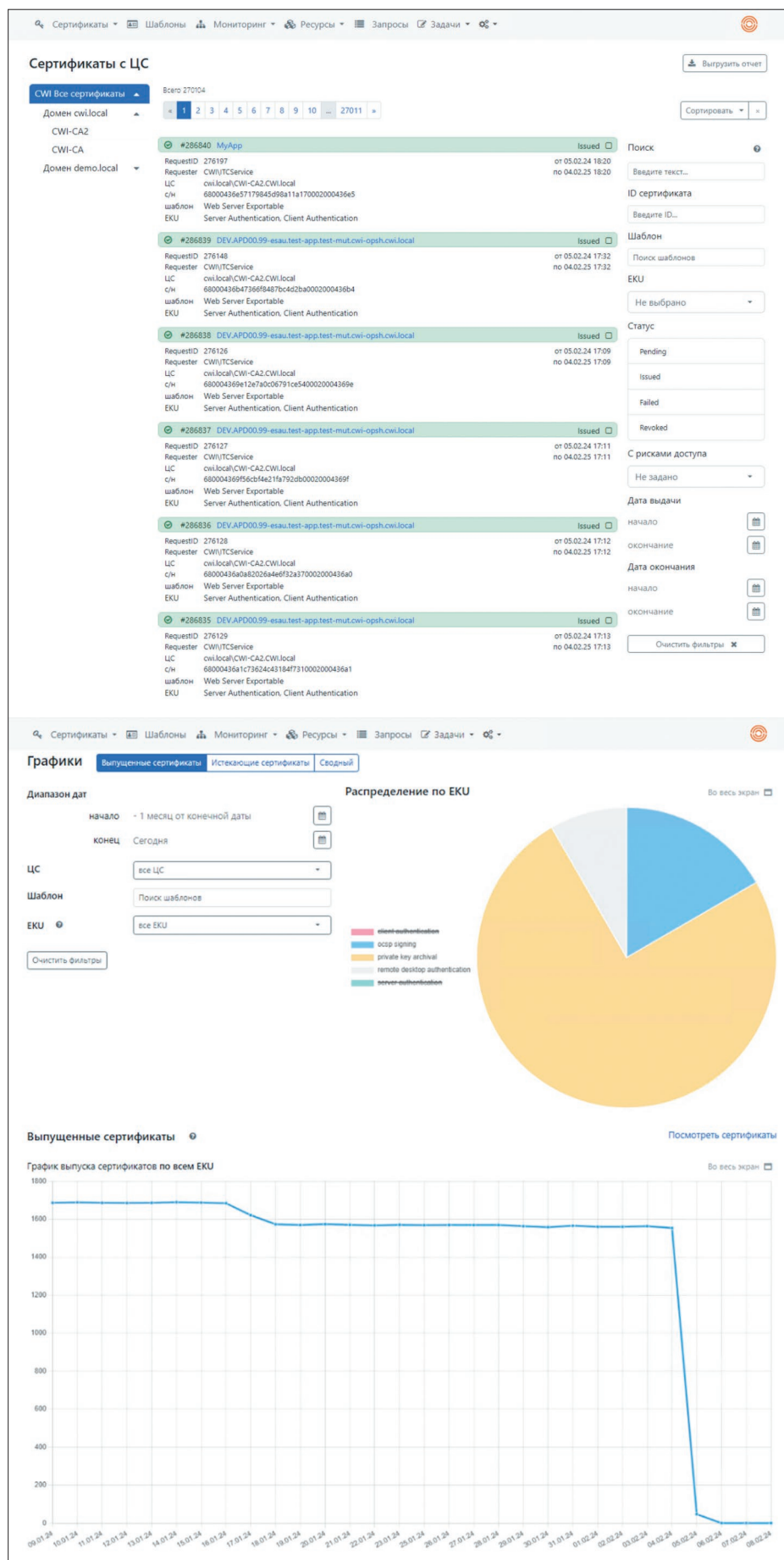
5.1 Импортозамещение серверов УЦ RSA Microsoft CA

В этом вопросе выбрано самое очевидное решение — использование встроенного в большинство ОС семейства Linux пакета OpenSSL который при определенных настройках и программной обвязке позволяет реализовать почти все основные функции технологического УЦ. Такое решение дополнено модулем, поддерживающим протокол SCEP и автоматизирующим процесс формирования и публикации списка отзыва сертификатов (CRL, Delta CRL) и точек доверия (AIA). Как показывают испытания, решение достаточно производительное и при этом не требующее заметных вложений. Однако следует отметить, как будет видно дальше, подобный УЦ с лёгкостью может быть заменён на другие промышленные решения без необходимости какой-либо перенастройки ИОК и информационных систем — потребителей сертификатов.

5.2 Автоматизация выпуска технологических сертификатов для АРМ, серверов и контейнерных сред

Этот компонент — Единая Система Автоматического Управления Сертификатами (ЕСАУС), пожалуй, наиболее важный во всей архитектуре. Именно он обеспечивает автоматизацию выпуска, доставки и установки сертификатов. Кратко представим из чего такая подсистема состоит (см. схему):

- ◆ кроссплатформенный Агент, поддерживающий ОС семейства Windows, Linux, MacOS, IBM AIX и др.;
- ◆ ЦУГИ Citadel, ЦУГИ операторы Kubernetes — компоненты кластеров Kubernetes, поддерживающие процесс выпуска сертификатов для служб и компонентов Kubernetes;
- ◆ мосты ЦУГИ — сервера, обеспечивающие балансировку нагрузки, отказоустойчивость и управление очередями сообщений, а также связность топологии в сегментированных сетях;
- ◆ драйвер УЦ — компонент системы, реализующий набор вендор-не-



зовании сертификатов и выпуске их десятками тысяч в день нам необходимо обеспечить очень высокую доступность и надёжность всех компонентов системы. Кроме архитектурных решений, необходимо реализовать автоматический структурированный мониторинг как самих УЦ RSA, так и всех вспомогательных компонентов ИОК. Для этой цели реализована специализированная Система Мониторинга ИОК (СМИОК), в которую встроена индивидуальная «модель здоровья» ИОК, включающая в себя (рис. 2):

- ◆ проверку состояния процессов УЦ в ОС сервера;
- ◆ снятие счётчиков производительности УЦ;
- ◆ анализ журналов и логов УЦ;
- ◆ проверку доступности и содержания точек распространения CDP/AIA;
- ◆ анализ состояния и работоспособности HSM (при наличии);
- ◆ постоянный пробный выпуск тестового сертификата;
- ◆ анализ шаблонов сертификатов в Microsoft Active Directory;
- ◆ анализ выпущенных сертификатов на типовые риски и требования безопасности;
- ◆ поиск и фильтрацию единой БД всех выпущенных в организации сертификатов.

Также, помимо классических задач мониторинга, система обеспечивает дополнительные функции мониторинга и сопровождения ИОК, а именно (рис. 3):

- ◆ оповещения при отзыве или достижении предельных сроков жизни сертификатов;
- ◆ мониторинг срока действия выпущенных на внешних УЦ сертификатов;
- ◆ мониторинг списка отзыва для сертификатов, полученных на внешних УЦ;
- ◆ централизованное снятие резервных копий конфигурации и БД УЦ;
- ◆ сканирование сетевых сегментов для поиска портов, поддерживающих SSL/TLS-подключение и фиксацию фактически установленных сертификатов;
- ◆ учёт и ведение разовых и регулярных задач дежурной смены ИОК;

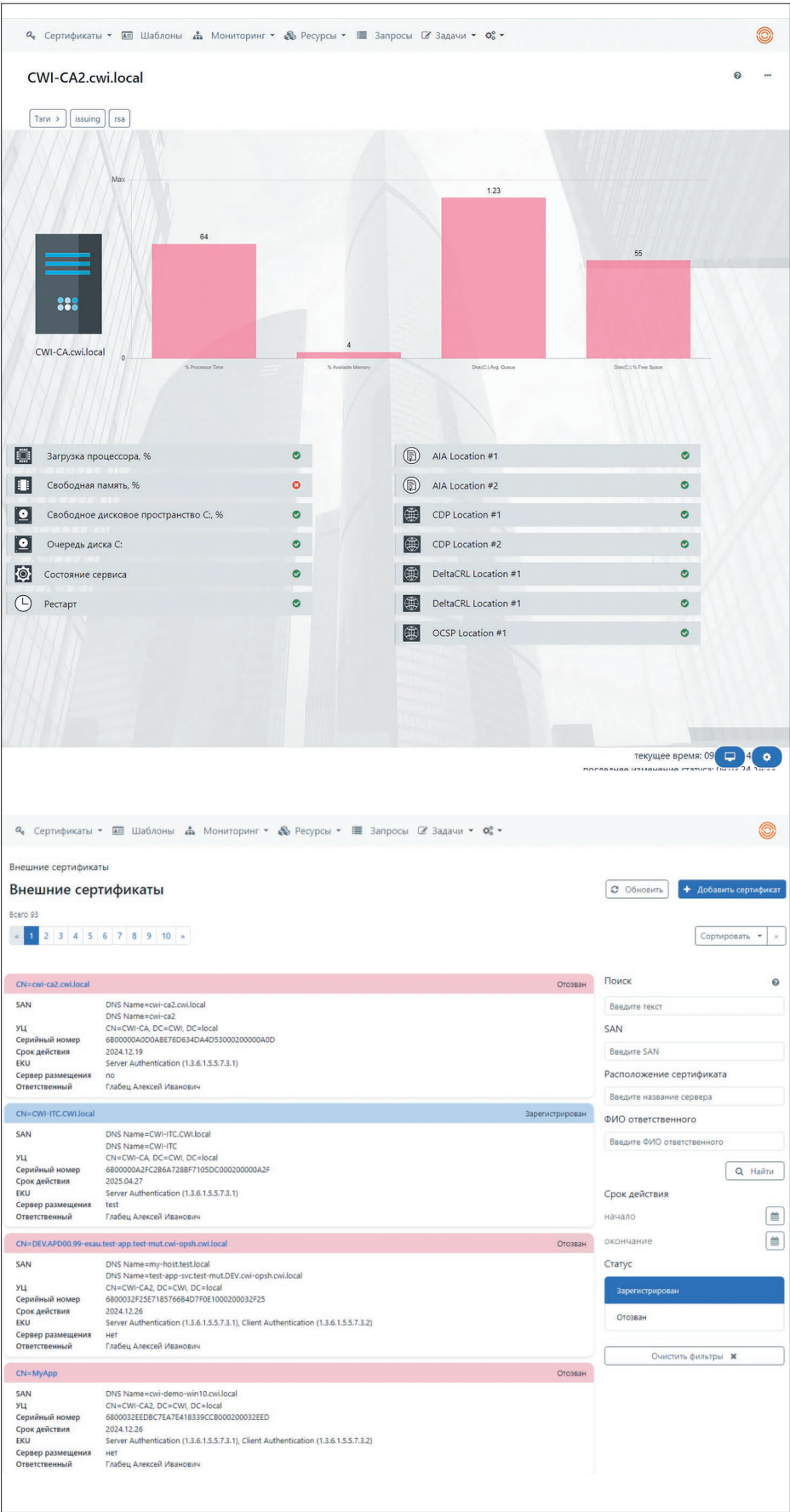


Рисунок 3. Помимо классических задач мониторинга, система обеспечивает дополнительные функции мониторинга и сопровождения ИОК

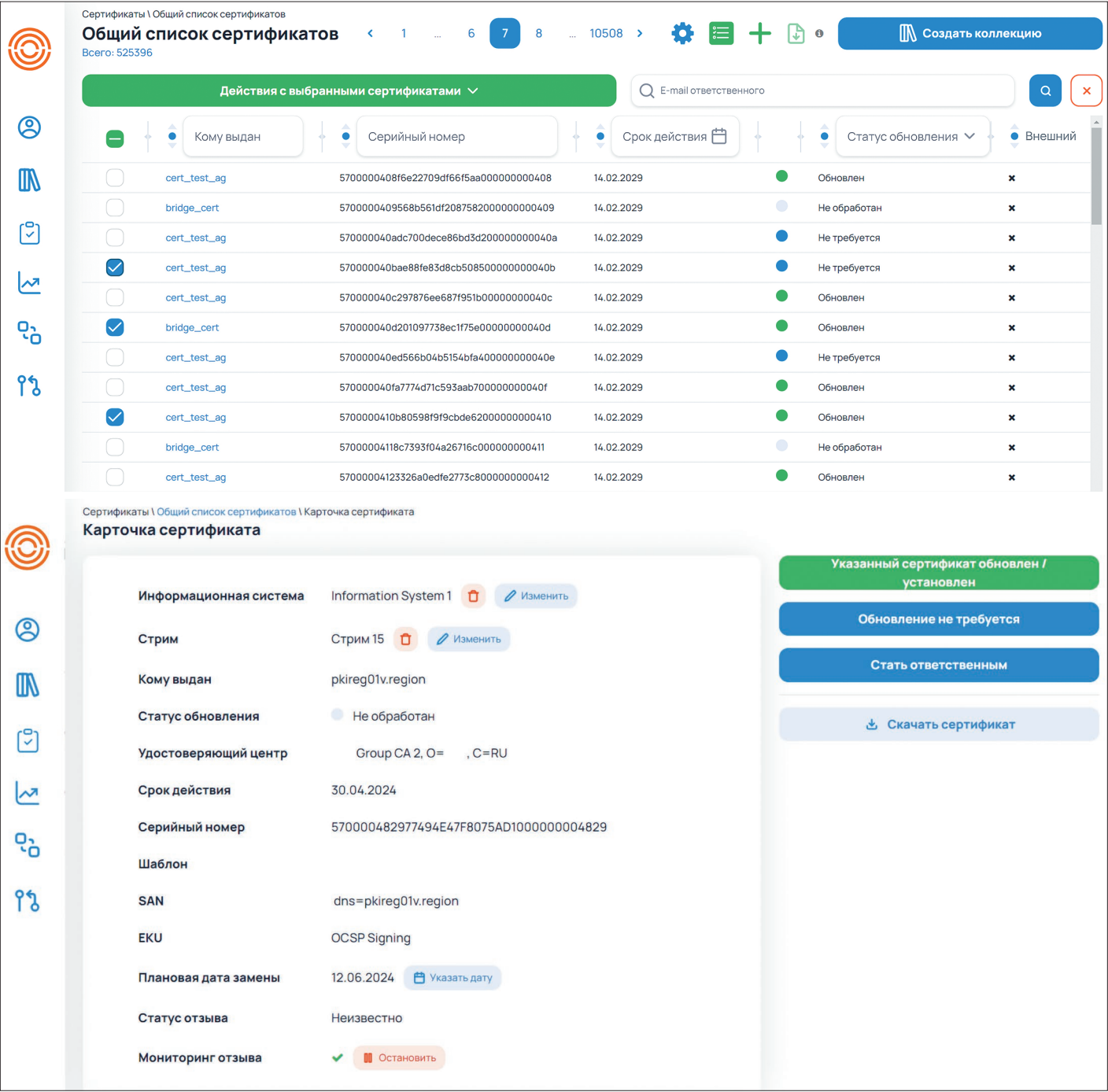


Рисунок 4. Для пользователей и администраторов информационных систем, которые являются потребителями технологических сертификатов, личный кабинет — это единое окно для решения всех основных задач

♦ инвентаризация версий установленных криптобиблиотек и провайдеров.

5.4 Самообслуживание потребителей сертификатов через Личный Кабинет

Этот компонент архитектуры Личный Кабинет Пользователя Сертификатами (ЛКПС) предоставляет интерфейс к Единому Справочнику Сертификатов (ЕСС), используемых в организации,

и отвечает за работу пользователей и администраторов информационных систем, которые являются потребителями технологических сертификатов. Для таких пользователей Личный Кабинет является единым окном для решения всех своих основных задач:

- ♦ указание контактов и способов оповещения пользователя;
- ♦ поиск и сортировка по единому справочнику всех сертификатов организации;

- ♦ создание коллекций сертификатов для удобства управления сертификатами;
- ♦ назначение себя или своих подчинённых ответственными за конкретные сертификаты;
- ♦ просмотр карточек сертификата, где все поля разобраны и проведён анализ рисков;
- ♦ просмотр в карточке сертификата расширенной информации о сертификате, его статусе и местах ис-

пользования, поступившей из других систем: системы мониторинга, системы автоматического выпуска, учёта СКЗИ, CMDB, Active Directory и т.д.;

- ♦ ручной запрос на отзыв или перевыпуск своего сертификата;
- ♦ отметки о статусе выполнения задач установки и обновления сертификатов в своих прикладных системах;
- ♦ связывание сертификатов с данными корпоративной CMDB и кодами информационных систем (место установки/применения сертификата).

5.5 Интеграция технических решений в бизнес-процессы

Рассмотрим совместимость архитектуры ЦУГИ с наиболее актуальными отечественными решениями. В первую очередь опишем возможности интеграции с УЦ, выпускающими RSA сертификаты российского производства:

- ♦ КриптоПро Кластер УЦ – интеграция реализована для выпуска RSA сертификатов.
 - ♦ SafeTech CA – драйвер на финальной стадии тестирования, релиз запланирован в 3 квартале 2024 года.
 - ♦ Aladdin eCA – драйвер в разработке, релиз ожидается в 2024 году.
- Кратко обозначим и другие средства интеграции:
- ♦ Универсальное API для работы с внешними системами – в завершающей стадии разработки.
 - ♦ Системы мониторинга на базе Prometheus – реализованы разнообразные метрики для мониторинга.
 - ♦ Ряд распространённых корпоративных бизнес-приложений – интеграция в разработке.

6. ВМЕСТО ЗАКЛЮЧЕНИЯ

Описанные в статье подходы и программные продукты не просто теория, а зарекомендовавшие себя в реальной эксплуатации (некоторые компоненты успешно работают уже более 2 лет) системы и сервисы построенные на платформе ЦУГИ производства ООО «Клируэй Текнолоджис» (торговая марка Clearway Integration).

Одним из успешно использующих их заказчиков является Банк ВТБ. В частности, на момент написания

статьи в Банке ВТБ из намеченных к концу 2024 года 700 информационных систем и приложений уже подключены и обсуживаются в режиме полностью автоматического выпуска сертификатов более 150. При этом разработана методическая и техническая документация, необходимая для ускорения и упрощения процесса подключения информационных систем потребителей сертификатов к ЦУГИ.

Планы развития ЦУГИ на ближайшую перспективу включают (рис. 5):

- ♦ Создание функционала для более гибкого управления расписанием обновлений и технологическими окнами обновления сертификатов;
- ♦ Разработку мобильного приложения Личного Кабинета Пользователя для управления Сертификатами;
- ♦ Проектирование и реализация модуля ЦУГИ для учёта СКЗИ и/или

интеграция с существующими рыночными решениями;

- ♦ Создание и развитие публичной библиотеки сценариев выпуска сертификатов для конкретных приложений и систем;
 - ♦ Разработку новых драйверов УЦ для УЦ различных производителей, ещё не интегрированных с системой;
 - ♦ Реализацию протоколов CMP, EST и ACMEv2 (SCEP уже реализован) в Агенте и в Драйвере УЦ для расширения сценариев интеграции;
 - ♦ Интеграцию с доверенными хранилищами секретов (аналоги HashiCorp Vault) для расширения сценариев обращения с закрытыми ключами, включая безопасный Key Recovery;
- Сертификацию отдельных модулей и решений на базе ПО ЦУГИ во ФСТЭК и ФСБ.

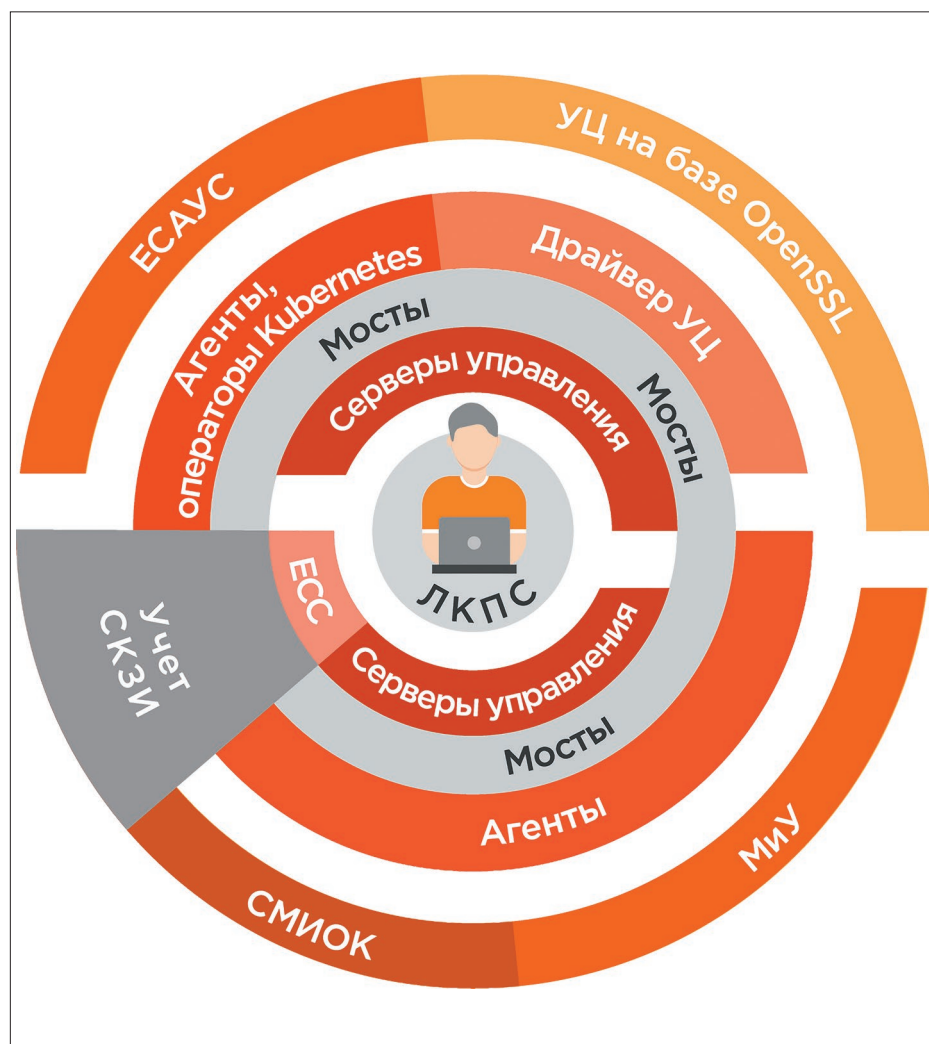


Рисунок 5. Планы развития ЦУГИ на ближайшую перспективу