Подписание документов простой электронной подписью

Оглавление

RooX UIDM позволяет подписывать документы и операции клиента для того, чтобы в последствии можно было доказать выполнение операции.

Документом является как традиционный "документ", например, платежное поручение, так и вообще любая операция клиента в системах самообслуживания.

Примеры:

1. Переписка клиента с Банком - каждое сообщение это документ, содержащий тело сообщения и вложения
2. Включение входа через 2 фактор - это "документ", телом которого является новый номер телефона
3. Заявление на предоставление кредита
4. Смена/назначение пин-кода карты
5. Подключение нового тарифа
6. Смена типов подписи

ЗАМЕТКА

RooX UIDM не накладывает ограничений на то, чем является документ и какими характеристиками он обладает.

Сценарии

Подписание документа через простую электронную подпись через СМС

1. Клиент инициирует операцию в веб или мобильном приложении самообслуживания
2. Backend приложения самообслуживания формирует документ, соответствующего операции Документ состоит из основного содержимого (например, тела заявления) и метаданных в формате ключ-значение.
3. Backend запрашивает у RooX UIDM подписание документа, передавая документ, текущий access token клиента и

учетные данные себя, как приложения

4. RooX UIDM сохраняет в свою БД тело и метаданные, назначает идентификатор, возвращает его backend'у
5. RooX UIDM генерирует одноразовый пароль, отправляет СМС-сообщение с ним
6. Клиент вводит одноразовый пароль, backend транслирует его в RooX UIDM
7. RooX UIDM сверяет введенный одноразовый пароль
8. Если одноразовый пароль введен верно, RooX UIDM производит подписание документа и метаданных по заданному алгоритму. В алгоритме обязательно участвует тело документа (либо его хешсумма, если документ слишком велик для сохранения в БД), метаданные документа, номер телефона, на который был отправлен одноразовый пароль, сам одноразовый пароль. Вычисленная подпись сохраняется рядом с документом.
9. RooX UIDM возвращает одноразовый access token, разрешающий выполнение запрашиваемой операции (токен под операцию)
10. Backend выполняет операцию, используя одноразовый access token
11. RooX UIDM записывает в таблицу аудита событие "доступа к защищаемому ресурсу"

ЗАМЕТКА

Возможно подписание нескольких документов одним запросом

Модель данных

SigningRequest - запрос на подписание

Группирует документы, подписываемые в рамках одного пользовательского действия.

Если в рамках пользовательского действия выполняется всего лишь одна операция, то SigningRequest все равно существует.

Содержит ссылку на принципала (клиента, FK на Principal), медатанные о запросе на подписание в формате ключ-значение, дату создания. Идентификатор является глобально уникальным и назначается RooX UIDM.

Идентификатор запроса на подписания кладется в клеймы `токена под операцию` и записывается в аудит. Это важный идентификатор, по которому в дальнейшем производится сопоставление действий.

Document - документ (совершаемая операция в формате документа)

Подписываемый документ или операция в формате документа.

Содержит полезные данные (тело), метаданные в формате ключ-значение, ссылку на родительский запрос на подписание, внешний идентификатор документа (назначаемый системой-владельцем документа), дату создания, MIME-тип тела.

Как формировать тело?

В случае подписания документа - телом является само бинарное содержимое документа. В теле документа-операции должна содержаться вся существенная информация об операции. В случае платежного поручения это будут реквизиты получателя, реквизиты плательщика, сумма, назначение платежа.

Рекомендуется составлять тело одинаковым алгоритмом для всех операций, например, выстроить все значимые данные в алфавитном порядке и сконкатенировать в одну строку. Перед получившейся строкой или в метаданные добавить версию алгоритма, поскольку в дальнейшем вы можете его изменить.

Что сохранять в метаданных

Метаданные это пары ключ-значение, которые так же могут содержать существенную информацию об операции или документе. Метаданные участвуют в формировании подписи, и по ним также обеспечивается неотказуемость.

Телом документа может быть бинарное содержимое, а ключ и значение метаданных - всегда строка.

Текст СМС-сообщения может быть шаблонизирован с подстановкой значений из метаданных запроса на подпись.

Signature - подпись документа

Содержит ссылку на подписываемый Document, ссылку на принципала (клиента), наименование алгоритма, дату подписания, вычисленное значение подписи, учетные данные, специфичные для алгоритма.

Особенности и ограничения

1. Для документов с размером тела больше, чем 2000 байт, вместо тела сохраняется хешсумма (согласно выбранному в конфигурации алгоритму). Это работает прозрачно внутри RooX UIDM.
2. Метаданные сохраняются в поле с форматом JSON. При применении JSON-индекса возможен поиск по ключам (по умолчанию не применен)
3. Поиск по телу документа не предусматривается
4. Общая длина метаданных не может быть больше 2000 байт (ограничение можно увеличить; значение по умолчанию выбрано с учетом, чтобы данные не попали в LOB)
5. В текущей версии RooX UIDM API поддерживает наложение только одной подписи, но модель данных БД поддерживает цепочку подписей
6. RooX UIDM не определяет, каким пользователям разрешено подписывать документы, пользователь с текущим access token может подписывать любые документы среди тех, которые он создал сам

Алгоритм OtpGost3411_2012_512DigestSigningStrategy

Это простая электронная подпись - ПЭП. Одноразовый код генерируется генератором случайных чисел на сервере RooX UIDM, длина кода настраивается, код имеет время жизни, каждое сообщение пронумеровано, счетчик сбрасывается в полночь.

Учетными данными, участвующими в расчете подписи помимо документа и метаданных являются:

1. номер телефона (нормализованный согласно E.164 без знака +, например 79001234567)
2. введенный OTP-код (например, 12345)
3. порядковый номер СМС-сообщения (например, 12)

Подпись представляет собой хешсумму, рассчитанную по алгоритму ГОСТ 34.11-2012, длина 512 бит.

Как подтвердить, что клиент действительно выполнил операцию

Следует выгрузить из таблицы аудита `OperationAudit` следующую цепочку событий:

1. Аутентификация (вход пользователя по логину паролю или другому методу) - `sso.auth.success`. Искать по дате и principalId.
2. Авторизация запроса на подписание `sso.auth.protected.resource.success.access`. В поле data в xml-формате лежит идентификатор запроса на подписание sign_req_id=sso_7264abba-72e9-47f8-b591-9ecb9ed3f3e9 и подпись

sign=YmdFq+rzcwVWDBbOHUo95HK0Wy0m2czXSCzBQox4D8v38asP9TTHijTcoeMSizpDxFlwJCT6+DbZ99eu0Qs+6A==

3. По sign_req_id найти Document, затем их Signature
4. Вычислить подпись заново согласно алгоритму
5. Сравнить получившуюся подпись и сохраненную в Signature

Прочтите также

- Соответствие простой электронной подписи RooX UIDM требованиям законодательства
- Руководство по финансовым операциям и электронной подписи