Наименование задачи (проекта)
Разработка веб-системы подписания документов электронной подписью OpenPGP

Цель и описание задачи (проекта)
Разработать клиент-серверное веб-приложение для подписания документов электронной подписью OpenPGP с локальным использованием закрытого ключа в браузере и серверной проверкой подписи. Основной сценарий: внешняя информационная система передает документ и email получателя через API. Сервис проверяет наличие зарегистрированного открытого ключа получателя, сохраняет документ и создает заявку на подписание. Пользователь входит через существующую инфраструктуру Keycloak, видит доступные ему документы, может скачать документ и подписать его в браузере. На сервер передается отдельный файл подписи. После успешной проверки сервис сохраняет исходный документ, подпись и сведения о завершении операции. Передающая система получает состояние заявки через API.
Регистрация открытого ключа выполняется авторизованным пользователем. Ключ привязывается к его учетной записи и подтвержденному email из Keycloak. Закрытый ключ и пароль к нему должны оставаться исключительно в оперативной памяти браузера, без передачи на сервер и сохранения в постоянном хранилище браузера.
Дополнительно требуется отключаемый тестовый режим: пользователь выбирает локальный документ, подписывает его в браузере и получает результат серверной проверки. Тестовые документы и подписи после проверки удаляются; открытый ключ хранится только на время тестовой сессии.
Решение должно работать в актуальных браузерах на Windows, macOS и Linux без установки расширений, GPG или вспомогательных приложений.

Описание проблемы
Необходимо обеспечить единый процесс передачи документов из информационных систем на подписание конкретному пользователю, проверки полученной подписи и сохранения результата. Процесс должен гарантировать, что пользователь подписывает точные байты переданного документа, доступ к документу имеет только уполномоченный получатель, а система сообщает об успешном завершении только после надежного сохранения документа и подписи.
Также необходимо исключить передачу закрытых ключей на сервер, предотвратить подмену документов и открытых ключей, обеспечить повторные попытки при ошибках и сохранность заявок при сетевых сбоях, перезапуске сервиса или ошибках хранилища.

Ожидаемый эффект
Создание сервиса, позволяющего информационным системам направлять документы на подписание и отслеживать результат через API, а пользователям — подписывать документы в браузере без установки дополнительного ПО.
Ожидаемые результаты:

- Единый управляемый процесс: передача документа, ожидание подписи, проверка и сохранение результата.
- Подтверждение целостности подписанного документа: изменение его байтов приводит к отклонению подписи.
- Хранение закрытых ключей и паролей исключительно на стороне пользователя.
- Разграничение доступа к документам и операциям через Keycloak.
- Защита от перезаписи завершенных результатов и потери документов при сбоях.
- Возможность независимой проверки сохраненной пары «документ — подпись» совместимыми средствами OpenPGP.

Техническое задание
Предусмотренный стек: клиент — HTML, TypeScript и OpenPGP.js; сервер — Go, net/http и GopenPGP v3; аутентификация пользователей и приложений, а также разграничение прав — через существующую инфраструктуру Keycloak. Для хранения достаточно серверной файловой системы; база данных не обязательна.
Обязательные требования:

- Формирование отдельной бинарной подписи над точными исходными байтами документа и проверка совместимости клиентской и серверной криптографических библиотек.
- Сохранение неизменного документа на время ожидания подписи.
- Атомарное сохранение документа, подписи и метаданных без публикации частичного результата и перезаписи завершенных заявок.

- Восстановление после сбоев и корректная обработка одновременных попыток подписания.
- HTTPS, строгая политика CSP, отсутствие сторонних скриптов на страницах подписания, ограничения размеров запросов и защита файлового хранилища.
- Изоляция тестового режима от рабочего контура. Тестовый режим по умолчанию отключен.
- Отображение пользователю результатов операций и понятных сообщений об ошибках.

Email-уведомления и вебхуки в объем разработки не входят. Информационные системы проверяют состояние заявок через API.

Рекомендуется включить в договор передачу исходного кода, инструкций по сборке, настройке и развертыванию, описания API и результатов приемочных испытани. В предложении подрядчика необходимо указать сроки, стоимость, этапы работ, требования к инфраструктуре и условия гарантийного исправления дефектов.