прокси

Прокси-решифрование с децентрализованными идентификаторами в распределённых системах

АО «Промышленные Криптосистемы»

прокси

01 С 2017 года разрабатываем цифровые продукты на распределенных реестрах и смарт-контрактах для российских и зарубежных заказчиков: более 25 успешно выполненных проектов

02 Разработали Hauberk Pro — систему управления распределёнными реестрами и смарт-контрактами на базе открытой платформы Hyperledger Fabric с поддержкой отечественной ГОСТ-криптографии. Внесена в реестр отечественного ПО.

03 С 2020 года входим в группу «ИнфоТеКС» — лидера российского рынка информационной безопасности

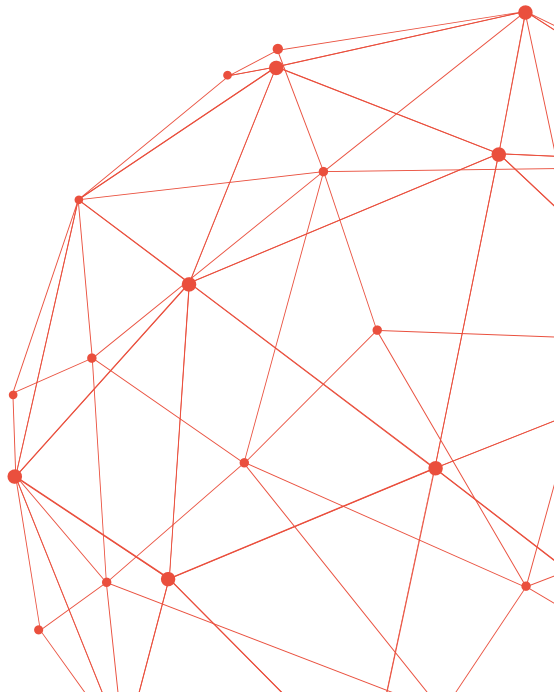
infotecs®

Клиенты и партнёры

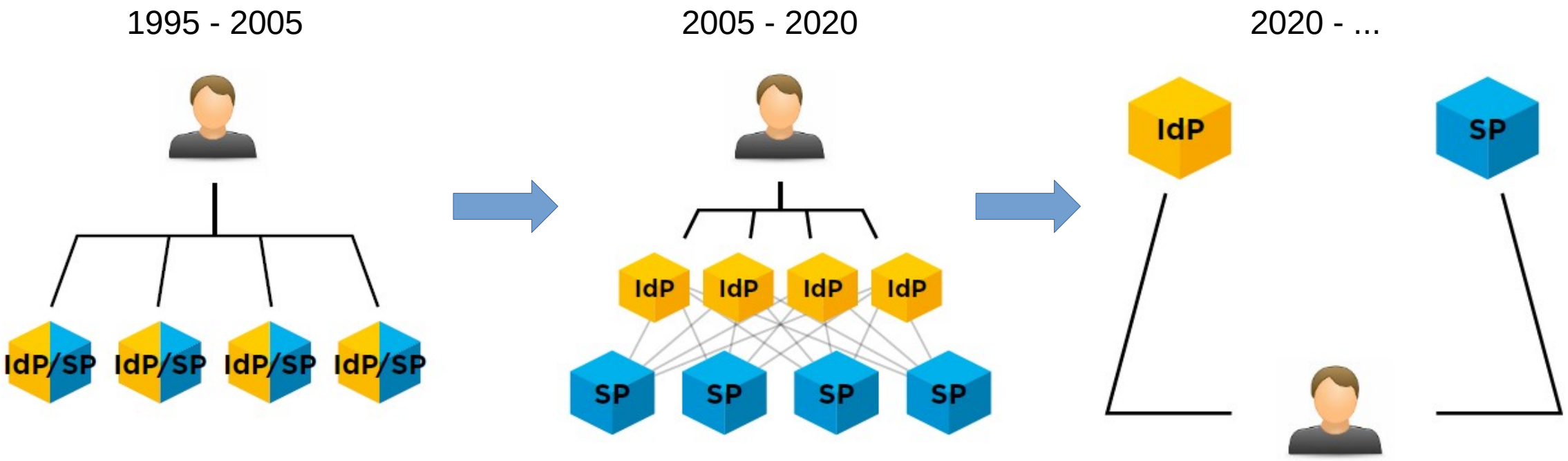
Газпром нефть · РЖД · Райффайзенбанк · ВТБ · ВНИИЖТ · UTair Aviation · marsat · ЛокоТех · smartavia · IPCHAIN · ATOMYZE · TRADELENS

Продукты

- СКЗИ ViPNet CryptoSmart
- Система управления Hauberk Pro
- Деловая сеть Контрактиум



DID: зачем?


1995 - 2005
2005 - 2020
2020 - ...
IdP/SP
IdP/SP
IdP/SP
IdP/SP
IdP
IdP
IdP
IdP
SP
SP
SP
SP
IdP
SP

DID: введение

прокси

DID идентификатор

did:example:123456789abcdefghi ➡

метод — идентификатор

DID URL

did/path["?"]["#"] ➡

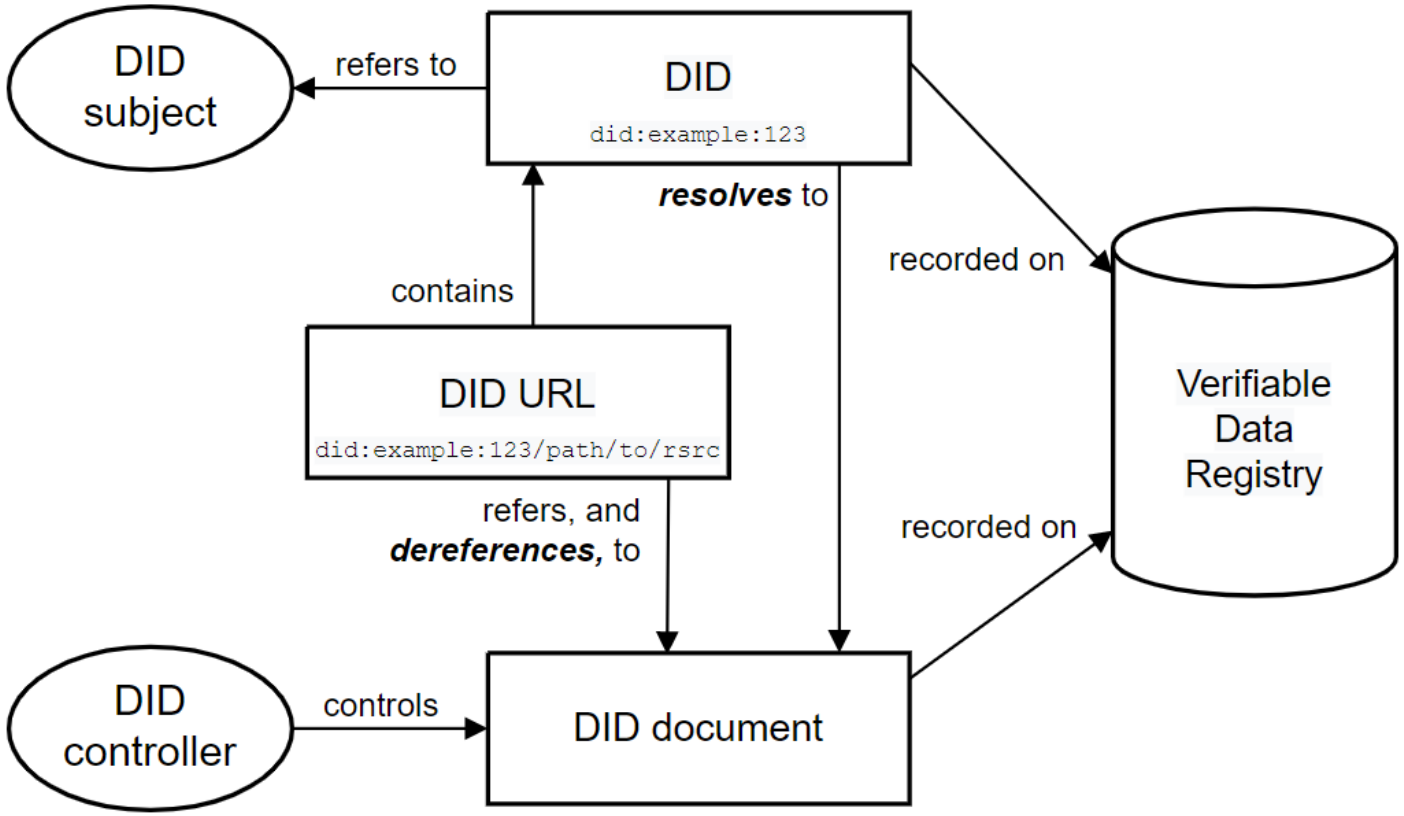
DID документ

```
{
   "@context": [
      "https://www.w3.org/ns/did/v1",
      "https://w3id.org/security/suites/ed25519-2020/v1"
   ]
   "id": "did:example:123456789abcdefghi",
   "controller": "did:example:bcehfew7h32f32h7af3",
   "authentication": [{
      "id": "did:example:123456789abcdefghi#keys-1",
      "type": "Ed25519VerificationKey2020",
      "controller": "did:example:123456789abcdefghi",
      "publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
   }]
}
```

Документация W3C

1. https://www.w3.org/TR/did-core/
2. https://www.w3.org/TR/did-use-cases/

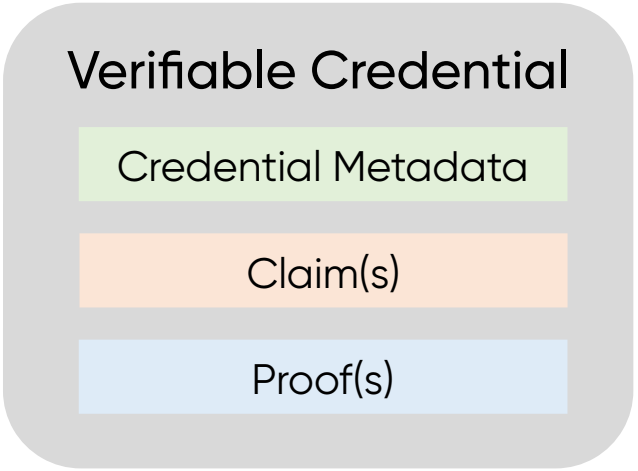
DID: архитектура

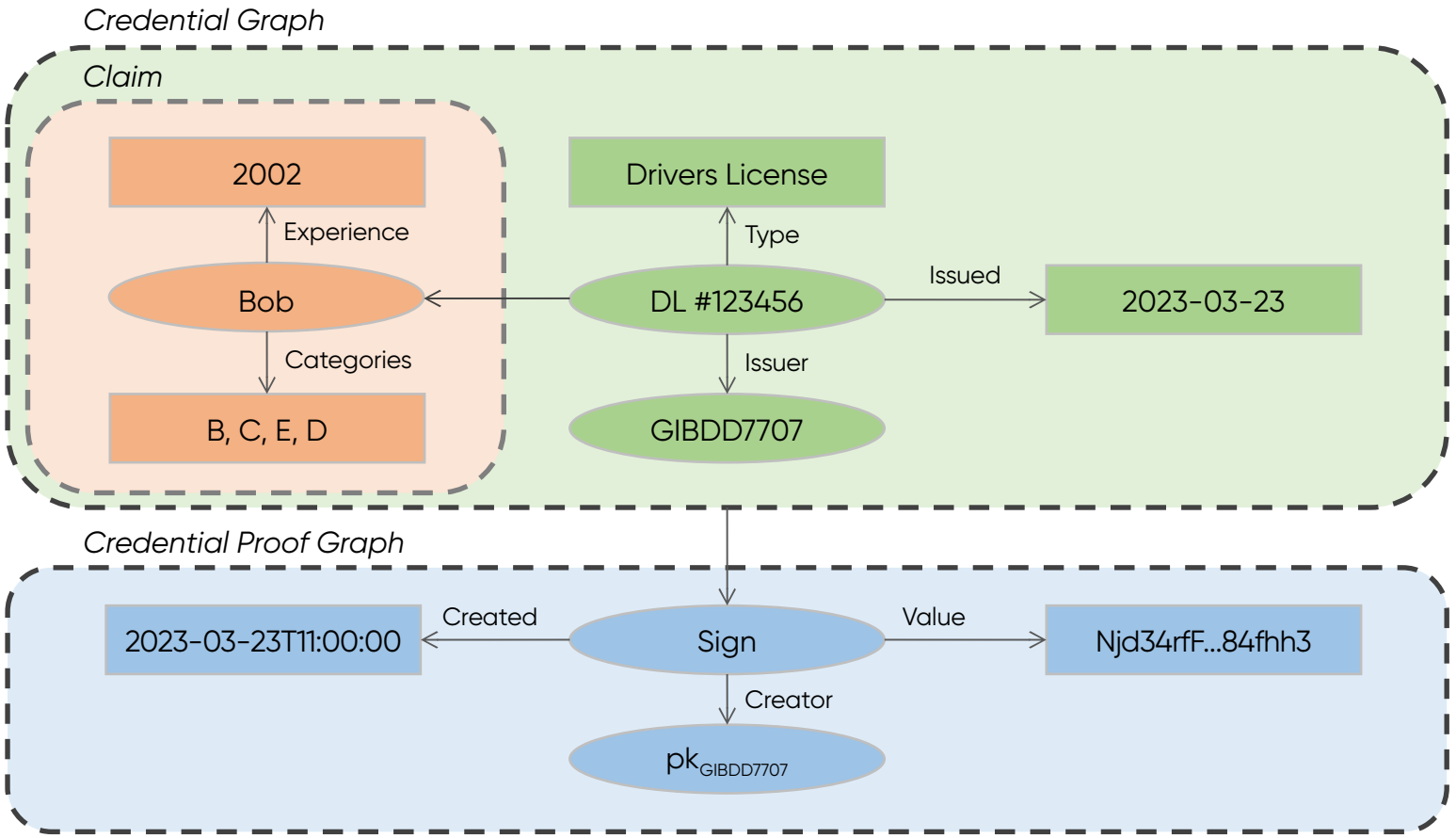


Документация:

1. https://w3c-ccg.github.io/did-resolution/
2. https://identity.foundation/didcomm-messaging/spec/v2.0/
3. https://identity.foundation/sidetree/spec/
4. https://www.w3.org/TR/did-spec-registries/

VC: верифицируемые учётные данные

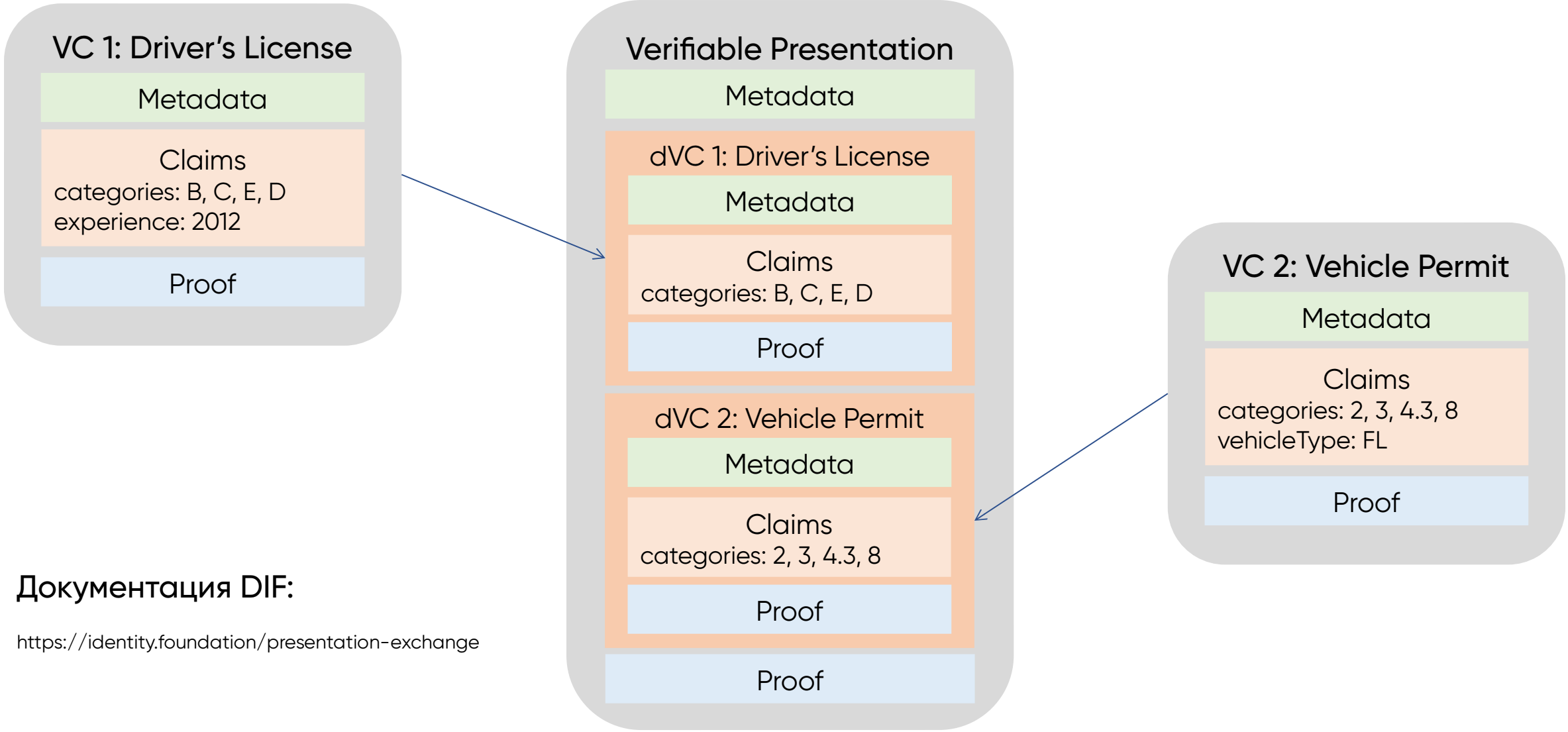




Документация W3C

1. https://www.w3.org/TR/vc-data-model/
2. https://www.w3.org/TR/vc-use-cases/

VP: верифицируемые представления

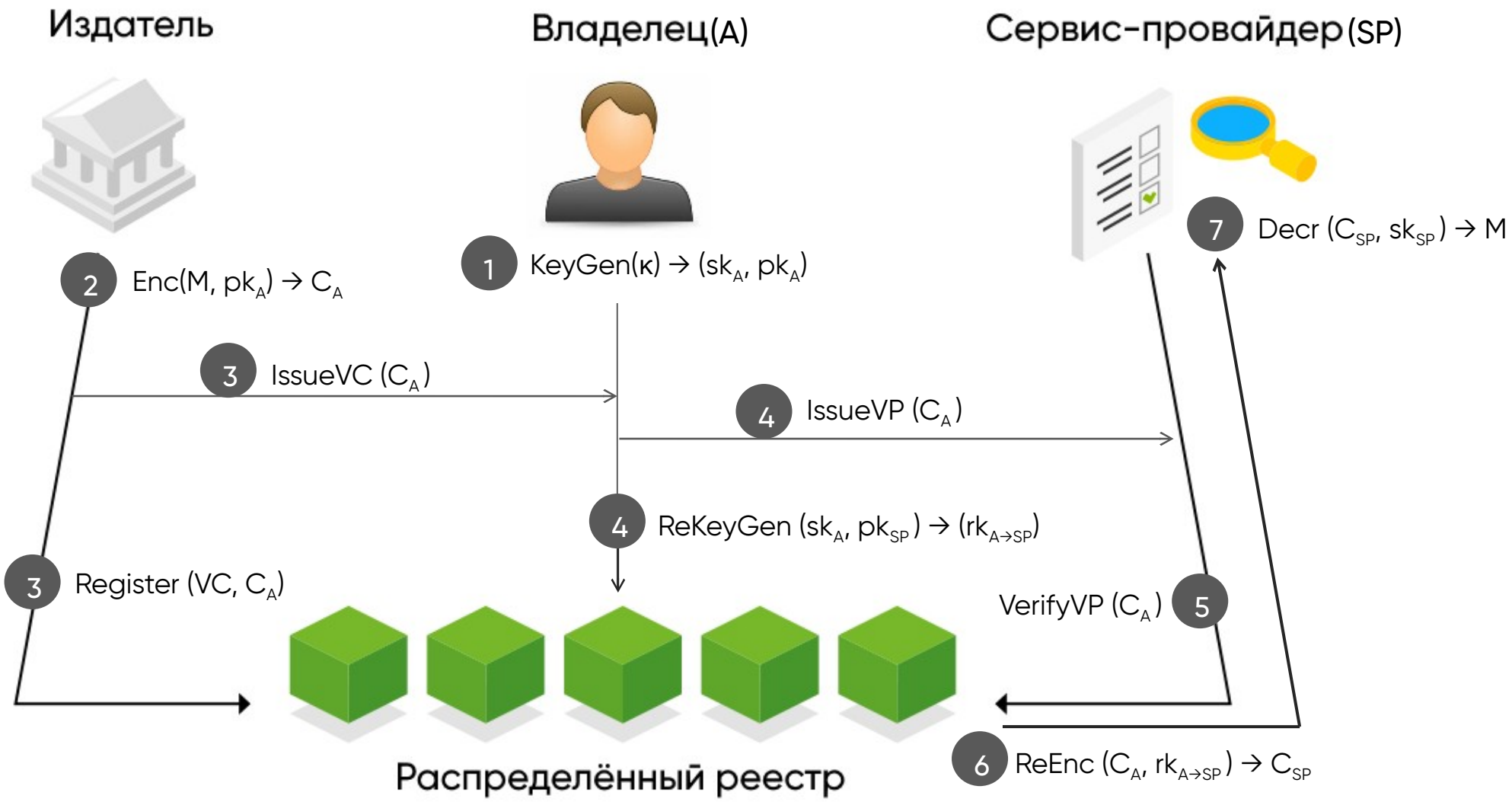


Документация DIF:

https://identity.foundation/presentation-exchange

DID: применение

DID + PRE


Издатель
Владелец(A)
Сервис-провайдер(SP)
1 KeyGen(κ) → (sk_A, pk_A)
2 Enc(M, pk_A) → C_A
3 IssueVC (C_A)
4 IssueVP (C_A)
4 ReKeyGen (sk_A, pk_SP) → (rk_A→SP)
3 Register (VC, C_A)
VerifyVP (C_A) 5
7 Decr (C_SP, sk_SP) → M
6 ReEnc (C_A, rk_A→SP) → C_SP
Распределённый реестр

Литература и интересные проекты

1. Jiayu He , Dong Zheng, Rui Guo, Yushuang Chen, Kemeng Li, and Xiaoling Tao
   Efficient Identity-based Proxy Re-encryption Scheme in Blockchain-assisted Decentralized Storage System
   International Journal of Network Security, Vol.23, No.5, PP.776-790, Sept. 2021
2. Song, J.; Yang, Y.; Mei, J.; Zhou, G.; Qiu, W.; Wang, Y.; Xu, L.; Liu, Y.; Jiang, J.; Chu, Z.;
   Proxy Re-Encryption-Based Traceability and Sharing Mechanism of the Power Material Data in Blockchain Environment. Energies 2022, 15, 2570.
3. B. Chen, D. He, N. Kumar, H. Wang and K. -K. R. Choo,
   "A Blockchain-Based Proxy Re-Encryption With Equality Test for Vehicular Communication Systems,"
   IEEE Transactions on Network Science and Engineering, vol. 8, no. 3, pp. 2048-2059, 1 July-Sept. 2021
4. K. O.-B. O. Agyekum, Q. Xia, E. B. Sifah, C. N. A. Cobblah, H. Xia and J. Gao,
   A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain,
   IEEE Systems Journal, vol. 16, no. 1, pp. 1685-1696, March 2022
5. Gaofan Lin, Haijiang Wang, Jian Wan, Lei Zhang, Jie Huang,
   A blockchain-based fine-grained data sharing scheme for e-healthcare system,
   Journal of Systems Architecture, Volume 132, 2022, 102731

БЛАГОДАРЮ ЗА ВНИМАНИЕ!

Михаил Чеканов
Генеральный директор АО «ПроКСи»

m@procsy.ru