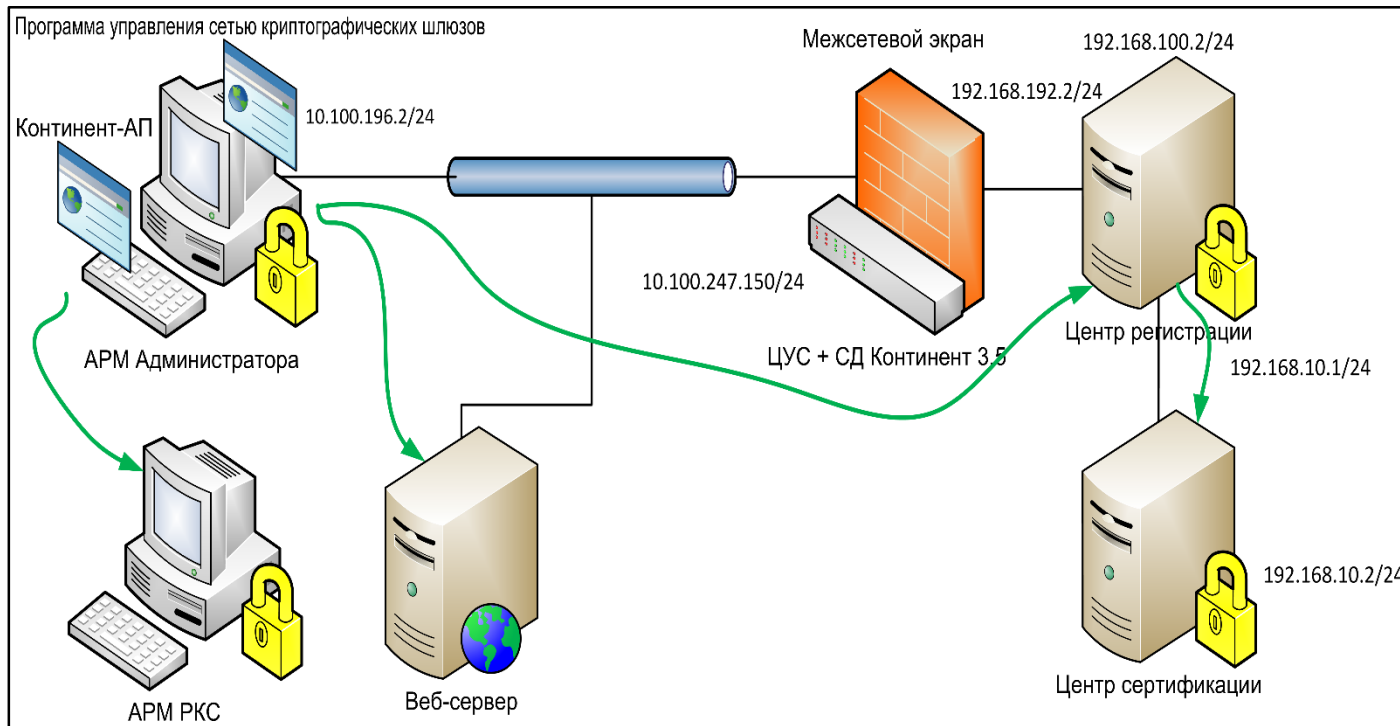


Опыт реализации РКІ инфраструктуры в масштабах федеральной компании. Мобильная электронная подпись.

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

Удостоверяющий центр ПАО «МегаФон» ПАК УЦ 1.5

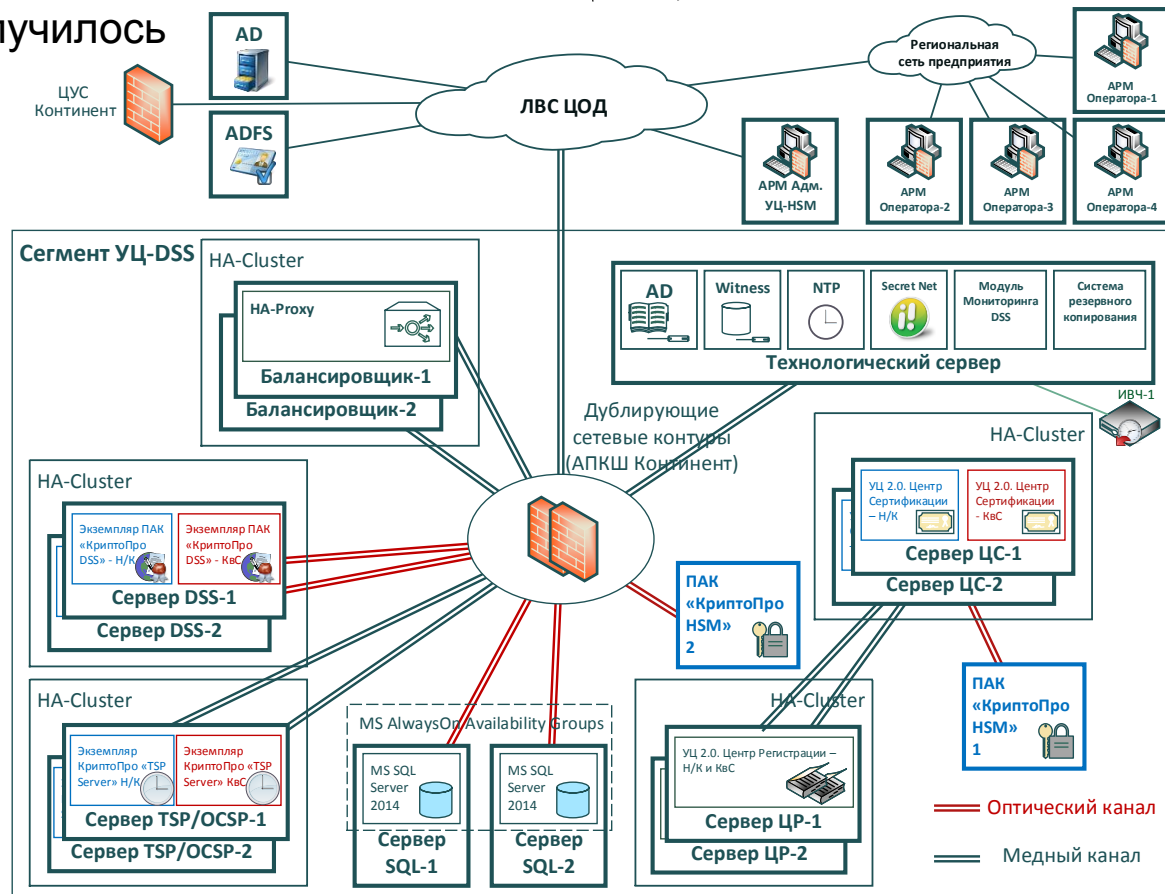
Структурная схема – с чего начинали



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)



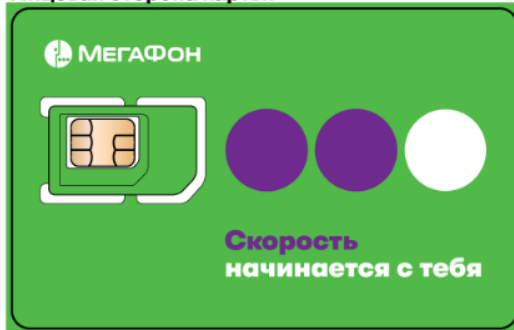
Позволяет сервису электронной подписи выполнить требования, предъявляемые регулятором к средствам электронной подписи.

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

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.

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, утвержденным приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для файлов и данных, содержащимся в областях оперативной памяти, вычисление имитовывода 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.

Временный исполняющий обязанности
начальника Центра защиты информации
и специальной связи ФСБ России

А.М. Шойтов

Настоящий сертификат зарегистрирован в государственном реестре сертификатов ФСБ России.

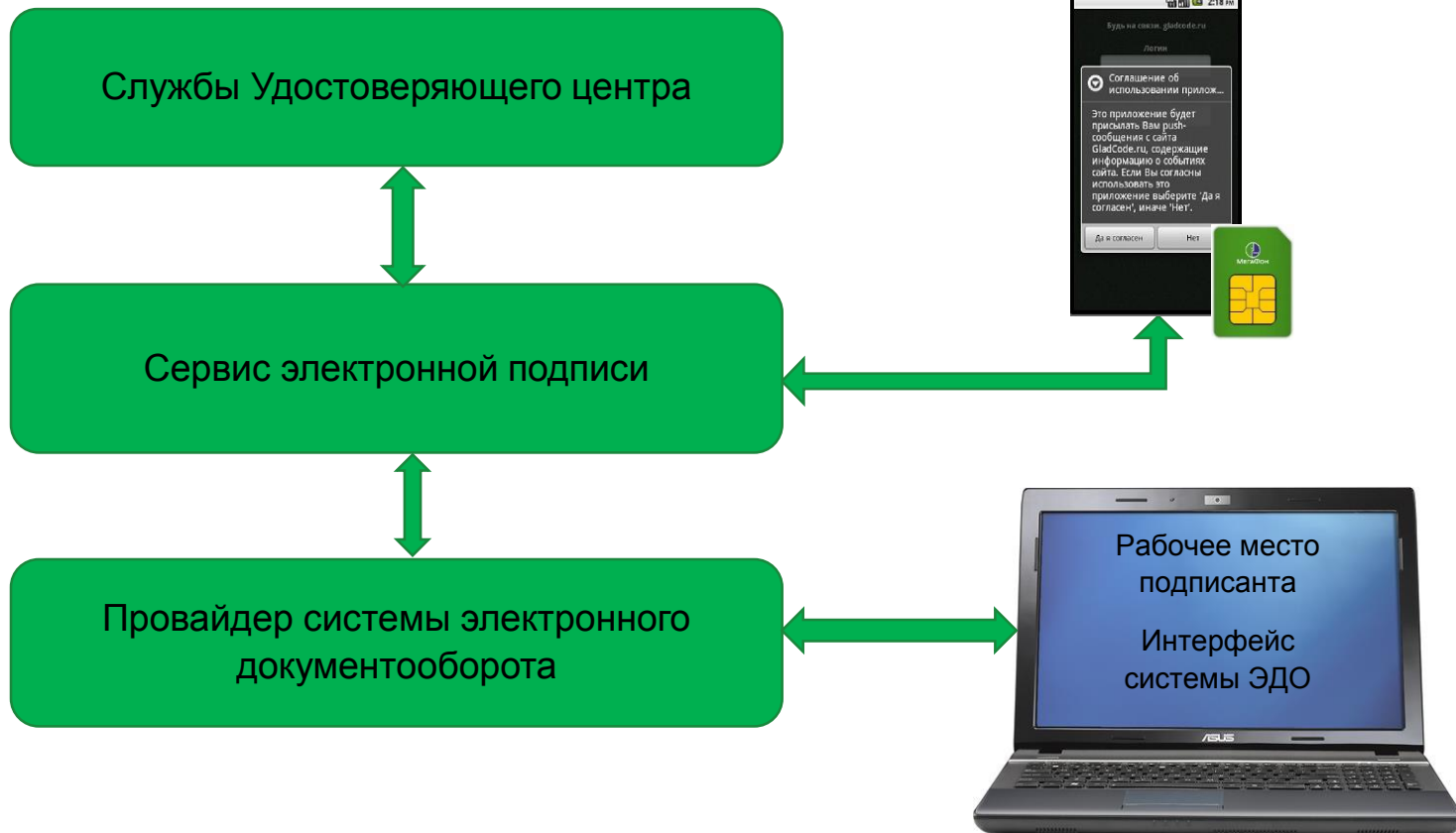
Заместитель начальника Центра по лицензированию,
сертификации и защите государственной тайны ФСБ России

А.В. Парфенов



Мобильная Электронная Подпись (МЭП)

Организация предоставления сервиса



Решение для самообслуживания сотрудника

Схема взаимодействия корпоративных систем

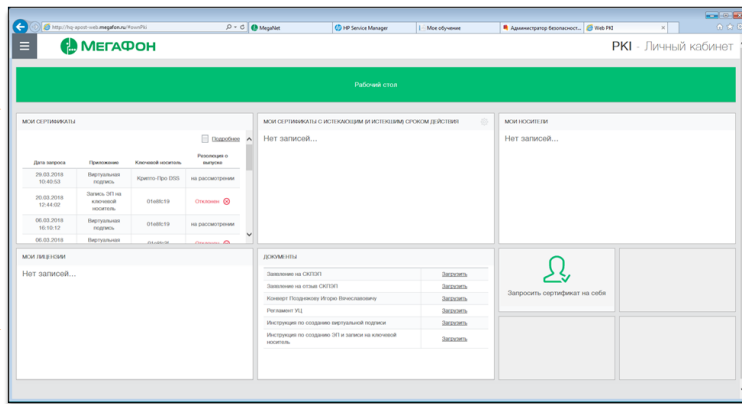
Источники данных о сотрудниках
для пред заполнения полей
сертификата ЭП



Сервер AD



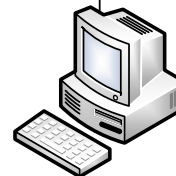
Сервер SAP HR



Сервер КриптоПро DSS



МЭП



Рабочие места сотрудников



Решение для самообслуживания сотрудника

Интерфейс личного кабинета управления сертификатами ЭП

Рабочий стол

МОИ СЕРТИФИКАТЫ

Дата запроса	Приложение	Ключевой носитель	Резолюция о выпуске
20.09.2018 10:03:45	Виртуальная подпись	natalia.kurtaeva	Установлен
19.09.2018 10:58:09	Запись ЭП на ключевой носитель	natalia.kurtaeva	Отклонен
18.09.2018 12:38:48	Виртуальная подпись	natalia.kurtaeva	Установлен
14.09.2018	Запись ЭП на		

МОИ СЕРТИФИКАТЫ С ИСТЕКАЮЩИМ (И ИСТЕКШИМ) СРОКОМ ДЕЙСТВИЯ

Нет записей...

МОИ НОСИТЕЛИ

№ носителя по производителю	Дата закрепления за сотрудником	Тип носителя	
01e8fc19	08.06.2018 15:31:09	eToken	Разблокировать
natalia.kurtaeva	16.07.2018 14:07:16	CryptoPro DSS	Разблокировать

МОИ ЛИЦЕНЗИИ

СКЗИ	Серийный номер	Ключ	АРМ
КриптоПро CSP 4.0	4040W-50000-016E1-LY2FT-3D1F9		
КриптоАрт	TD5DV-KNDQW-JFKQQ-FGKHG-VKJWF-AQJRR-XJCGX		
Администратор	CR20B-R1000-01M6D		

ДОКУМЕНТЫ

Заявление на СКПЭП	Загрузить
Заявление на отзыв СКПЭП	Загрузить
Конверт в УЦ ПАО "МегаФон"	Загрузить
Регламент УЦ	Загрузить
Инструкция по созданию виртуальной подписи	Загрузить
Инструкция по созданию ЭП и записи на ключевой носитель	Загрузить

Запросить сертификат на себя

Решение для самообслуживания сотрудника

Получение сертификата ЭП

1 Выбор шаблона 2 Выбор сопроводительных документов 3 Создание ключевого контейнера 4 Характеристики запроса на сертификат

Сотрудник:

Поздняков Игорь Вячеславович	Безопасность	ПАО "МегаФон" Головной офис ПАО "МегаФон"	Руководитель Удостоверяющего центра
------------------------------	--------------	---	-------------------------------------

Выбор шаблона: **Шаблоны сертификатов:** **Шаблоны объектов:**

Временный пользователь. (Тестовый сертификат) ▼

Описание:

Для тестирования и служебных нужд.

Временный пользователь. (Тестовый сертификат)

Отменить × Вперёд →

Инструкция по созданию виртуальной подписи Загрузить

Решение для самообслуживания сотрудника

Получение сертификата ЭП

1 Выбор шаблона 2 Выбор сопроводительных документов 3 Создание ключевого контейнера 4 Характеристики запроса на сертификат

Сотрудник:

Иванов Иван Иванович	Безопасность	Экономическая безопасность	Специалист	а
----------------------	--------------	----------------------------	------------	---

Документы, которые будут прикреплены к запросу:

Выбрать документ(-ы)

Отменить × ← Назад Вперёд →

Решение для самообслуживания сотрудника

Получение сертификата ЭП

1 Выбор шаблона 2 Выбор сопроводительных документов 3 Создание ключевого контейнера 4 Характеристики запроса на сертификат

Выбрать файл запроса файл не выбран

Название	Значение
Общее имя	ГАО "МегаФон"
Фамилия	Иванов
Имя	Иван Иванович
Страна/регион	RU
Область	52 Нижегородская область
Город	Нижний Новгород

Отменить X ← Назад Создать запрос

Решение для самообслуживания сотрудника

Получение сертификата ЭП

Дата запроса	Приложение	Ключевой носитель	Резолюция о выпуске	
17.10.2017 8:14:27	Пользователь. Тестовый сертификат. DSS	Крипто-Про DSS	Одобрено	Заккрыть

Общие сведения	
Дата запроса:	17.10.2017 8:14:27
Дата начала действия:	27.12.2017
Дата окончания действия:	27.03.2019
Дата установки сертификата:	
Дата отзыва сертификата:	

CN	Закутский Евгений Владимирович
SN	Закутский
G	Евгений Владимирович
C	RU
S	77
L	Город из свойств организации
E	evgeny.zakutsky@megafon.ru
SNILS	05525667370

Сопроводительные документы	
INN-zev11.jpg	Загрузить
pass-zev.jpg	Загрузить
SNILS-zev10.jpg	Загрузить

[Установить сертификат](#) [Получить PFX-файл](#)

[Сохранить запрос](#)

[Распечатать](#) [Показать запрос на сертификат](#) [Получить сертификат](#)

Давайте обсудим...

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

