Общие положения

Декомпозиция сервисов

1. Сервис Аутентификации - "Цифровой паспорт НК"
2. Сервер документооборота - Центральное хранилище документов
3. Цифровой СПК
4. Цифровой ЦОК
5. Социальная сеть Я-Эксперт
6. Мониторинг регионов ФЗ: обучение
7. Конструктор проф стандартов и ОС

Все сервисы являются взаимосвязанынми, для целей аутентификации используется единый OAuth2 сервис «Цифровой паспорт "Национальные Квалификации"»

Объектная модель сервисов

Цифровой паспорт АО НК

Цифровой паспорт реализует полную модель OAuth2 аутентификации. Включая выдачу списка ролей, доступных пользователю. OAuth2 токен используется для Baerer механизма аутентификации и по умолчанию выдается на срок 24 часа. Однако может быть запрошен и на больший срок, но не более 30 календарных дней с даты получения токена. Сервер аутентификации формирует Baerer как base64 от json структуры: Профиль пользователя, Привилегии доступа, Подпись сервера аутентификации. При запросе делегирования токена, данные токена дополнительно разбавляются солью и шифруются хешем пинкода пользователя. Для получения делегированного токена пользователь должен правильно ввести пинкод. Примером использования делегированного токена является МАК, где значение ключей не велико и возможна аутентификация эксперта только по пинкоду. В иных случаях требуется допонительно к делегированному токену хранить идентификатор пользователя. Пример:

1. Эксперт регистрируется в цифровом паспорте АО НК
2. СПК присваивает эксперту статус Эксперта и назначает права доступа в ЦОК
3. Эксперт проходит аутентификацию на портале ЦОК (в закрытой сети)
4. ЦОК запрашивает обычный и делегированный токен сроком на 30 дней
5. Цифровой паспорт добавляет к токену соль, шифрует его хешем пинкода пользователя и отправляет на сервер ЦОК.
6. Сервер ЦОК реплицирует полученный делегированный токен на МАК
7. На планшете эксперта подключенному к МАК Эксперт вводит персональный пинкод
8. МАК перебирает хранимые токены экспертов и пытается расшифровать их с помощью хэша пинкода эксперта
9. Если расшифрованный токен проходит проверку подлинности (без соли), токен принимается как токен эксперта. Аутентификация пройдена.
10. Полученный токен используется клиентом для аутентификации как на сервере МАК, так и на сопуствующих сервисах, таких как виртуальный узел сети блокчейн.

Версия #2
★Баталин Иван Анатольевич создал 2 апреля 2024 03:01:55
✎Баталин Иван Анатольевич обновил 2 апреля 2025 06:40:10