КРИПТОПРО

Ключевое слово
в защите информации

конференция
РусКрипто

РусКрипто’2021

23 – 26 марта. Для профессионалов в криптографии и ИБ

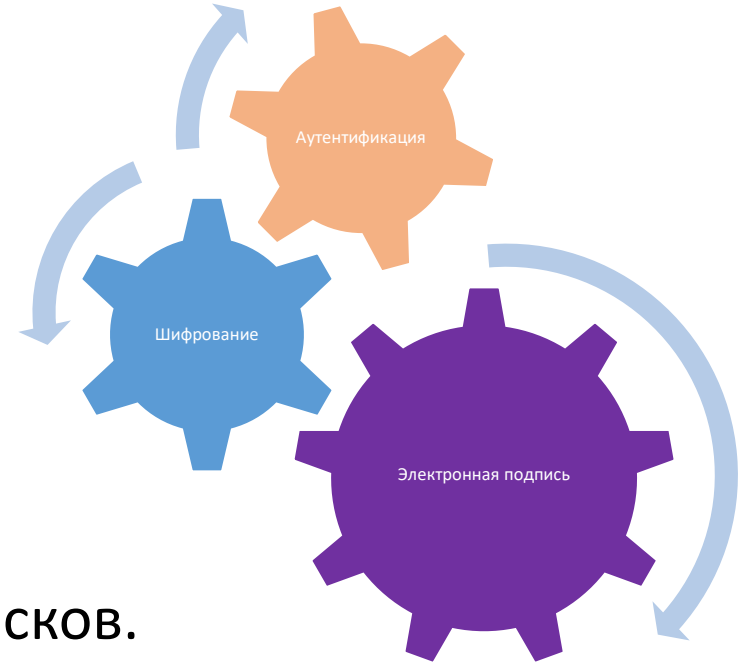
«Есть ли жизнь после монополии ГосУЦ?»

Маслов
Юрий Геннадьевич
Коммерческий директор

maslov@cryptopro.ru

Аутентификация:

- пользователей;
- компонент;
- ресурсов.



Шифрование:

- каналов связи;
- траффика;
- файлов, разделов и дисков.

Электронная подпись:

- документов;
- сообщений;
- файлов.

PKI

сертификат

УЦ

Основные этапы жизненного пути

2002

УЦ: сертификаты для ЭЦП, шифрования и аутентификации

2012

АУЦ: КСКПЭП для КЭП

Сертификаты для НЭП, для шифрования и аутентификации

2022

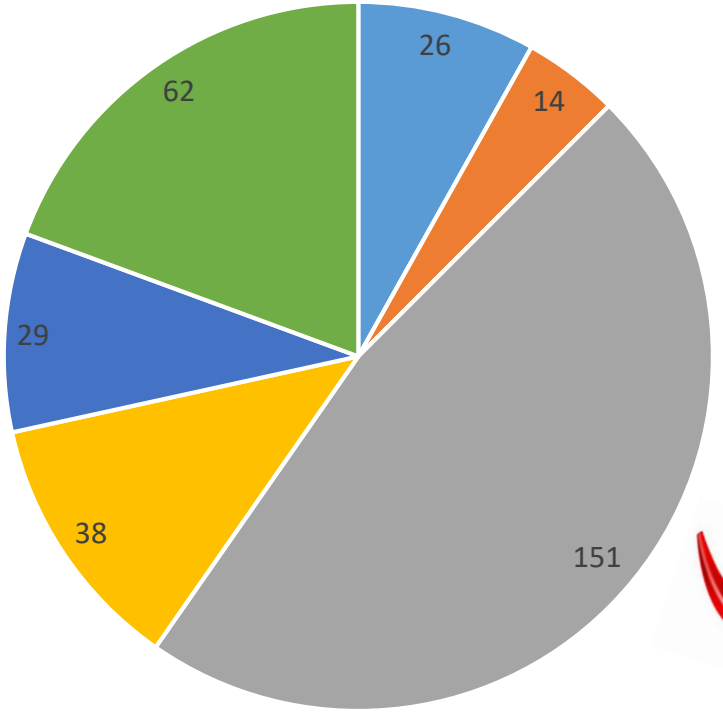
ГосАУЦ: КСКПЭП юрлиц, ИП, должностных лиц, для кредитно-финансовой сферы для КЭП

АУЦ: КСКПЭП физлиц для КЭП

Сертификаты для НЭП, для шифрования и аутентификации


ОПА, ЧЁ В СИНГУЛЯРНОСТЬ ЗАХОТЕЛ?
ПОЙДЕМ ЗА ГОРИЗОНТ СОБЫТИЙ ВЫЙДЕМ

Аккредитованные УЦ по состоянию на 12.02.2021



Пользователи

Государственные АУЦ:

- ФНС России
- Казначейство России
  - **УЦ органов власти**
  - **УЦ для органов власти**
  - **УЦ для публичных ГИС**
- Банк России

УЦ

АУЦ

Точки выдачи АУЦ

Что делать остальным УЦ?

Ближайшие годы будут расширяться ниши бизнес-возможностей поставщиков:

- сервисов обеспечения применения неквалифицированных электронных подписей
- сервисов обеспечения применения систем защищённого удалённого доступа
- сервисов поддержки документооборота
- сервисов цифровых платформ, построенных по технологии ESB (Enterprise Service Bus)

Под сервисом в рамках данного выступления понимается как непосредственно услуга, так и поставка продуктов/услуг для реализации сервиса у потребителя

Почему будет расти потребность в НЭП?

- Риски обеспечения непрерывности бизнеса, связанные с применением КЭП
- Риски нарушения коммерческой и служебной тайны
- НЭП – отличный механизм аутентификации

Какие сервисы будут востребованы на рынке и как их реализовать?

Облачная электронная подпись

- ❑ Дёшево
- ❑ Надёжно
- ❑ Гибко

Сервер электронной подписи **ПАК «КриптоПро DSS»**:

1. Любые форматы ЭП
2. Любые устройства, любые браузеры и любые ОС
3. Множество способов аутентификации:
    1. Приложение на смартфоне
    2. Апплет на SIM-карте
    3. Логин+пароль по TLS-ГОСТ
    4. Логин+пароль по SSL
    5. OTP по СМС
    6. OTP-токен
4. Возможность интеграции с СЭД через API
5. Возможность не интегрироваться с СЭД, а работать через специализированный криптопровайдер КриптоПро Cloud CSP (СКЗИ «КриптоПро CSP» версии 5.0)
6. Возможность работать через пользовательский интерфейс

Управление ключами и сертификатами

- ❑ Привычно
- ❑ Масштабируемо
- ❑ Производительно

Средство УЦ **ПАК «КриптоПро УЦ»**:

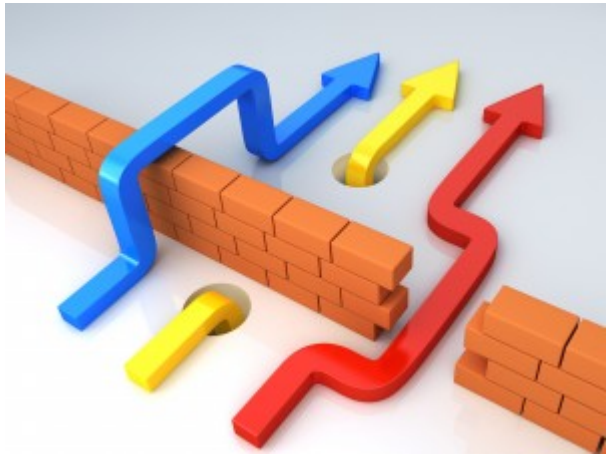
1. Доказанная работоспособность при числе пользователей свыше 15 млн
2. Доказанная производительность изготовления свыше 100 сертификатов в секунду
3. Возможность в одной инсталляции ПО поддерживать:
    1. Разные форматы сертификатов
    2. Разные регламенты получения сертификатов
    3. Разные криптографические алгоритмы издателя и владельца сертификатов
4. Один Центр Сертификации – несколько Центров Регистрации
5. Один Центр Регистрации – несколько Центров Сертификации
6. API для интеграции с внешними системами
7. API для подключения своих АРМов точек выдачи сертификатов
8. Возможность работать через пользовательский интерфейс

Сервисы штампов времени и актуальных состояний сертификатов

Службы УЦ **«КриптоПро TSP» и «КриптоПро OCSP»** :

Возможность выдавать штампы времени не только на события, связанные с электронной подписью, но и для подтверждения существования любых документированных фактов деятельности

Возможность выдавать статусы сертификатов, изданных несколькими УЦ, для упрощения процедур верификации сертификатов пользователей



С чем связан рост потребности в защищённом доступе?

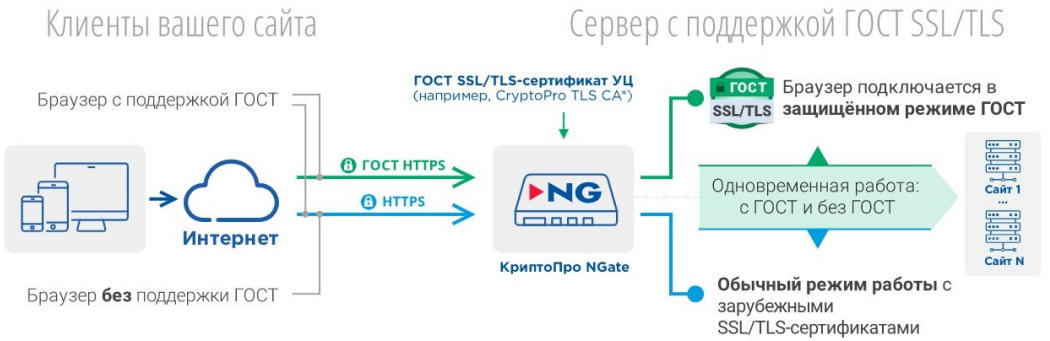
- Дистанционная работа, так же как и пандемии, пришли к нам надолго, а может и навсегда
- «В ближайшем будущем значительный объем рисков будет иметь не финансовую, а технологическую природу» - председатель Банка России Эльвира Набиуллина
- Курс на TLS ГОСТ

TLS-шлюз и VPN КриптоПро NGate

это универсальное высокопроизводительное средство криптографической защиты сетевого трафика, объединяющее в себе функционал:

TLS-сервера доступа к веб-сайтам

обеспечивается прозрачный защищённый доступ пользователей к защищаемым публичным веб-сайтам, таким как госпорталы, ЭТП, ДБО, сайты организации, с использованием браузера (до КС3)



Сервера портального доступа

для организации персонального аутентифицированного доступа пользователей с использованием браузера к опубликованным на портале NGate ресурсам

VPN-сервера

для предоставления пользователям доступа к произвольным ресурсам корпоративной сети с помощью VPN-клиента, поддерживающего все популярные платформы

Поддержка документооборота будет востребована?

- Системы документооборота – не коробочный продукт
- Рост количества разноплановых и разноплатформенных систем электронного документооборота и передачи документов с одновременным ростом потребности в их интеграции
- Экономическая целесообразность становится владельцем какого-либо сервиса появляется только при достаточно большом числе пользователей

Какие сервисы будут востребованы на рынке и как их реализовать?

Сервис обеспечения долговременного хранения документов, подписанных электронной подписью

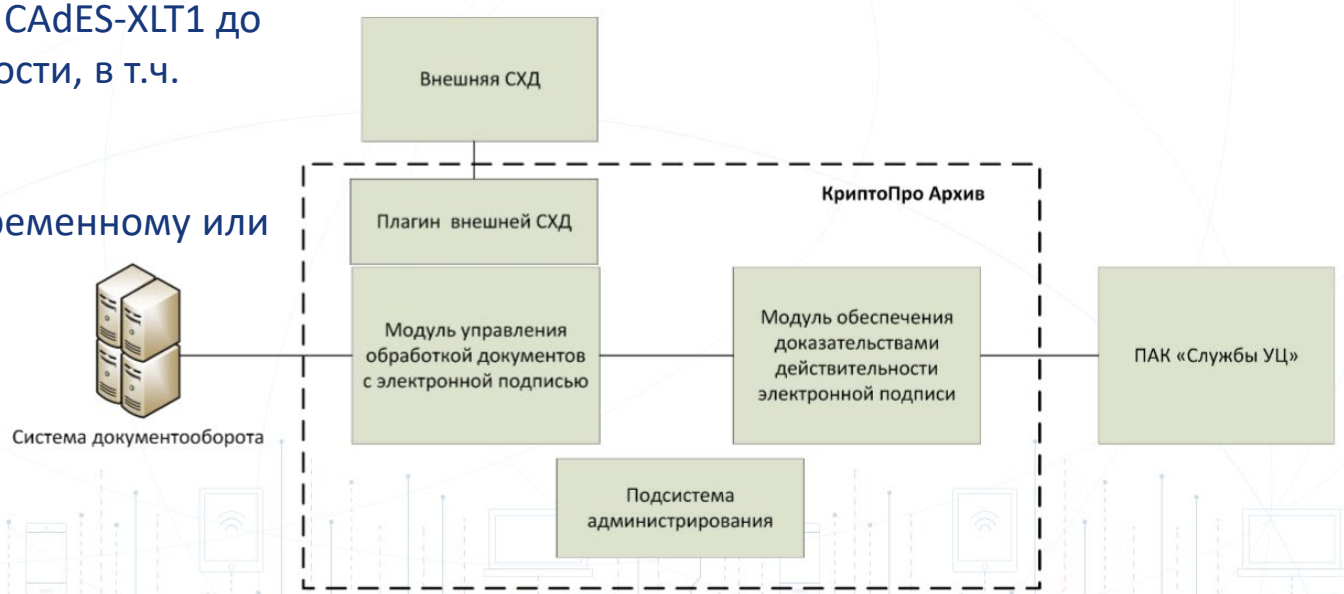
Программный комплекс «КриптоПро Архив»

Обеспечивает юридическую значимость долговременно хранящихся электронных документов, подписанных ЭП, за счет поддержания ЭП в актуальном состоянии

Усовершенствование CAdES-BES, CAdES-T, CAdES-C, CAdES-XLT1 до формата CAdES-E-A за счет доказательств подлинности, в т.ч. архивных штампов времени

Подготовка ЭП документов к временному, долговременному или постоянному хранению

Контроль сроков действия доказательств юр. значимости документов при их хранении и при необходимости их автоматическое обновление



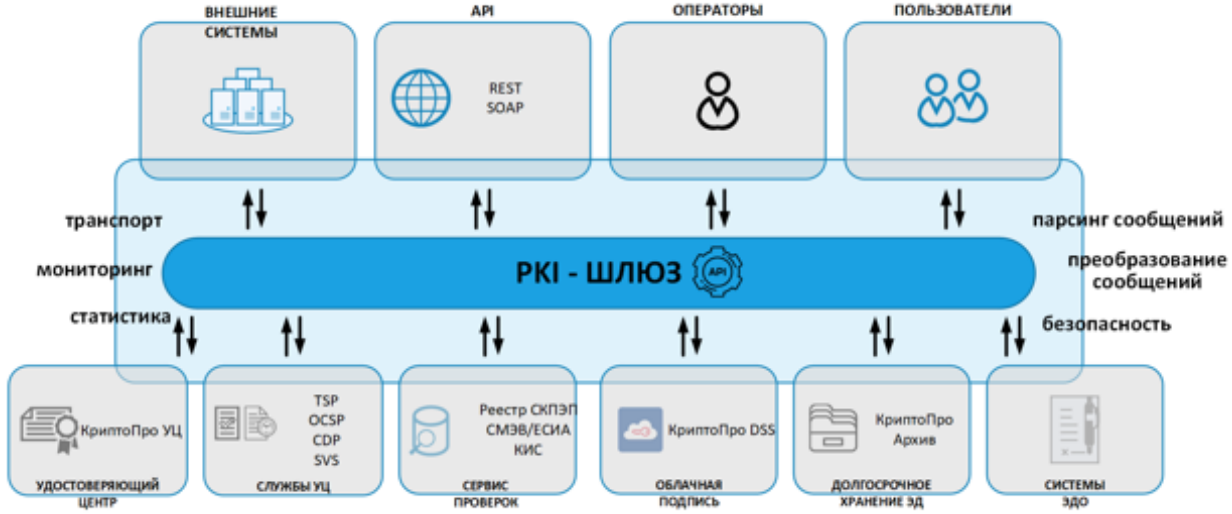
Сервис цифровых платформ

Программный комплекс «КриптоПро PKI-шлюз»

Разработан в технологии ESB (Enterprise Service Bus)

Интеграция внутренних и внешних информационных систем с обеспечением семантического контроля передаваемых сообщений с обеспечением аутентификации и авторизации взаимодействующих компонент на основе криптографических методов

Интеграция различных приложений путём установки коммуникационной шины (брокера сообщений) между ними и настройка «общения» этих приложений с шиной. Шина отделяет приложения друг от друга, позволяя им коммуницировать независимо от других приложений и даже «не зная» о существовании друг друга.



Что бы меньше рисков от действий или бездействий супостата…

Срок завершения перевода указанного ПО на отечественные ОС и СУБД – 2022-23 годы

КРИПТОПРО

Ключевое слово
в защите информации

СПАСИБО ЗА ВНИМАНИЕ!

127018, г. Москва, ул. Сущевский Вал, д.18
Тел./факс: +7 (495) 995-48-20

https://cryptopro.ru

Общие вопросы: **info@cryptopro.ru**
Контрактный отдел: **kpo@cryptopro.ru**
Для дилеров: **dealer@cryptopro.ru**