Опыт реализации PKI инфраструктуры в масштабах федеральной компании.

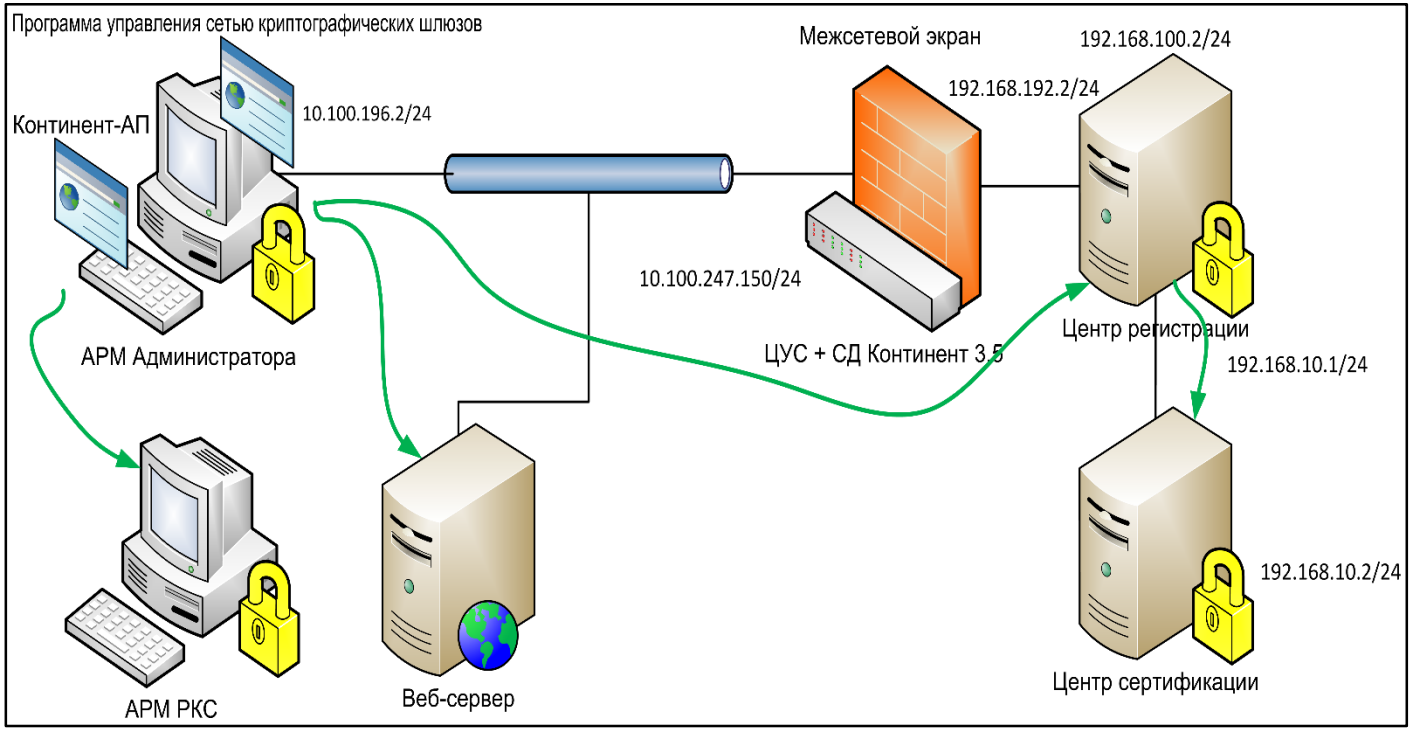
Мобильная электронная подпись.

Поздняков Игорь, Руководитель УЦ ПАО «МегаФон», 27 сентября, 2018 год

МегаФон

Удостоверяющий центр ПАО «МегаФон» ПАК УЦ 1.5

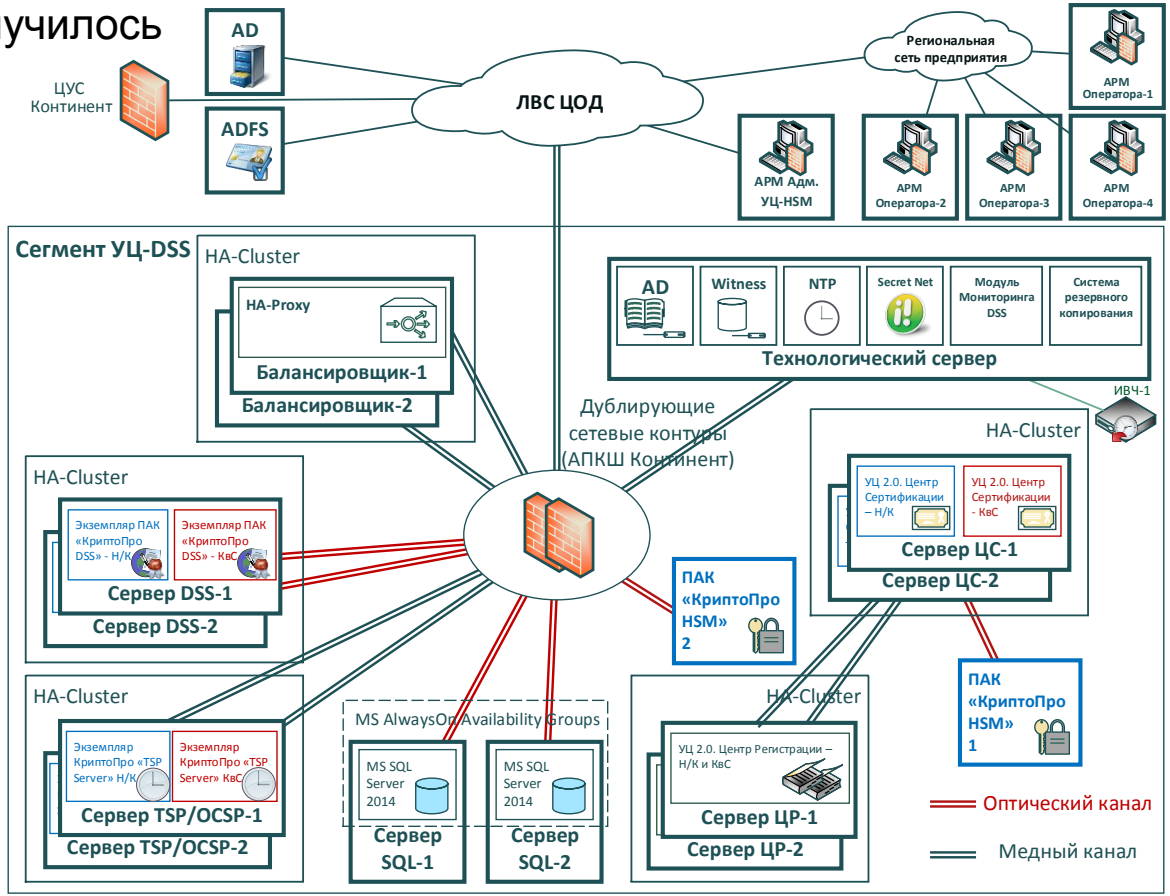
Структурная схема – с чего начинали



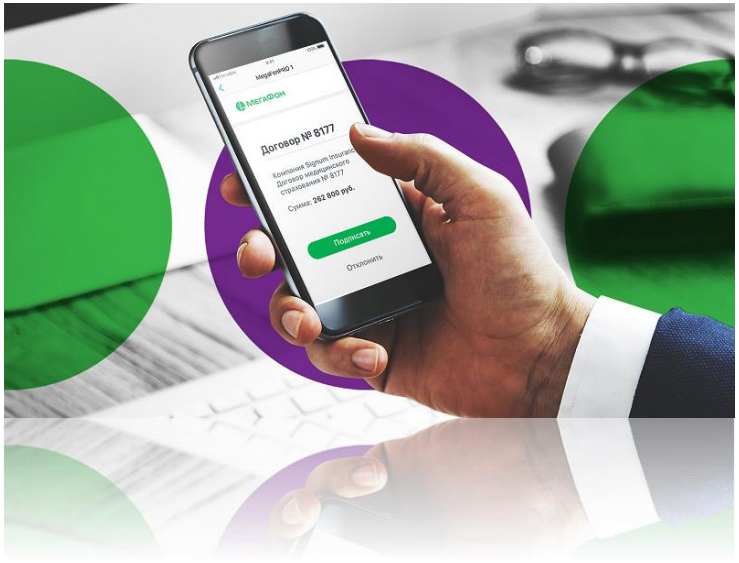
Удостоверяющий центр ПАО «МегаФон» ПАК УЦ 2.0, ПАК DSS 2.0

Структурная схема – что получилось

- ✓ Построена уникальная, замкнутая, самодостаточная экосистема, которая реализует полное резервирование всех компонент и систем УЦ. Следующий шаг – георезервирование.
- ✓ В построении схемы использовался весь накопленный опыт эксплуатации УЦ и сервисов ЭП.
- ✓ Позволяет реализовать балансирование нагрузки, что дает реализовать высокие SLA.
- ✓ Решение на реализацию представленной схемы основано на повышающихся требованиях бизнеса и особенности работы через сервис КриптоПро DSS.
- ✓ Интенсивная интеграция облачной ЭП в корпоративные ИС.



Мобильная Электронная Подпись (МЭП)



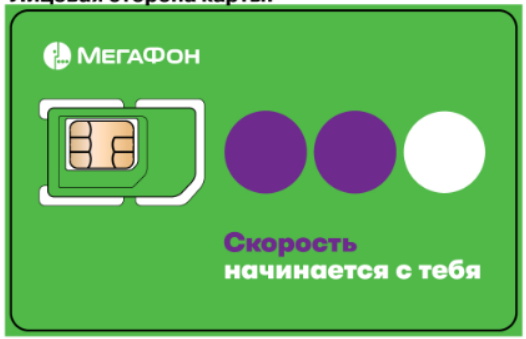
МЭП – апплет на SIM карте, который позволяет подтвердить подписание квалифицированной электронной подписью документов и контролировать действия пользователя в системах ЭДО, ДБО и т.д.

В основе мобильной электронной подписи реализована технология, которая обеспечивает криптографическую аутентификацию пользователей, безопасное online-взаимодействие и подтверждение операций с ЭП на сервере КриптоПро DSS.

Позволяет сервису электронной подписи выполнить требования, предъявляемые регулятором к средствам электронной подписи.

Разработка компании КриптоПро на базе сертифицированного средства криптографической защиты КриптоПро HSM, КриптоПро DSS.

Лицевая сторона карты:



Обратная сторона карты:

Мобильная Электронная Подпись (МЭП)

- Безопасность

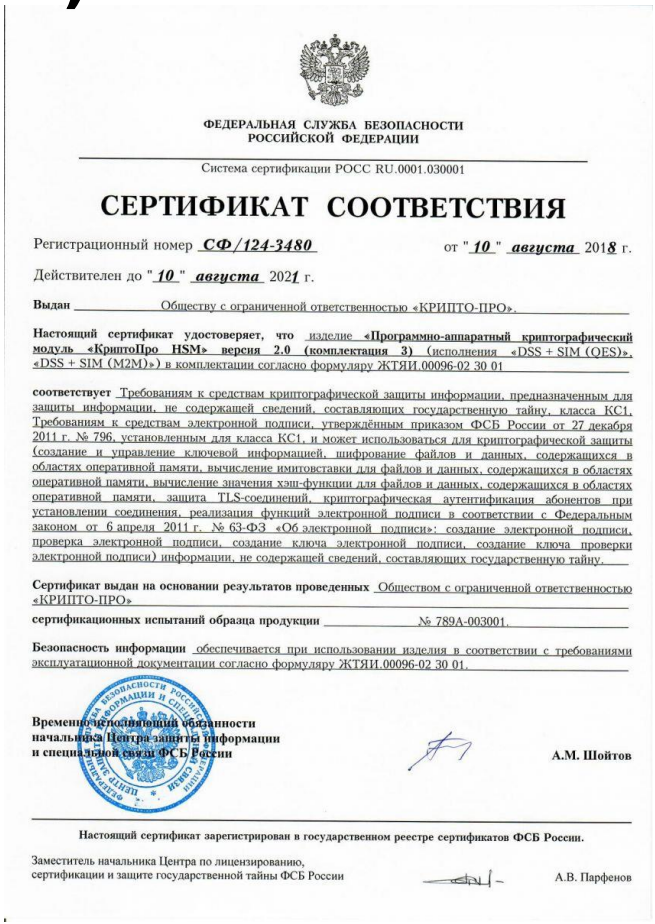
При работе с МЭП визуализация информации выполняется в браузере пользователя ЭДО. Формирование подтверждения на его подписание в КриптоПро DSS производится по защищенному каналу с помощью апплета на SIM карте.

Криптографическая аутентификация и защита канала между апплетом и сервером КриптоПро DSS гарантируют, что только легальный пользователь сможет воспользоваться ключами подписи.

Ключи электронной подписи пользователей хранятся в сертифицированном HSM в неизвлекаемом виде.

- Юридическая значимость подписи

Документ и другие действия пользователя заверяются квалифицированной электронной подписью, что обеспечивает неотказуемость действий. Пользователь не только подтверждает содержание документа, но и в дальнейшем не имеет возможности отказаться от совершенного действия.



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-3480 от "10" августа 2018 г.

Действителен до "10" августа 2021 г.

Выдан Обществу с ограниченной ответственностью «КРИПТО-ПРО».

Настоящий сертификат удостоверяет, что изделие **«Программно-аппаратный криптографический модуль «КриптоПро HSM» версия 2.0 (комплектация 3)** (исполнения «DSS + SIM (QES)», «DSS + SIM (M2M)») в комплектации согласно формуляру ЖТЯИ.00096-02 30 01

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1. Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1, и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, защита TLS-соединений, криптографическая аутентификация абонентов при установлении соединения, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «КРИПТО-ПРО»

сертификационных испытаний образца продукции № 789А-003001.

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями эксплуатационной документации согласно формуляру ЖТЯИ.00096-02 30 01.

Временно исполняющий обязанности
начальника Центра защиты информации
и специальной связи ФСБ России **А.М. Шойтов**

Настоящий сертификат зарегистрирован в государственном реестре сертификатов ФСБ России.

Заместитель начальника Центра по лицензированию,
сертификации и защите государственной тайны ФСБ России А.В. Парфенов

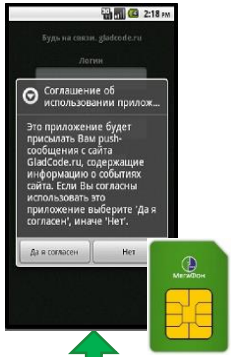
Мобильная Электронная Подпись (МЭП)

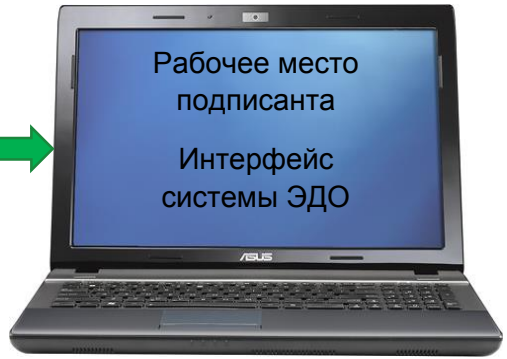
Организация предоставления сервиса

Службы Удостоверяющего центра

Сервис электронной подписи

Провайдер системы электронного документооборота





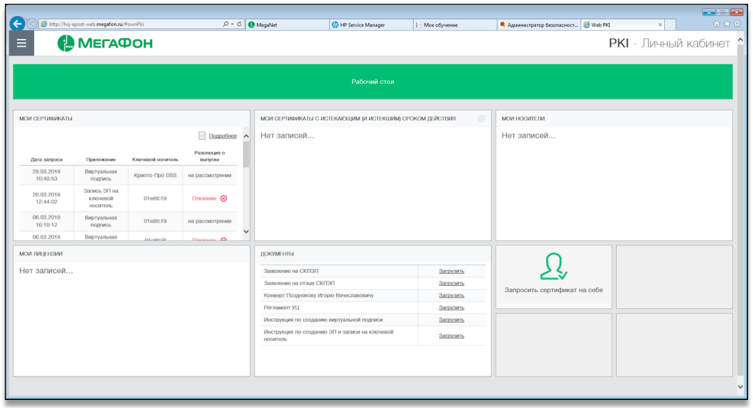
Решение для самообслуживания сотрудника

Схема взаимодействия корпоративных систем

Источники данных о сотрудниках
для пред заполнения полей
сертификата ЭП

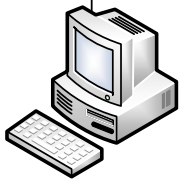
Сервер AD

Сервер SAP HR



Сервер КриптоПро DSS

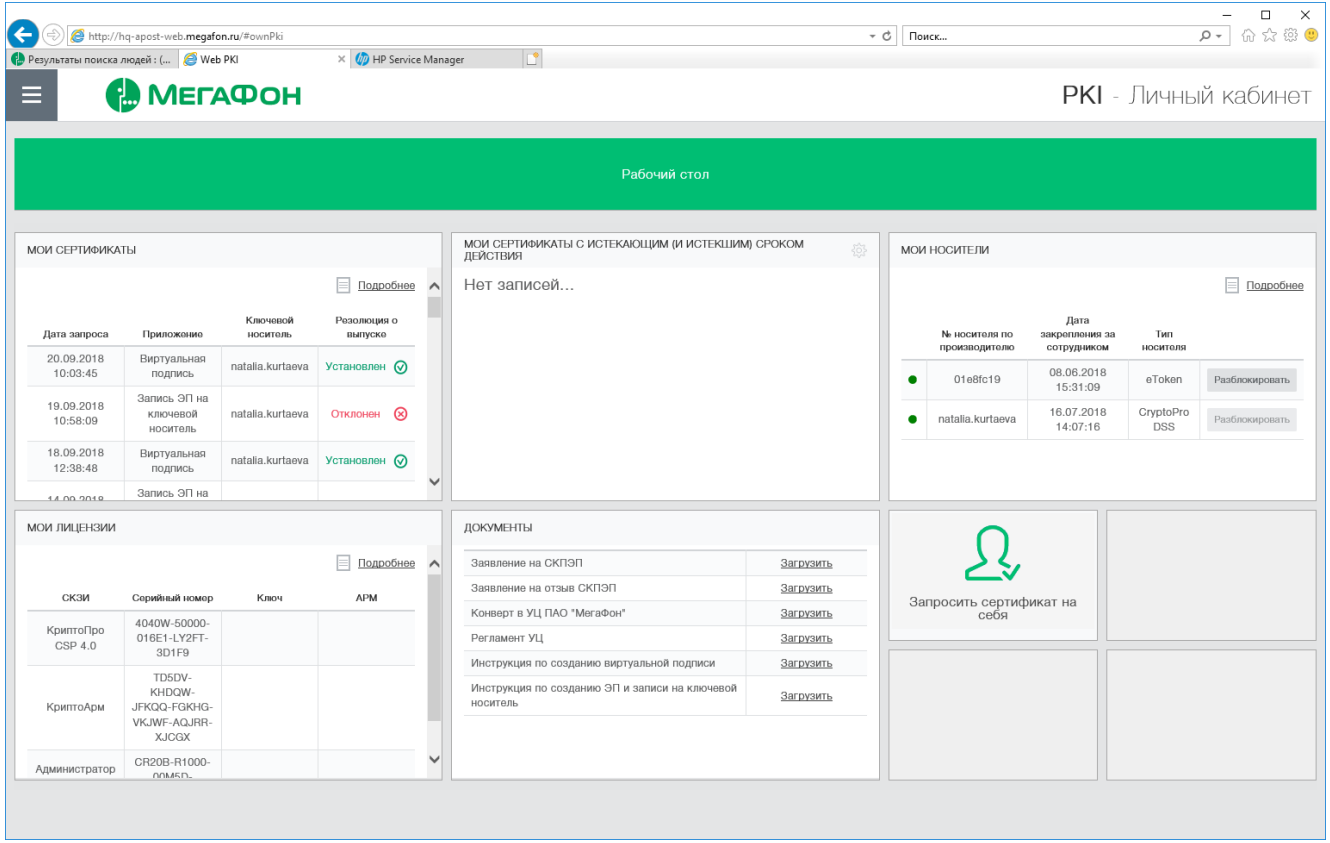
МЭП



Рабочие места сотрудников

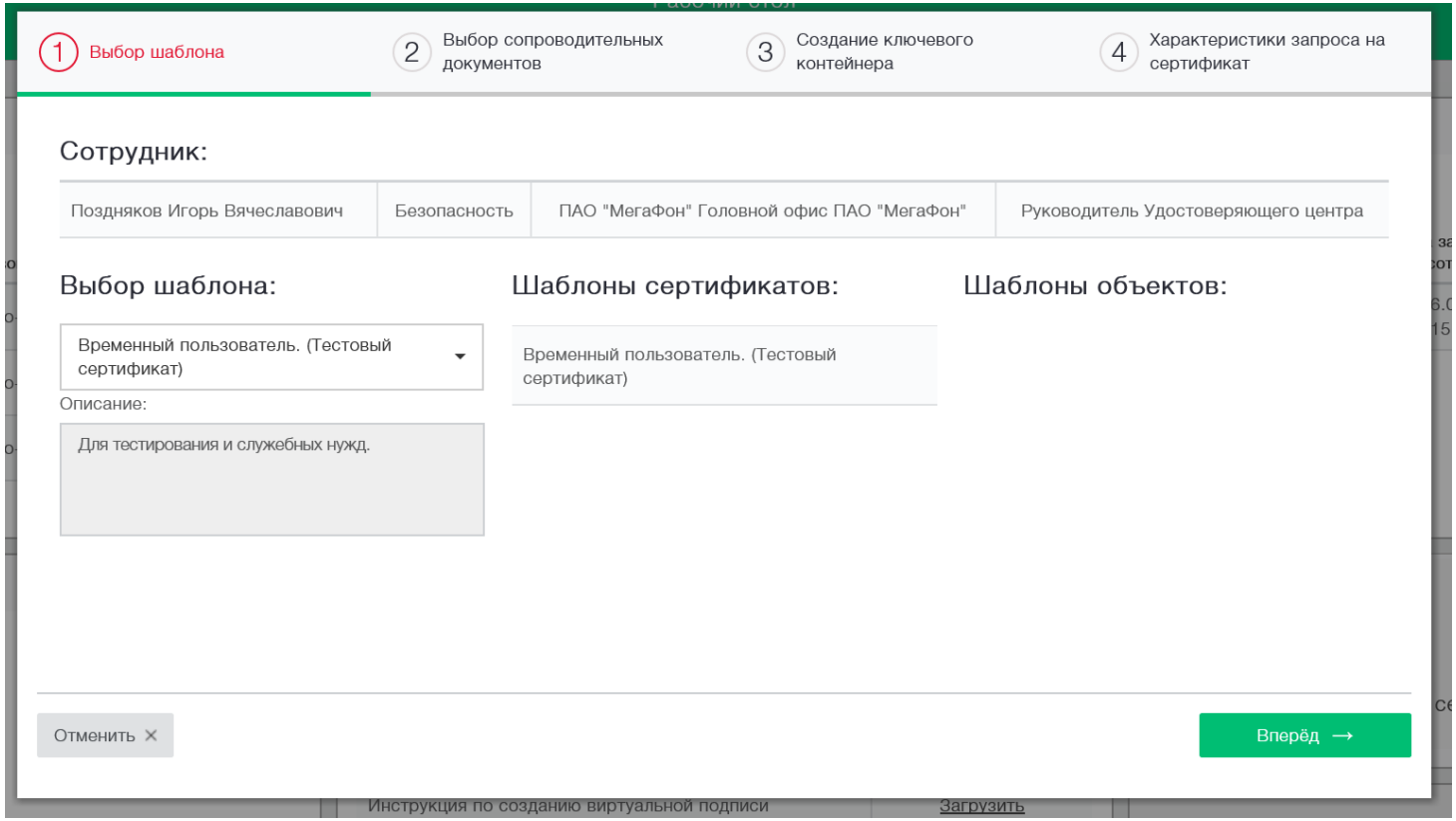
Решение для самообслуживания сотрудника

Интерфейс личного кабинета управления сертификатами ЭП



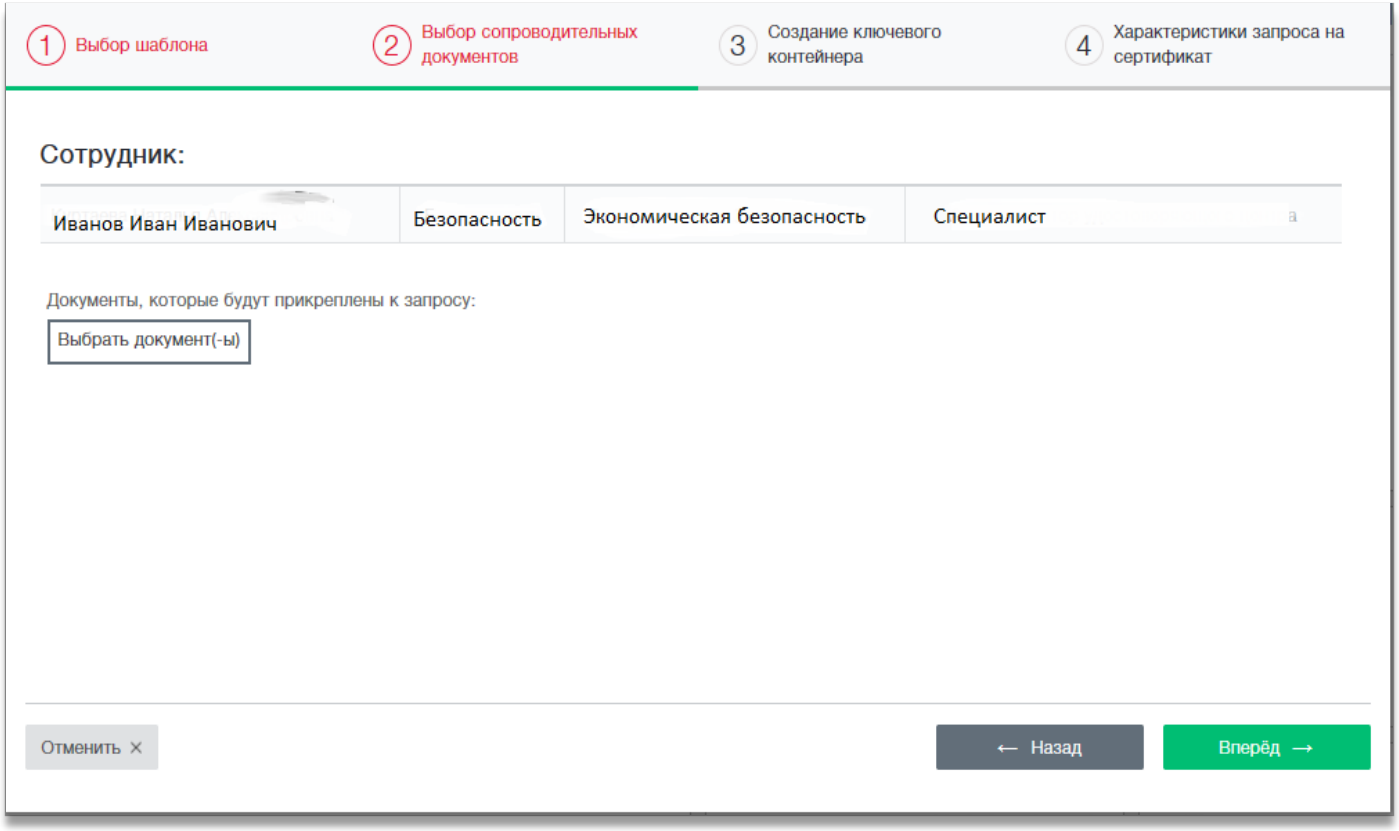
Решение для самообслуживания сотрудника

Получение сертификата ЭП



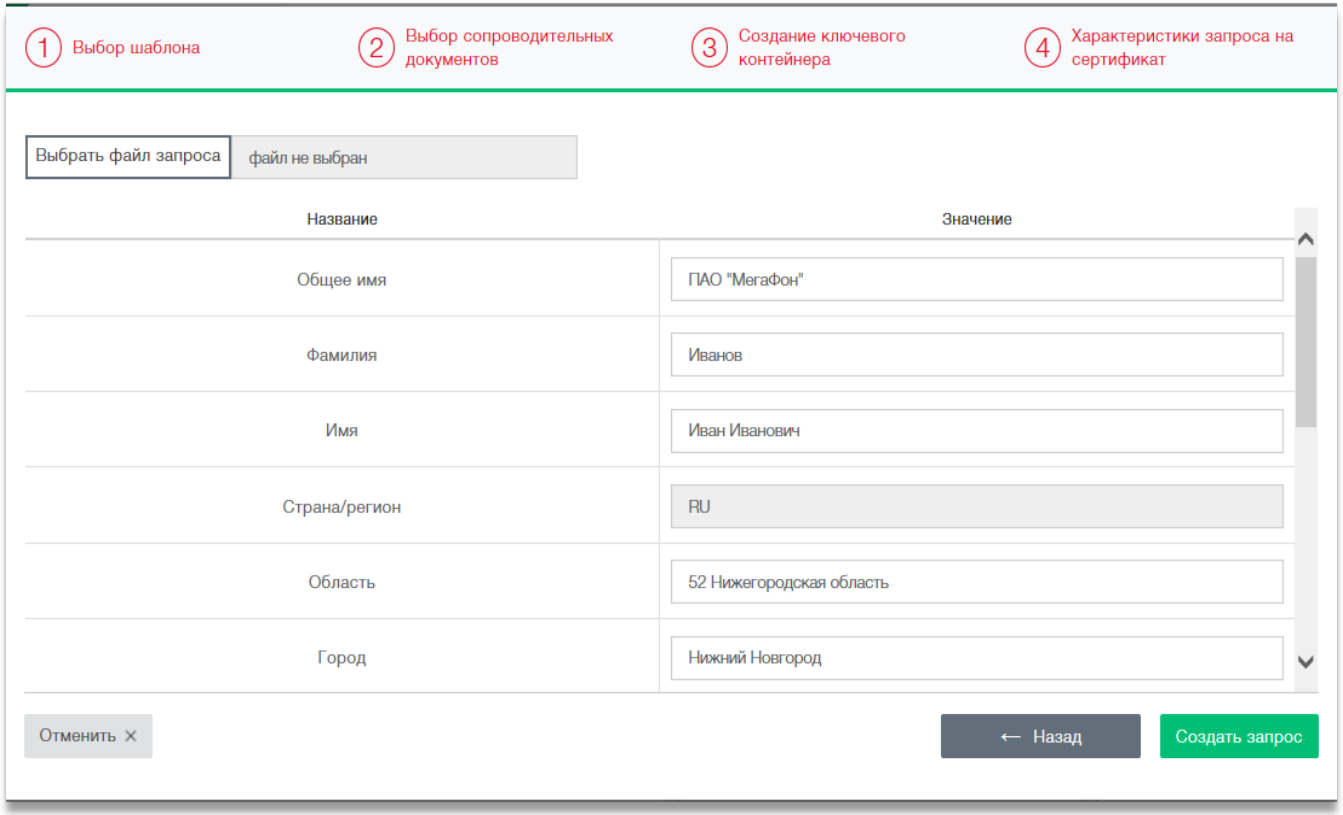
Решение для самообслуживания сотрудника

Получение сертификата ЭП



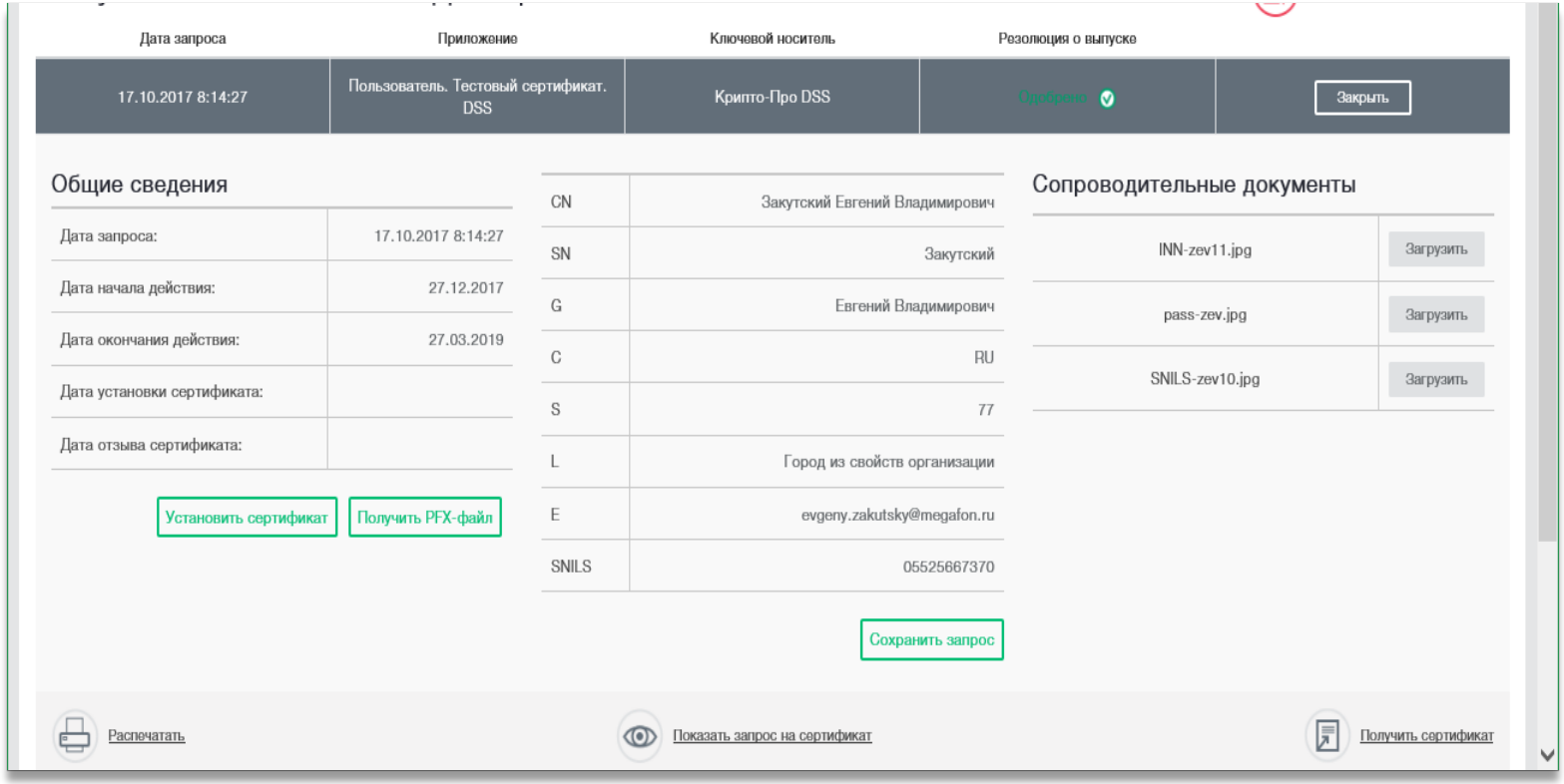
Решение для самообслуживания сотрудника

Получение сертификата ЭП



Решение для самообслуживания сотрудника

Получение сертификата ЭП



Давайте обсудим...

Игорь Поздняков
Телефон +7926 503 19-82
E-mail ipozdnyakov@megafon.ru

МегаФон