САЙФЕР

# Система криптографической защиты информации «Шифр-CaaS»

Криптография как сервис (CaaS)

ООО “Сайфер БИС”: Влад Ковтун
Александр Стокипный
Андрей Охрименко

САЙФЕР

# О компании “Сайфер”

- На рынке средств криптозащиты с 1995 года
- Лицензия ГСССЗИ Украины на производство криптосистем и средств криптографической защиты информации
- Основным направлением деятельности является разработка, внедрение и сопровождение средств криптографической защиты информационных систем в банках и других организациях

САЙФЕР

# Приоритетные продукты компании

- СКЗИ «Шифр-CaaS».
- СКЗИ «Шифр-X.509».
- СКЗИ «Персональный сервис доверительных услуг».
- СКЗИ «Сервис электронной подписи».
- СКЗИ «Сервис шифрования».
- СКЗИ «Шифр-VPN».
- СКЗИ «Шифр-PKI».

САЙФЕР

# Agenda

- Проблемные вопросы применения криптографии в организации
- Описание Шифр-CaaS
- Выгоды от внедрения Шифр-CaaS в организации
- Демонстрация работы Шифр-CaaS и Агент Шифр-CaaS
- Документация на Шифр-CaaS и Агент Шифр-CaaS
- Успешное внедрение Шифр-CaaS

# Внедрение криптографии

- Ежегодные изменение в законодательстве, почти кардинальные
- Внесение изменений в различные автоматизированные системы (как следствие)
- Поддержка различных платформ, в том числе и мобильных
- Сложность понимания глубинных вопросов криптографии разработчиками сторонних систем при интеграции
- Поддержка широкого спектра алгоритмов и форматов данных
- Поддержка различных ЦСК/АЦСК/КПЭДУ от различных производителей, с учетом их специфики

# Внедрение криптографии

- Необходимость поддержки различных защищенных носителей:
  - Смарт-карт и USB токенов
  - Электронный паспорт гражданина украины
  - Network HSM
- Необходимость в интеграции с web-приложениями
- Обеспечение высокой производительности при пиковых нагрузках (окончание банковского дня)
- Управление доступом к различным криптографическим механизмам
- Растущая потребность в около-криптографических сервисах, для обеспечения безопасности и удобства работы
- Соответствие современным тенденциям развития ИТ

# Шифр-CaaS. Описание

- Набор микросервисов, которые позволяют легко выполнять криптографические операции, используя ключи электронной подписи и шифрования разных Квалифицированных предоставителей электронных доверительных услуг (КПЭДУ/АЦСК)
- Взаимодействие Шифр-CaaS с автоматизированными бизнес-системами, которые нуждаются в криптографических преобразованиях, обеспечивается через разработанный интерфейс взаимодействия (REST API)
- Возможность расширения возможностей существующего REST API, без необходимости обновления приложений, использующих его

# Шифр-CaaS. Описание

- Расширение возможностей посредством добавления дополнительных модулей:
  - Модуль по работе MobileID Vodafone
  - Модуль по работе MobileID LifeCell
  - Модуль по работе MobileID Kyivstar (ожидается)
  - Модуль интеграции UKey (ожидается)
  - Модуль формирования и анализа защищенных QR-кодов
  - Модуль вычисления хеш-функций (ГОСТ 34.311-95, SHA-1, SHA-2, ДСТУ 7564:2014)
  - Модуль интеграции с Active Directory
  - Могут быть разработаны различные интеграционные модули под заказ

# Шифр-CaaS. Описание

- Расширение возможностей посредством интеграции с внешними системами:
  - Система Шифр-Auth для ограничения доступа к API посредством JSON Web Token (JWT)
  - Система криптографической защиты (ЦСК) Шифр-X.509, для автоматизации механизмов генерации и смены ключей

# Шифр-CaaS. Описание

- Поддержка защищенных носителей:
  - Автор SecureToken-337, SmartCard-337
  - AvestKey, EfitKey
  - ИИТ Алмаз-1К, Кристалл-1
  - Gemalto eToken, IDPrime
  - Thales Luna HSM Network (ожидается)
  - И др.

САЙФЕР

# Шифр-CaaS. Алгоритмы

- Поддерживаемые национальные алгоритмы:
  - ДСТУ 4145-2002
  - ГОСТ 34.311-95
  - ДСТУ ГОСТ 28147:2009

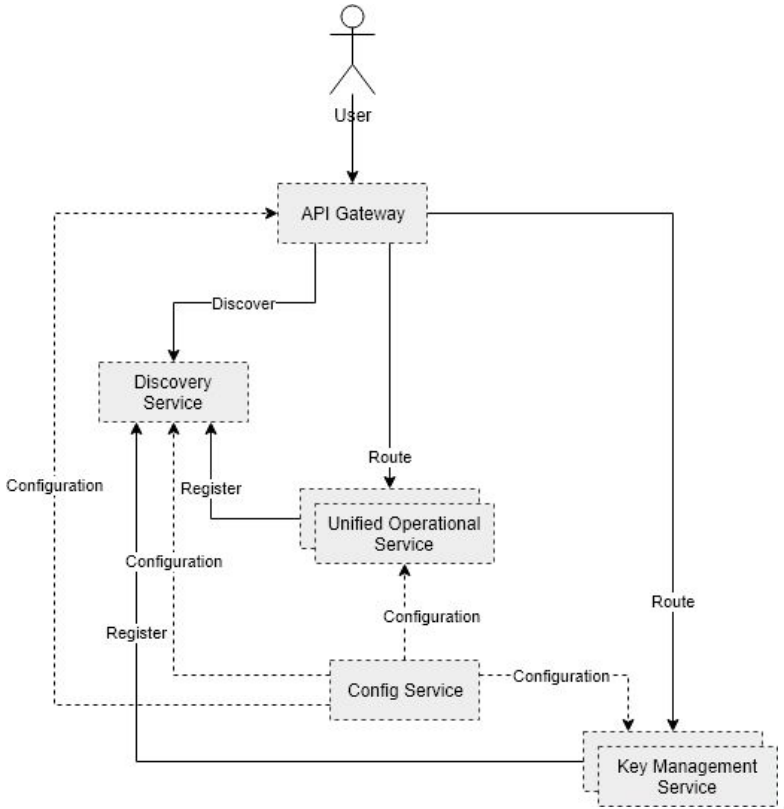
САЙФЕР

# Шифр-CaaS. Возможности

- Электронная подпись
  - Тип: Прикрепленная и открепленная
  - Формат: CAdES-BES, CAdES-T, CAdES X-Long и другие
  - Один конверт - много подписей
  - Вложенные подписи (добавление подписей к существующим, проверка всех подписей)
  - Расширение подписей до CAdES X-Long
- Направленное шифрование

# Шифр-CaaS. Архитектура

- Шифр-CaaS поставляется в виде образов Docker из репозитария компании Сайфер
- Образы разворачиваются в среде оркестрирования Docker Swarm либо Kubernetis
- Дополнительные сервисы поставляются в виде отдельных Docker контейнеров



# Выгоды от внедрения Шифр-CaaS

- Удобное и простое API для интеграции в сторонние автоматизированные система. Подробная документация и примеры. Наличие демонстратора технологии
- Централизованное обновление криптографических библиотек и примитивов
- Централизованное масштабирование ресурсов, а не “размазанность” их по различным системам
- Поддержка всех возможных клиентских платформ и технологий (даже мобильные, без аппаратных ограничений)
- Возможность интеграции с web-приложениями
- Генерация и смена ключей в интерактивном режиме (СКЗИ Шифр-X.509)

САЙФЕР

# Выгоды от внедрения Шифр-CaaS

- Серверная часть разворачивается на ОС Linux
- Высокая скорость выполнения криптографических операций
- Интуитивный интерфейс в работе с электронной подписью и шифрования данных
- Реализация механизмов идентификации согласно BankID НБУ

# Авторские права и заключения

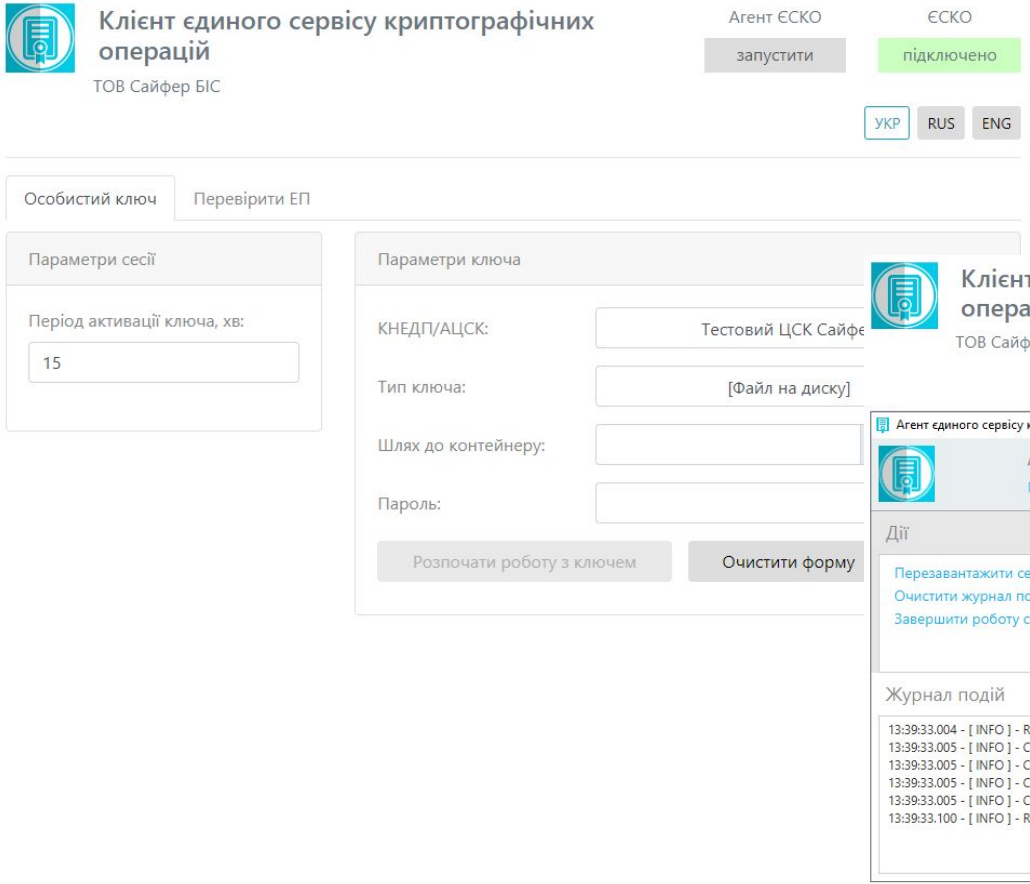
- Шифр-CaaS имеет авторское свидетельство Министерства экономического развития и торговли Украины 31.05.2019 №89189
- Шифр-CaaS построен на основе:
  - Библиотек криптографических примитивов Шифр+ v2.1, которые имеют позитивное экспертное заключение Госспецсвязи Украины от 16.05.2017 №04/03/02-1674
  - Библиотек Java из состава СКЗИ Шифр-X.509, которые имеют позитивное экспертное заключение Госспецсвязи Украины от 01.02.2017 №04/03/02-302

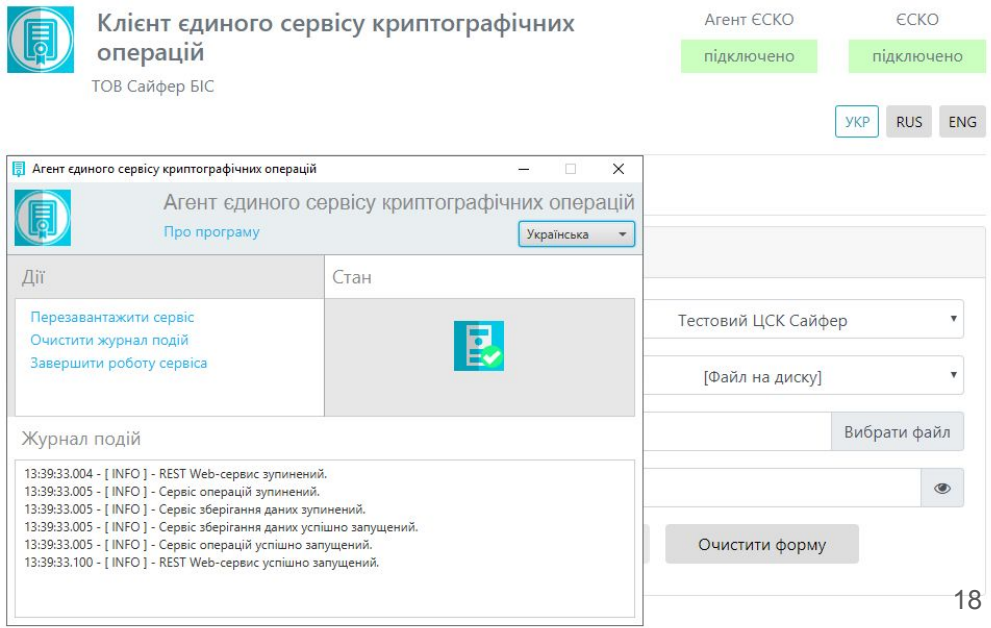
# Демонстрация работы Шифр-CaaS и Агента

https://cryptocenter.cipher.kiev.ua

САЙФЕР

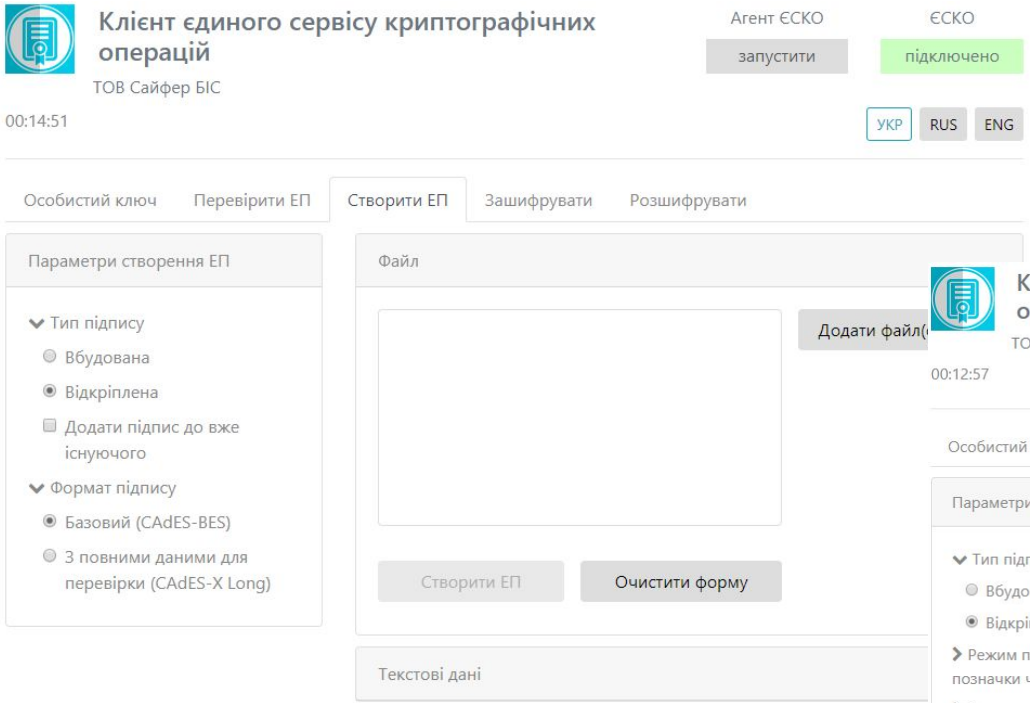
# Демонстрация работы Шифр-CaaS и Агента

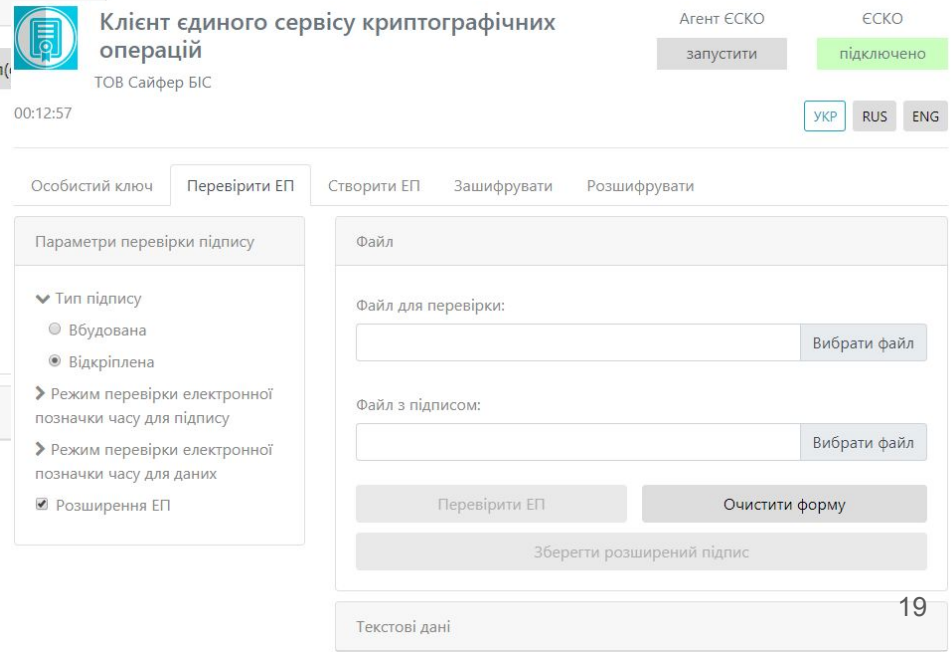


# Демонстрация работы Шифр-CaaS и Агента

САЙФЕР



# Документация на Шифр-CaaS и Агент

Документация (API):

- Шифр-CaaS
- Агент Шифр-CaaS

Инструкции и видеоинструкции пользователя:

- Шифр-CaaS
- Агент Шифр-CaaS

Автоматизированные тесты:

- Шифр-CaaS
- Агент Шифр-CaaS

Поддерживаемые АЦСК/КПЭДУ:

- Шифр-CaaS

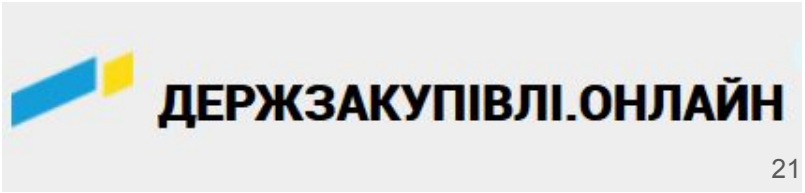
САЙФЕР

# Шифр-CaaS уже успешно внедрен

- АО "КРЕДОБАНК"
- АО "ПИРЕУС БАНК"
- АО "БАНК АЛЬЯНС"
- ООО "МОРИОН"
- ООО "Держзакупівлі.Онлайн"
- И др.







САЙФЕР

# Контакты

Александр Стокипный: as@cipher.com.ua

Андрей Охрименко: ao@cipher.com.ua

Влад Ковтун: vk@cipher.com.ua

www: https://cipher.com.ua