

## Смарт-конструктор PKI инфраструктуры

### KEYCONTROL

KeyControl — многофункциональная платформа для автоматизации работы с инфраструктурой открытых ключей. Решение работает по принципу конструктора, позволяя собирать любые бизнес-процессы, предоставляет функции самообслуживания объектов и субъектов и имеет развитую систему внешних интеграций, в том числе и с источниками данных о субъектах.

KeyControl призван существенно упростить процессы работы PKI-инфраструктуры, повысить её производительность и улучшить пользовательский опыт.

- ♥ Импортонезависимое решение, поддерживающее работу как на ОС Microsoft Windows, так и на всех ОС семейства Linux, включая отечественные (Astra, Альт, Ред ОС и т.д.)
- ✂ Net 6.0. СУБД: решение поддерживает работу с СУБД MS SQL и PostgreSQL
- ★ Может настраиваться под любые бизнес-процессы, включая самообслуживание

### КЛЮЧЕВЫЕ ФУНКЦИИ

- Управление жизненным циклом и учёт:
  - сертификатов и ключей пользователей и информационных систем
  - ключевых носителей и пользователей, и информационных носителей
  - СКЗИ пользователей и информационных систем
- Учёт автоматизированных рабочих мест
- Подготовка отчётности о всех объектах учёта системы, в том числе и по требованию регуляторов
- Оповещение пользователей и администраторов о событиях в системе
- Полный аудит всех действий администраторов и пользователей системы
- Формирование заявок из личного кабинета работника или администратора
- Создание бизнес-процессов и автоматический старт на основании событий, происходящих в системе
- Поддержка юридической значимости электронного документооборота с использованием электронной подписи при создании и согласовании заявок



## УДОБСТВО

### Автоматизация процесса учёта и управления жизненным циклом

- от создания запроса до выдачи готового сертификата субъекту
- работа с СКЗИ от первичного учёта закупленных лицензий СКЗИ до возврата от владельца с фиксацией всех действий, произведенных с СКЗИ
- полный цикл работы с ключевыми носителями: от первичного учёта закупленных носителей до возврата от владельца с фиксацией всех действий, произведенных с ключевыми носителями
- каталог субъектов в системе может вестись как вручную, так и автоматизированно (доступна полная автоматическая и частичная загрузка данных, а также синхронизация изменений)

KeyControl позволяет отследить полную историю изменений по любому учтённому в системе сертификату, ключевому носителю и СКЗИ и построить отчётные документы как по требованиям регуляторов, так и по внутренним требованиям безопасности.

Система даёт возможность в автоматическом режиме осуществлять инвентаризацию СКЗИ, установленных на АРМ, и контроль за средой функционирования СКЗИ.

## БЕЗОПАСНОСТЬ

Платформа интегрирована с сервисами СМЭВ и ЕСИА, что обеспечивает возможность проверки корректности поданных заявлений на изготовление УКЭП. По умолчанию доступны проверки в МФД и Социальном фонде России (Пенсионном фонде), в сервисах Федеральной налоговой службы и ЕСИА — KeyControl ищет или регистрирует новый субъект в каталоге ЕСИА и публикует выпущенный для него сертификат.

## Управление процессами

Позволяет настроить в системе полноценные процессы управления элементами инфраструктуры открытых ключей и автоматический старт бизнес-процесса по какому-либо событию, например:

- процесс перевыпуска сертификата при приближении истечения срока его действия
- передачу лицензий СКЗИ или токенов из центра в филиалы
- согласование заявлений на выпуск сертификатов УКЭП с проверками заявлений в СМЭВ и сторонних системах.

# KEYCONTROL

## Личный кабинет пользователя

Единый центр управления всеми объектами пользователя, в том числе ключевыми носителями и сертификатами. В личном кабинете можно:

- запросить сертификат
- оформить заявку на отзыв или перевыпуск сертификата
- заказать ключевой носитель или лицензию на СКЗИ
- разблокировать ключевой носитель и получить от него ПИН-код
- получать вспомогательные уведомления (например, напоминания об окончании срока действия сертификата)

Модель организации каталога субъектов\* в системе является иерархической. С помощью механизмов разграничения доступа администраторов и учета владельцев информационных систем можно задать требуемый уровень доступа, что обеспечивает безопасность системы и эффективное разделение полномочий доступа.

\* В качестве субъектов может выступать как пользователь (сотрудник, физическое лицо), так и информационная система (например, веб-сервер)

