MongoDB

```
{
  _id: ObjectId('670ec7516db8041167fe6911'),
  userID: '6',
  personalInfo: {
    name: 'Carlos Maia',
    address: 'Rua das Flores, 123',
    birthDate: '1990-01-01'
  },
  financialData: { salary: 5000, creditHistory: 'Bom', transactions: [] },
  medicalExams: [ { type: 'Sangue', result: 'Normal', date: '2023-01-15' } ],
  medicalRecords: {
    consultations: [ { date: '2023-02-10', notes: 'Paciente saudável' } ]
  },
  h_1: 'f132f0c067108ab938712f9e7924ec6a05de992ee6b34ccf473ec901f2f45ea4',
```

Verificador

A partir do acesso a base de dados ou a uma blockchain pública onde se encontram os dados a serem verificados:

Envia para o provador via API um identificador do dado a ser verificado ou o hash.

Provador

O provador recebe via Api solicitações de um verificador para provar que é dono e conhece o dado que originou o hash público.

Ao receber a solicitação com a identificação do documento ou do hash a ser validado:

- Faz a leitura do documento na base de dados.

- Gera uma prova ZPK Fiat-Sharmir/Schnorr **apartir do dado original** salvo no banco incluindo no cálculo, um valor nonce (r) aleatório só conhecido pelo provador, o nonce (v) recebido via API como prova designada pelo verificador para evitar não Simulabilidade e transferibilidade das provas.

- Responde ao verificador:

- h_1: Esse é o hash do JSON, que serve como compromisso inicial do provador.

- Desafio (c): O desafio é gerado utilizando o heurístico Fiat-Shamir-Schnorr c = H(h_1, r, v),

- Resposta (s): A resposta s é gerada pelo provador com base em um cálculo que envolve o nonce r, o compromisso (h_1) e o nonce v.

Verificador

O verificador deve usar os valores recebidos (h_1, c, s) para validar que o provador realmente conhece o conteúdo original que produziu o hash público h_1.

O verificador faz o seguinte:

Recalcular o Desafio c:

O verificador usa os valores fornecidos pelo provador h_1 e a resposta s e o nonce v que o verificador conhece, para recalcular o valor do desafio (c, o qual chamamos de cv. Esse recalculo pode ser descrito pela mesma função hash que foi usada pelo provador:

cv = H(h_1, r, v), onde r está embutido nos cálculos que o provador fez na geração de s.

Comparação entre c e cv:

Se cv for igual a c, isso significa que a prova é válida.