

Финтехрешения «Современных систем»: ЕБС, цифровой профиль. Готовность – 2025



Евгений Захуцкий,
коммерческий директор
«Современные системы»

Система «Взаимодействие с государственными органами»

Программное обеспечение системы «Взаимодействие с государственными органами» включено в Единый реестр российских программ для электронных вычислительных машин и баз данных.

[Запись в реестре N 11623 от 28.09.2021](#) произведена на основании приказа Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации [от 27.09.2021 N 1011](#).



Решения для взаимодействия с госорганами

Взаимодействие со СМЭВ

ФНС, ФССП, Equifax, ОКБ, НБКИ, ЕФРСБ, ЕИСН, ГИС ГМП, ГИС ЖКХ, ЕГРЮЛ / ЕГРИП, ПФР, Минсельхоз, ГУВМ МВД, Одно окно, ЕСИА и т. д.

ЭДО с ФНС (440-П, 311-П)

Поддержка маршрутно-транспортной логики при обмене, криптография и мониторинг сообщений

Взаимодействие с ЕСИА/ЕБС

Решение по регистрации и удаленной идентификации биометрических образцов в ЕБС. Соответствие всем требованиям по ИБ

Взаимодействие с цифровым профилем

Решение по получению данных из цифрового профиля ЮЛ и ФЛ

Криптомодуль/ Криптоадаптер для расчета с ЦБ

Поддержка ЗСК, ЭДО, поддержка УФЭБС, СКЗИ

Взаимодействие с платформой цифрового рубля

Транспортная часть + криптография в части обмена с ПЦР, исследования в ФСБ

Маркетплейсы. Взаимодействие с финансовыми платформами

Московская биржа, Банки.ру, Сравни.ру

Типичные проблемы офицеров ИБ при работе с сертификатами

Основные проблемы

Управление жизненным циклом сертификатов

Сложность отслеживания сроков действия сертификатов
Пропуск момента своевременного отзыва сертификатов
Отсутствие автоматизации перевыпуска после отзыва

Распределение и учет ключей

Нет точного учета объектов, где хранятся закрытые ключи
Сложности при определении места для подкладывания новой ключевой пары после выпуска

Взаимодействие с клиентами и серверами

Отсутствие четкой привязки клиентов к серверным компонентам
Необходимость оповещать клиентов о замене цепочек сертификатов
Учет клиентов, взаимодействующих с сервером (например при изменении сертификата)

Ручные процессы и человеческий фактор

Зависимость от ручного ввода данных (риск ошибок)
Отсутствие автоматизированных сценариев для массовых операций

Типичные проблемы офицеров ИБ при работе с сертификатами

Интеграция с инфраструктурой

Сложности при работе с HSM (настройка, обновление ключей)
Несовместимость форматов сертификатов между системами

Другие частые проблемы

Аудит и отчетность

Неполный аудит действий с сертификатами (кто, когда, зачем)
Отсутствие централизованного журнала отозванных и выпущенных сертификатов

Безопасность ключей

Риск утечек закрытых ключей из-за некорректного хранения
Отсутствие ротации ключей в соответствии с политиками

Доверенные УЦ и цепочки

Проблемы с доверенными удостоверяющими центрами (например истечение срока действия их сертификатов)
Отсутствие резервных копий цепочек сертификатов

Модуль по работе с сертификатами

Модуль автоматически формирует запросы в удостоверяющий центр (УЦ)

Аутентификация через ЕСИА

Для выпуска сертификатов:

- ФЛ (физические лица) – обязательна аутентификация в ЕСИА
- ЮЛ (юридические лица) – аутентификация владельца сертификата в ЕСИА

В сертификате ЮЛ указывают лицо, уполномоченное действовать без доверенности

Типы сертификатов

Серверный сертификат

- не требует указания лица
- не требуется аутентификация в ЕСИА
- привязка к конкретной системе обязательна

Сертификат для ФЛ

- аутентификация через ЕСИА

Сертификат для ЮЛ

- аутентификация через ЕСИА
- указывается уполномоченное лицо

Доставка сертификатов

на устройство клиента – для ФЛ и ЮЛ
на сервер – для серверных сертификатов

Централизованное управление сертификатами

Уведомления и автоматизация

Возможность отправки уведомлений клиентам

Для серверных сертификатов:

- автоматический перевыпуск
- подкладывание сертификатов в цепочку без участия клиента

Перевыпуск сертификатов

Для ФЛ и ЮЛ – требуется запрос от клиента на перевыпуск

Для серверных сертификатов – перевыпуск происходит автоматически

Интеграция с HSM

Модуль по работе с сертификатами может быть установлен рядом с HSM для повышения безопасности

- возможность установки агента на серверы, где хранятся ключи

Настройка цепочки событий

Гибкая настройка оповещений:

- уведомления о скором истечении срока действия сертификатов
- оповещения об успешном перевыпуске или ошибках



Реализация протокола OpenID Connect и выпуск сертификатов с учетом 63-ФЗ

1. Реализация OpenID Connect

Аутентификация через OIDC:

- использование протокола для безопасной идентификации пользователей
- получение JWT-токена с данными о пользователе

Связь с выпуском сертификатов:

- данные из токена OIDC автоматически передаются в модуль для формирования сертификата

2. Выполнение требований 63-ФЗ

Ключевые аспекты:

- надежная аутентификация пользователя перед выпуском сертификата
- фиксация уполномоченных лиц для ЮЛ
- гарантия соответствия форматам и алгоритмам, утвержденным регулятором

3. Функция определения личности

Процесс верификации:

- пользователь аутентифицируется через OIDC (ЕСИА)
- модуль проверяет полученные данные
- на основе данных формируется запрос в УЦ для выпуска сертификата

Поддержка сценариев:

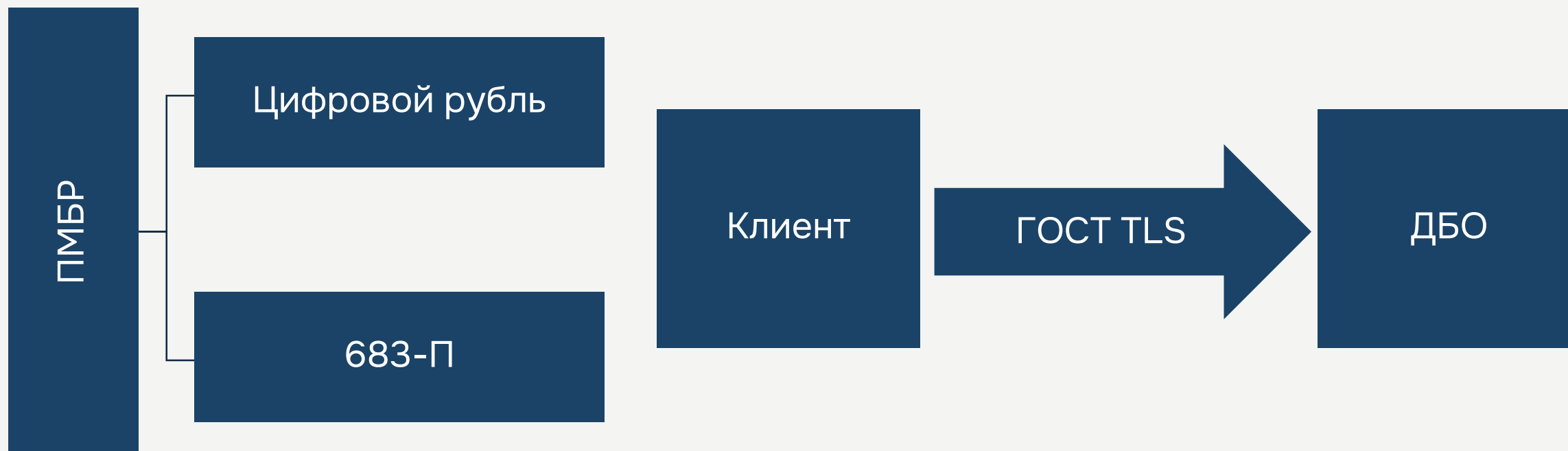
- для ФЛ – привязка сертификата к физическому лицу
- для ЮЛ – указание уполномоченного представителя в сертификате

Дополнительные функции модуля по работе с сертификатами

Сервис проверки
подписи

Отчетность

Реализация требований 683-П



Буду рад ответить на ваши вопросы



Евгений Захуцкий,
коммерческий директор
«Современные системы»

e.zakhutskij@modernsys.ru

+7 916 700 15 75