РусКрипто

XXVII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

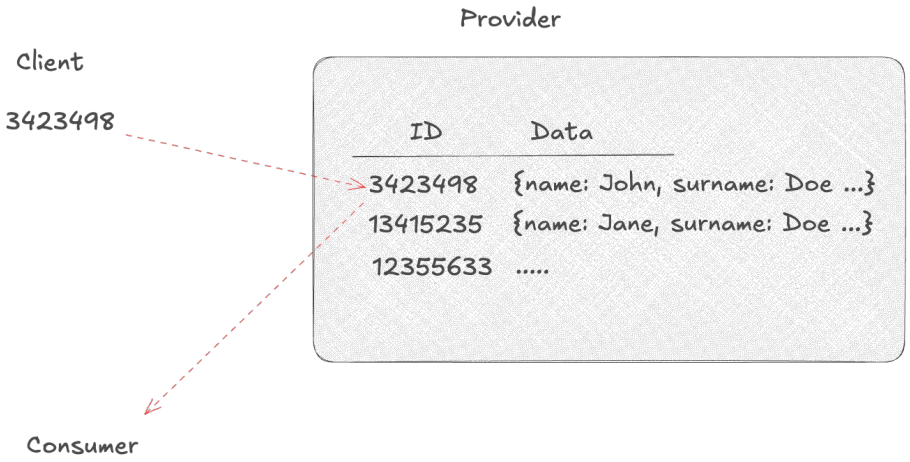
Предпосылки

- Для доступа к некоторым сервисам и товарам нужна авторизация, то есть проверка свойств пользователя:
  - Пользователь - человек?
  - Возраст $\geq X$
  - Гражданство $\in$ […]
  - …
- Авторизацию часто осуществляет сторонний провайдер
- Идентификация или аутентификация не всегда возможны или целесообразны

РусКрипто

Примеры

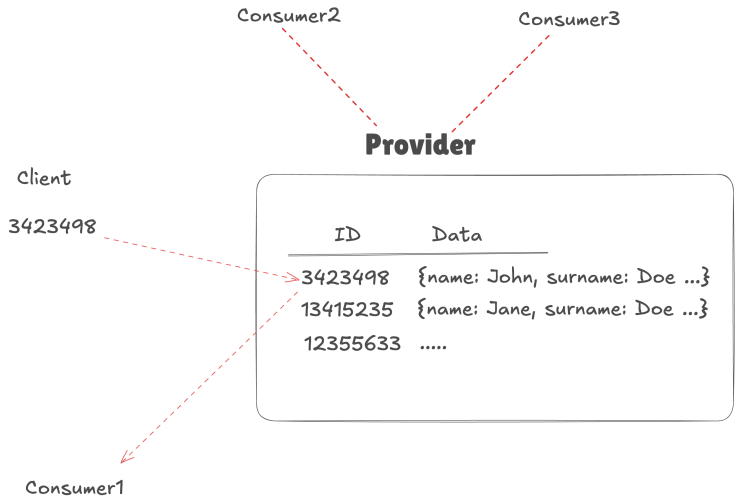
- Телеком: защита от спама
- Финансы: доступ к инвестиционным продуктам
- Розница и e-commerce: продажа алкоголя, энергетиков и других товаров



РусКрипто

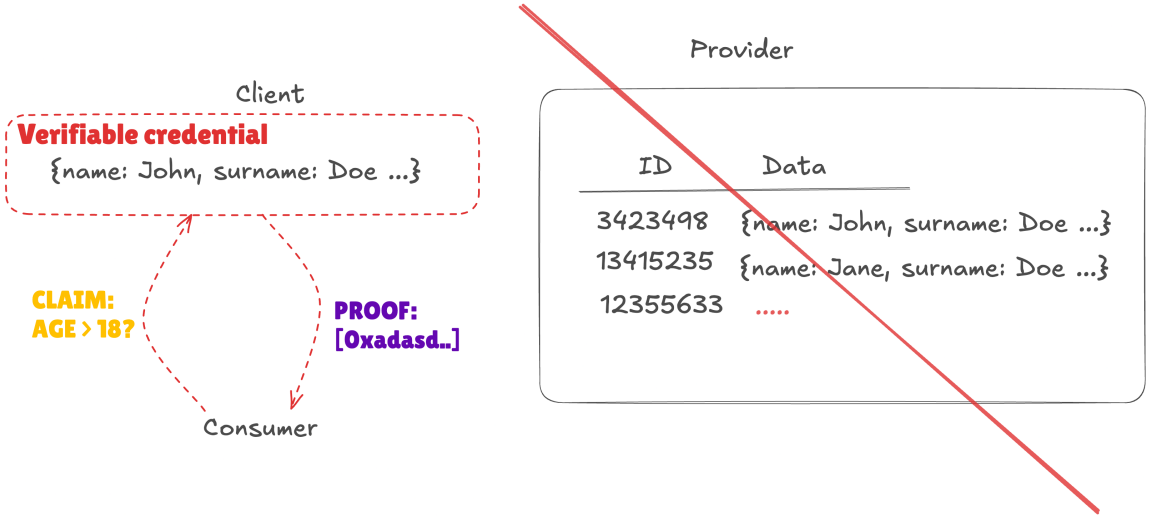
Проблема

- Провайдер не оставляет верифицируемых следов
- Именно Провайдер хранит данные
- Интеграция возможна только через соглашение с провайдером



Решение

- Создавать и хранить данные в верифицируемом виде
- Предоставлять только доказательство



Верифицируемые данные

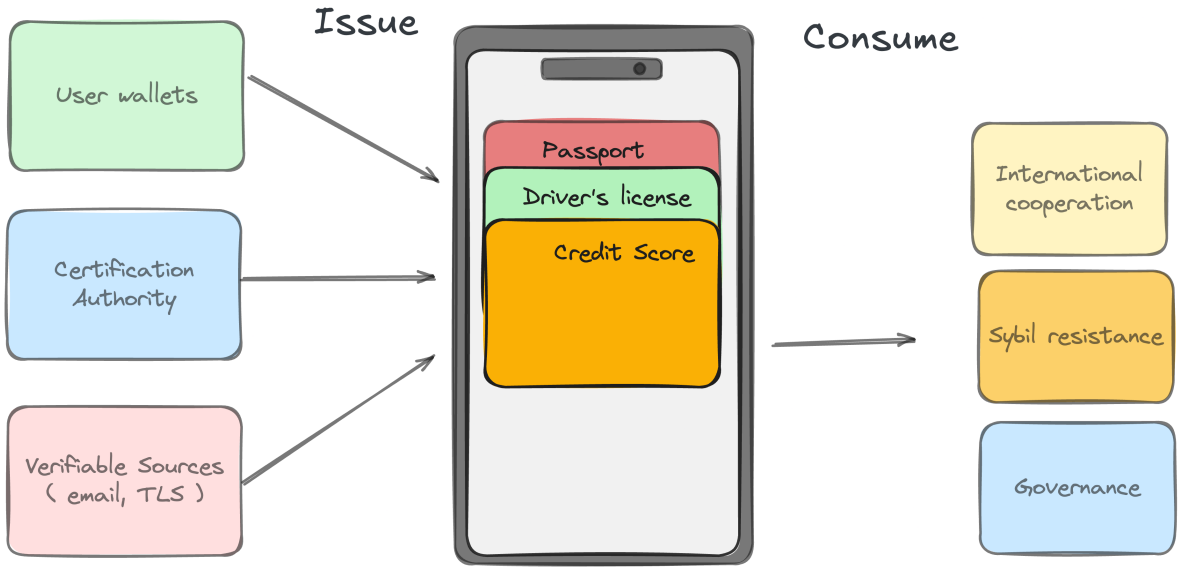
- Часть подписанного сообщения (ECDSA, ГОСТ, RSA, BBS+[1]) известным сертификатом, например (информация на чипе паспорта)
- Содержание email от известного отправителя
- Результат сетевого запроса (“нотариально заверенный скриншот”)
- Вхождение реквизитов пользователя в известное множество

РусКрипто

[1] Short Group Signatures, Dan Boneh and Xavier Boyen and Hovav Shacham, https://ia.cr/2004/174

Пользовательский путь

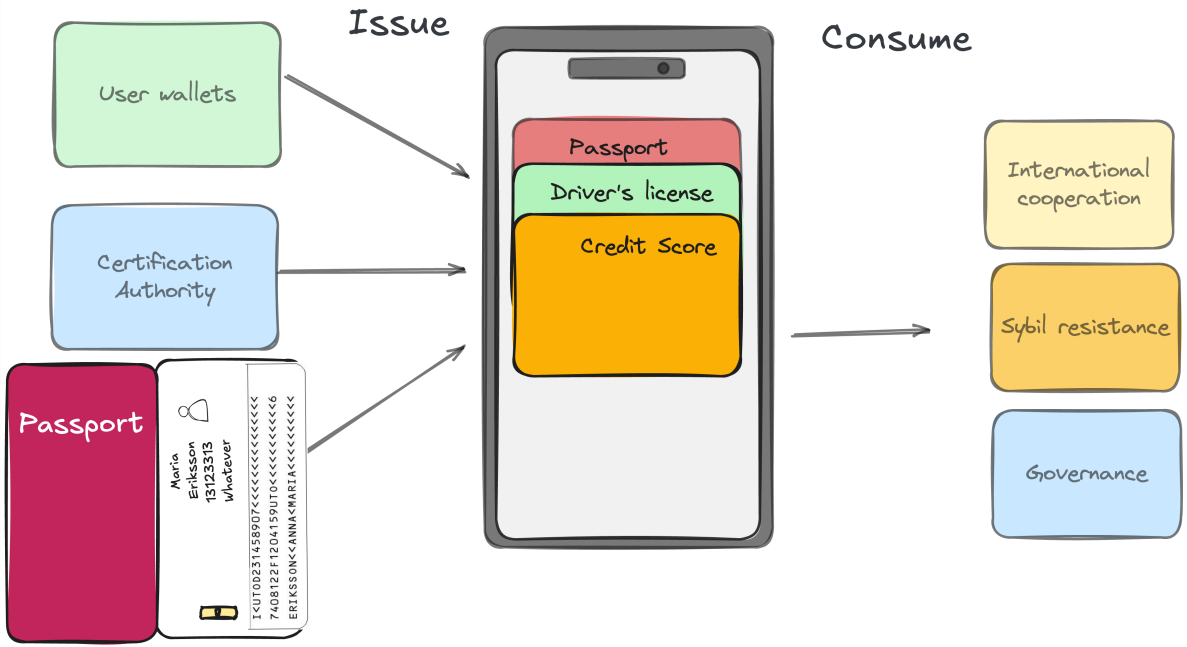
- Получаем удостоверение
- Сохраняем в устройство (например, мобильное приложение)
- Пользуемся для получения доступа к сервису



РусКрипто

Паспорт

- Содержит данные и фото пользователя с ЭЦП ФМС
- Задача: доказать возраст и гражданство без раскрытия остальных данных



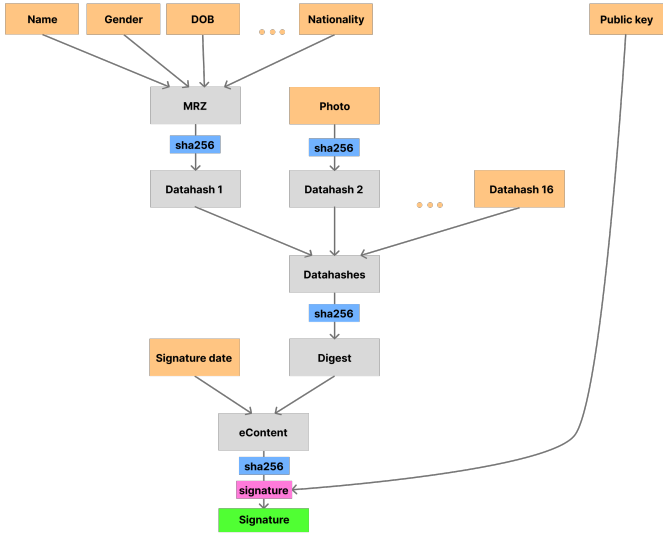
Постановка и условия

- Проверить **часть** данных в прообразе дайджеста
- Проверить подпись
- Не допустить возможность использования посторонними
- (Опционально) Не допустить связи между различными сессиями пользователя, то есть скрыть дайджест

РусКрипто

Проверяем дайджест. Groth16[1]

- Преобразуем программу в алгебраический контур
- Преобразуем контур в уравнение для полиномов
- Проверяем уравнение в случайной зашифрованной точке

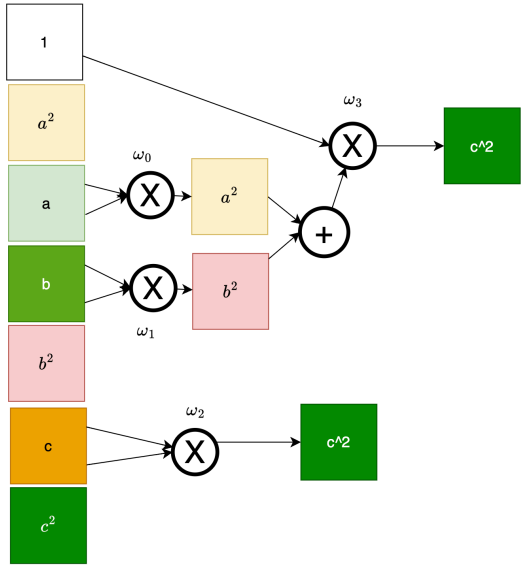


[1] On the Size of Pairing-based Non-interactive Arguments , Jens Groth https://ia.cr/2016/260

РусКрипто

Програма →Линейные уравнения

РусКрипто



Left wires

Gate	1	a	b	c	a^2	b^2	c^2
ω_0	0	3	0	0	0	0	0
ω_1	0	0	4	0	0	0	0
ω_2	0	0	0	5	0	0	0
ω_3	0	0	0	0	9	16	0

Right wires

Gate	1	a	b	c	a^2	b^2	c^2
ω_0	0	3	0	0	0	0	0
ω_1	0	0	4	0	0	0	0
ω_2	0	0	0	5	0	0	0
ω_3	1	0	0	0	0	0	0

Output wires

Gate	1	a	b	c	a^2	b^2	c^2
ω_0	0	0	0	0	9	0	0
ω_1	0	0	0	0	0	16	0
ω_2	0	0	0	0	0	0	25
ω_3	0	0	0	0	0	0	25

Линейные уравнения → полиномы

РусКрипто

Left wires

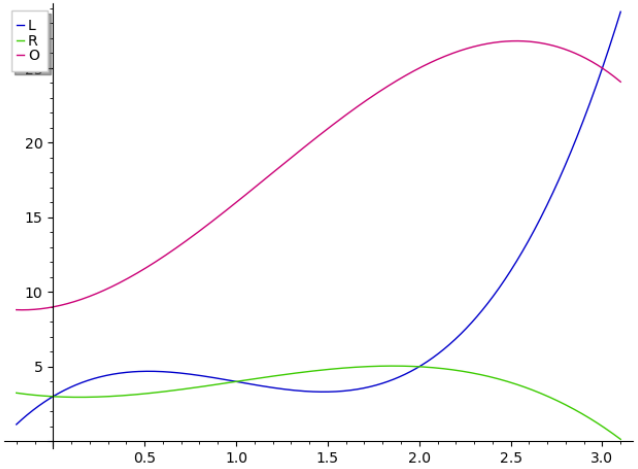
Gate	1	a	b	c	a^2	b^2	c^2
ω_0	0	3	0	0	0	0	0
ω_1	0	0	4	0	0	0	0
ω_2	0	0	0	5	0	0	0
ω_3	0	0	0	0	9	16	0

Right wires

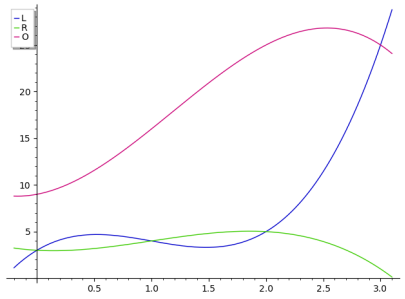
Gate	1	a	b	c	a^2	b^2	c^2
ω_0	0	3	0	0	0	0	0
ω_1	0	0	4	0	0	0	0
ω_2	0	0	0	5	0	0	0
ω_3	1	0	0	0	0	0	0

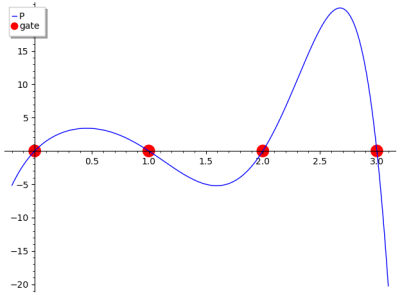
Output wires

Gate	1	a	b	c	a^2	b^2	c^2
ω_0	0	0	0	0	9	0	0
ω_1	0	0	0	0	0	16	0
ω_2	0	0	0	0	0	0	25
ω_3	0	0	0	0	0	0	25



Линейные уравнения →полиномы





$$P(x) = L(x) * R(x) - O(x)$$

$$\exists H(x) : P(x) = H(x) * \prod_i (x - \omega_i)$$

$$\forall \tau \quad H(\tau) \cdot t(\tau) = P(\tau)$$

$$\forall \tau \quad : e(H(\tau) \cdot t(\tau)) = e(L(\tau) \cdot R(\tau))$$

РусКрипто

Бонус: ослепление дайджеста

РусКрипто

$\sigma \xleftarrow{\$} \mathbb{F}_p$ - Ослепляющий фактор

$S = (r, s) \Longrightarrow \quad r' = (\sigma \cdot r)_x, s = r' \cdot r^{-1} \cdot \sigma^{-1} \cdot s \to S' = (r', s')$

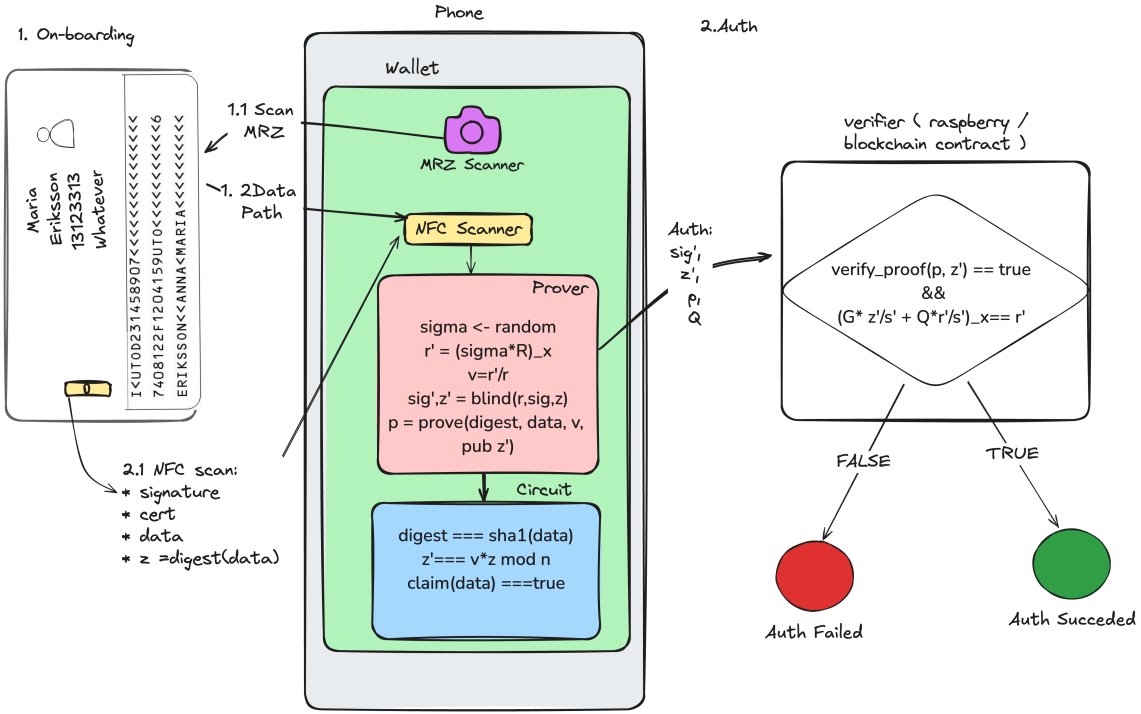
$z' = r' \cdot r^{-1} \cdot z$ - Ослепленный дайджест

$((s'^{-1} \cdot z') \cdot G + (s'^{-1} \cdot r') \cdot Q)_x = r' \quad ?$

$((s^{-1} \cdot r' \cdot r^{-1} \cdot z) \cdot \sigma \cdot r'^{-1} \cdot r \cdot G + (s^{-1} \cdot r) \cdot \sigma \cdot Q)_x = r \cdot \sigma \quad ?$

$((s^{-1} \cdot z) \cdot G + (s^{-1} \cdot r) \cdot Q)_x = r$ - стандартная проверка подписи

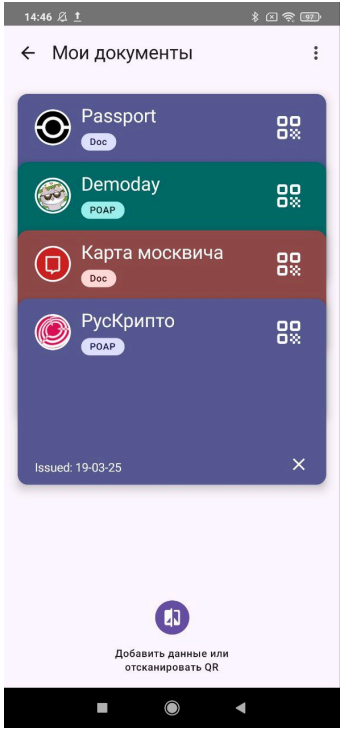
Схема прототипа



РусКрипто

Схема прототипа

РусКрипто



Видео

РусКрипто

Защита от передачи

- При создании документа сверяем фото с паспортом
- Данное решение требует доверия приложению
- Альтернативный вариант:
  - Доказательство для расстояния между (embedding) векторами
  - Включение вектора фото в само удостоверение
  - Liveness check

РусКрипто

Стандарты

- ISO/IEC 18013-5 - определяет формат mDoc (мобильный документ)
- JSON-LD - семантика JSON
- W3C DID - маршрутизация и возможные методы верификации
- W3C Data Integrity - возможные криптографические алгоритмы

- https://www.w3.org/TR/json-ld11/
- https://www.w3.org/TR/vc-data-model/
- https://www.w3.org/TR/vc-data-integrity/

РусКрипто

ISO/IEC 18013-5

- Поддерживается только ECDSA
- Не имеет (пока) готовых стандартов для частичного раскрытия данных, но позволяет расширения
- Для частичного раскрытия нужно подписывать каждый атрибут отдельно

РусКрипто

W3C VC

РусКрипто

Я знаю такую подпись CA для корня дерева, что листы содержат такие-то данные

```
{
  "id": "urn:uuid:123e4567-e89b-12d3-a456-426614174000",
  "type": ["VerifiablePresentation"],
  "verifiableCredential": {
…
    "credentialSubject": {
      "dateOfBirth": "1995-06-12"
    },
    "merkleProof": {
      "leaf": "0xhash_of_1995-06-12",  // Лист дерева
      "proofPath": ["0xhash1", "0xhash2", "0xhash3"],  // Путь к корню
      "root": "0xabcd1234ef567890...",  // Корень должен соответствовать подписи
    },
    "proof": {
      "type": "MerkleProofSignature",
      "created": "2025-03-13T00:00:00Z",
      "proofValue": "0xdeadbeefcafebabe...",
      "proofPurpose": "assertionMethod",
      "verificationMethod": "did:example:california-dmv#keys-1"
    }
  }
}
```

JSON-LD & BBS+

РусКрипто

Я знаю такую подпись CA, что прообраз дайджеста удовлетворяет условиям


```
{
  "@context": "https://www.w3.org/2018/credentials/v1",
  "type": "VerifiableCredential",
  "credentialSubject": {
    "ageOver21": true
  },
  "proof": {
    "type": "BBS+SignatureProof",
    "created": "2025-03-13T12:34:56Z",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "https://dmv.example.gov/keys/123",
    "proofValue": "z4FZzKw..."
  }
}
```

Стандарты

EIDAS 2.0 (цифровой паспорт ЕС) поддерживает только ISO/IEC 18013-5 по причине отсутствия явной подписи владельца

Стандарт	Метод	Приватность	ISO/IEC 18013-5
ISO/IEC 18013-5	JWS (ECDSA)	Низкая	✅
W3C VC	Д. Меркла	Средняя	❌
W3C VC	BBS+	Высокая	❌
Hyperledger AnonCreds	CL подписи	Высокая	❌
Iden3 / Polygon ID	Zk-SNARK	Очень высокая	❌

РусКрипто

Что дальше

- Прототип на основе BBS+ подписей в SIM-картах
- Поиск синергии с продуктами на основе ЦФА
- Верифицируемые запросы к внешним системам

РусКрипто

СПАСИБО!

РусКрипто

Контакты

Обратная связь