



*Blockchain
em evolução.*

GT-SWARM



GT-SWARM

Self-sovereign Wi-Fi Authentication Roaming

Caciano Machado, Carla Merkle,
Cristian Alves, Eduardo Hoffmann

Fevereiro/2026



Sumário

- Introdução
- Arquitetura
- Ambiente de testes
- Testes de desempenho
- Conclusão e trabalhos futuros

Introdução: Objetivo

Autenticação de redes federadas, como o eduroam, com identidades digitais descentralizadas (IDD) utilizando a infraestrutura padrão *de facto* do 802.1x



+ IDD

Introdução: Motivação do Eduroam + IDD



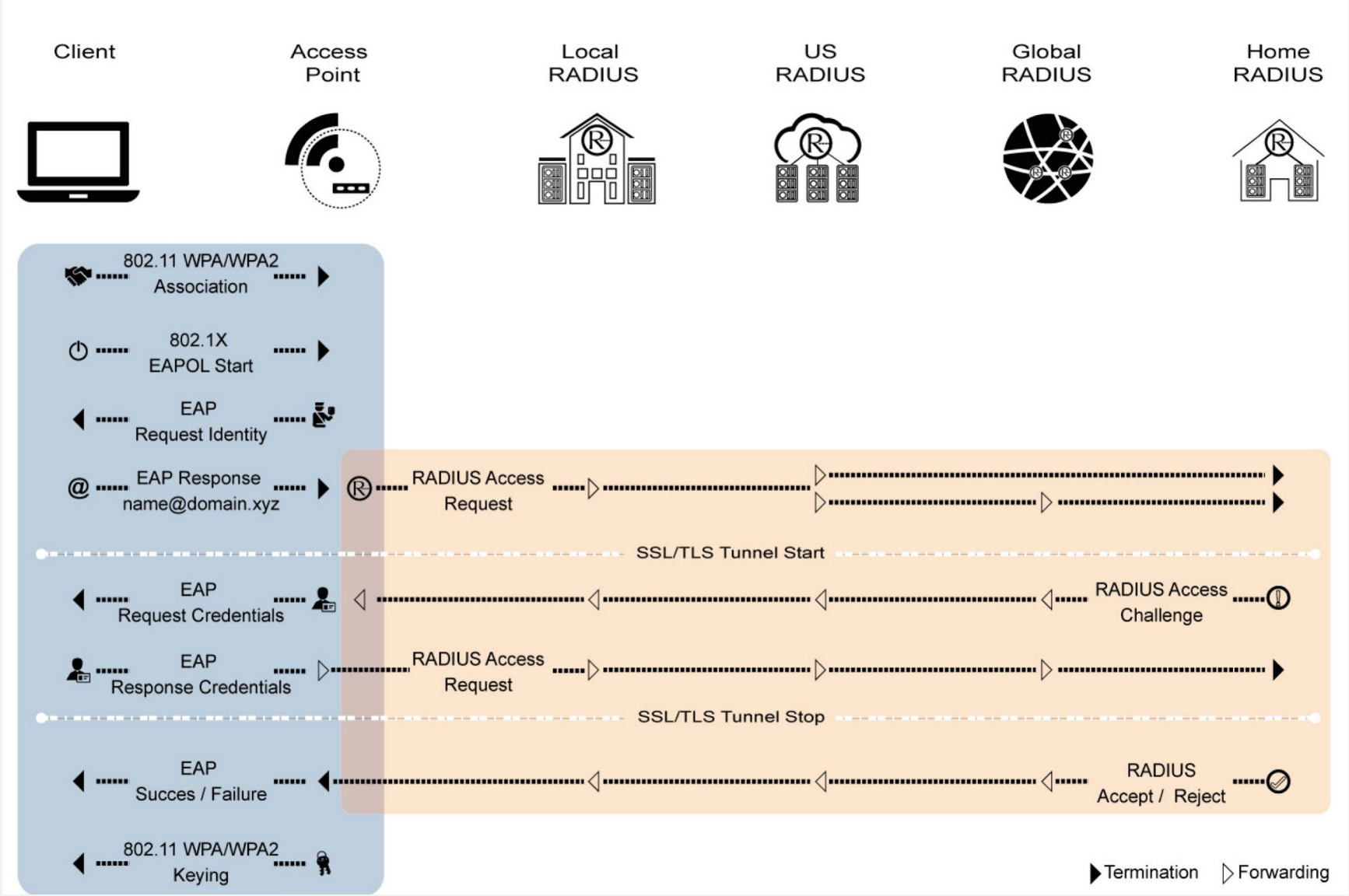
- Maior controle dos usuários sobre seus dados
- Autenticação sem senhas, baseada em VC
- Maior dependabilidade, não depende de toda uma infraestrutura de RADIUS, com utilização de VDR e blockchain
- Extensão para outras federações, como OpenRoaming
- Privacidade aprimorada (ZKP)

F. Ahmed and S. A. Hussain, "A Privacy-Preserving Cross-domain Network access Services Using Sovrin Identifier," 2021 International Conference on Cyber Warfare and Security (ICCWS 2021)

Petric, R, "Specifying SSI over EAP: Towards an Even Better Eduroam in the Future". In: Barolli, L. (eds) Advanced Information Networking and Applications. AINA 2024. Lecture Notes on Data Engineering and Communications Technologies, vol 202. Springer, 2024

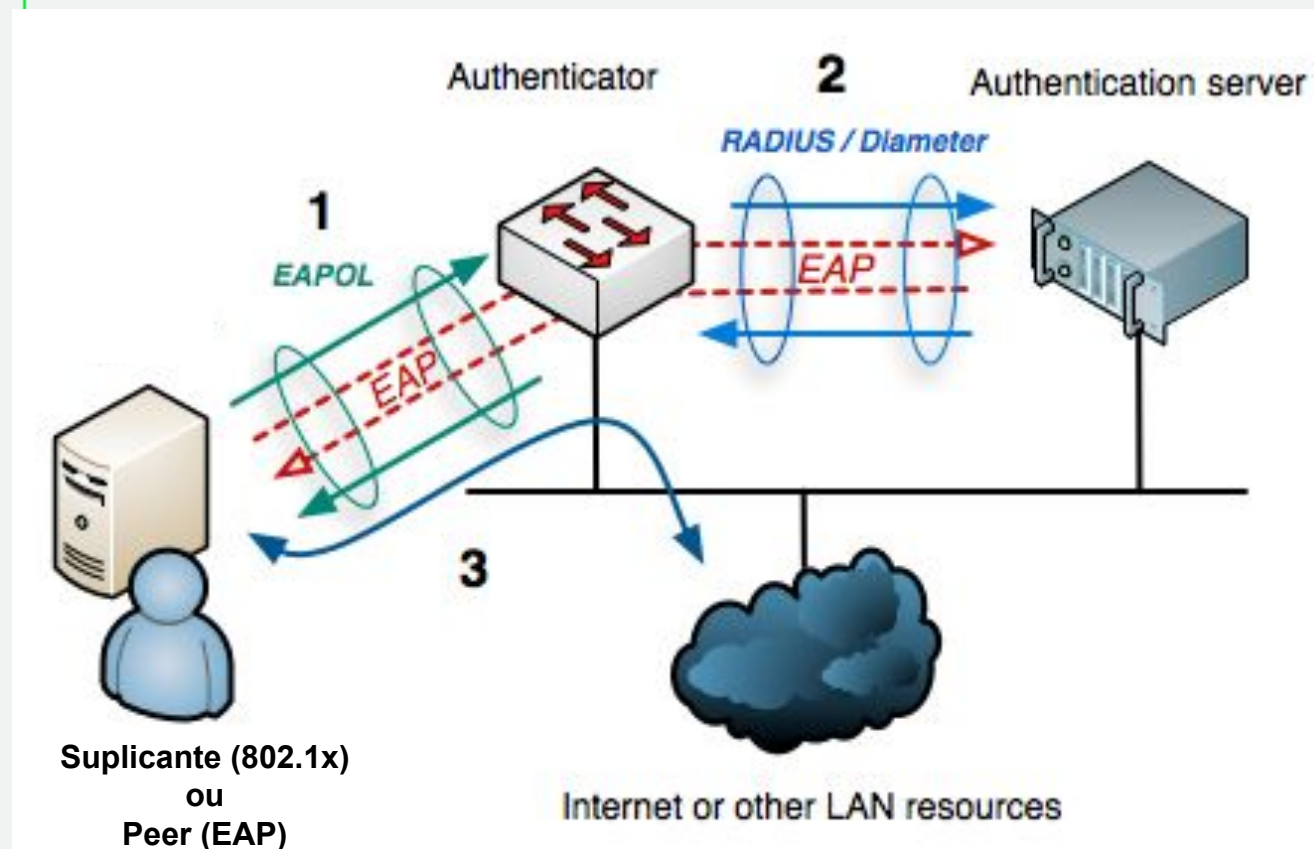


Introdução: Eduroam



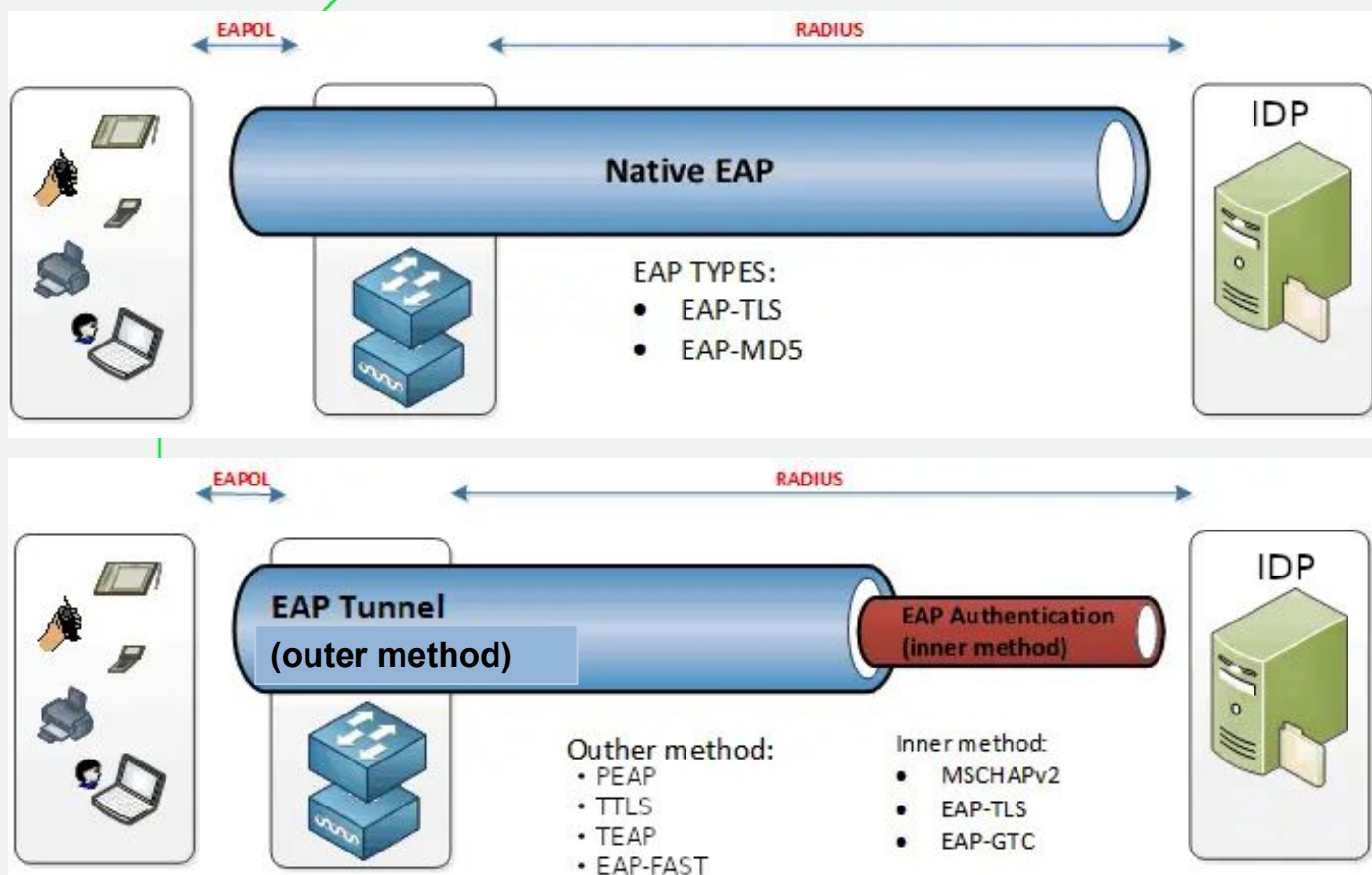
Introdução: 802.1x e EAP

- **Peer (EAP) / suplicante (802.1x)** – Dispositivo sendo autenticado
- **Autenticador / Cliente RADIUS** – Switch/Access Point de acesso
- **Servidor de Autenticação** – RADIUS com acesso à base de usuários



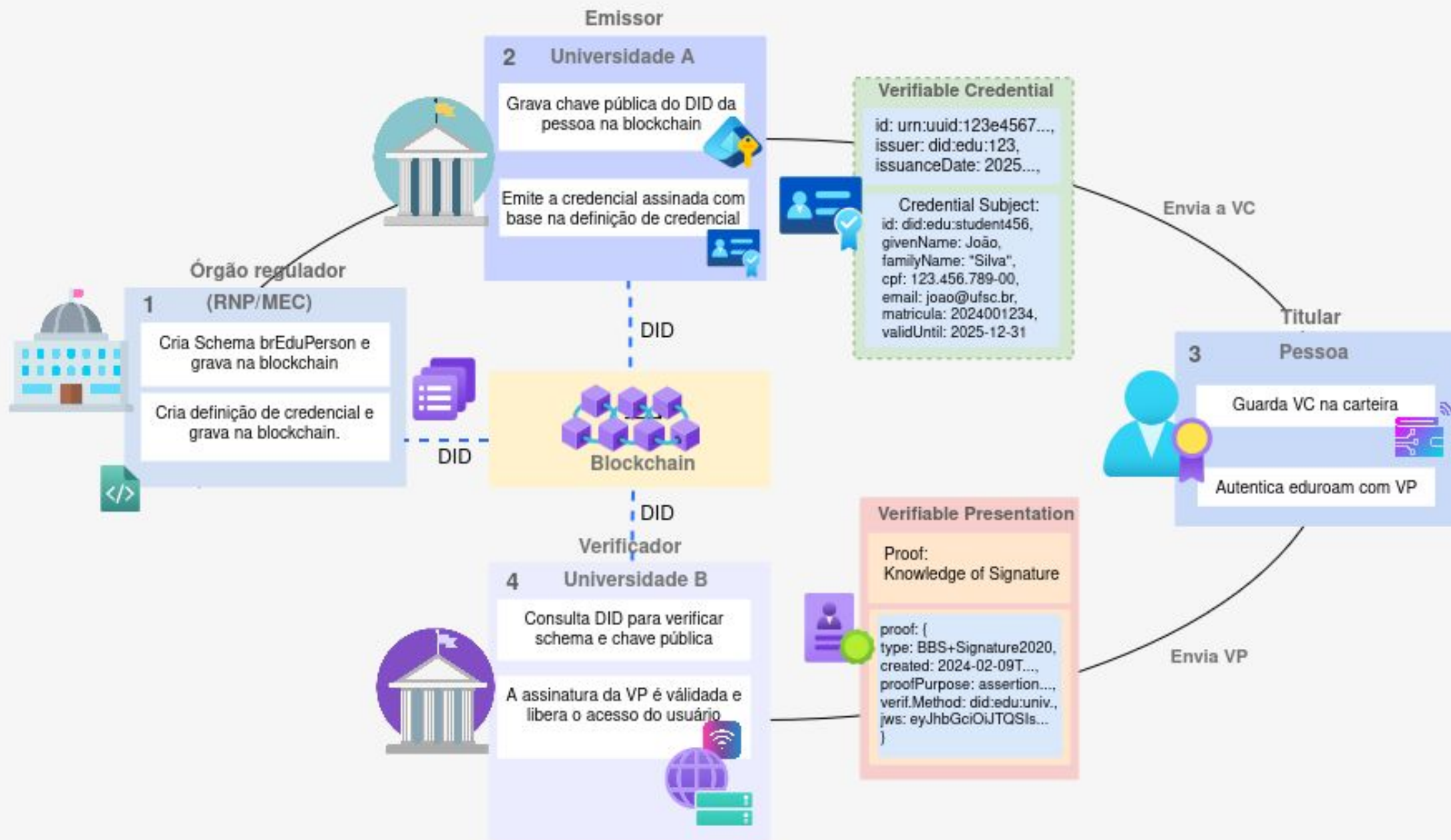
Introdução: Métodos EAP

Vários protocolos (métodos) de autenticação (nativos ou tunelados)

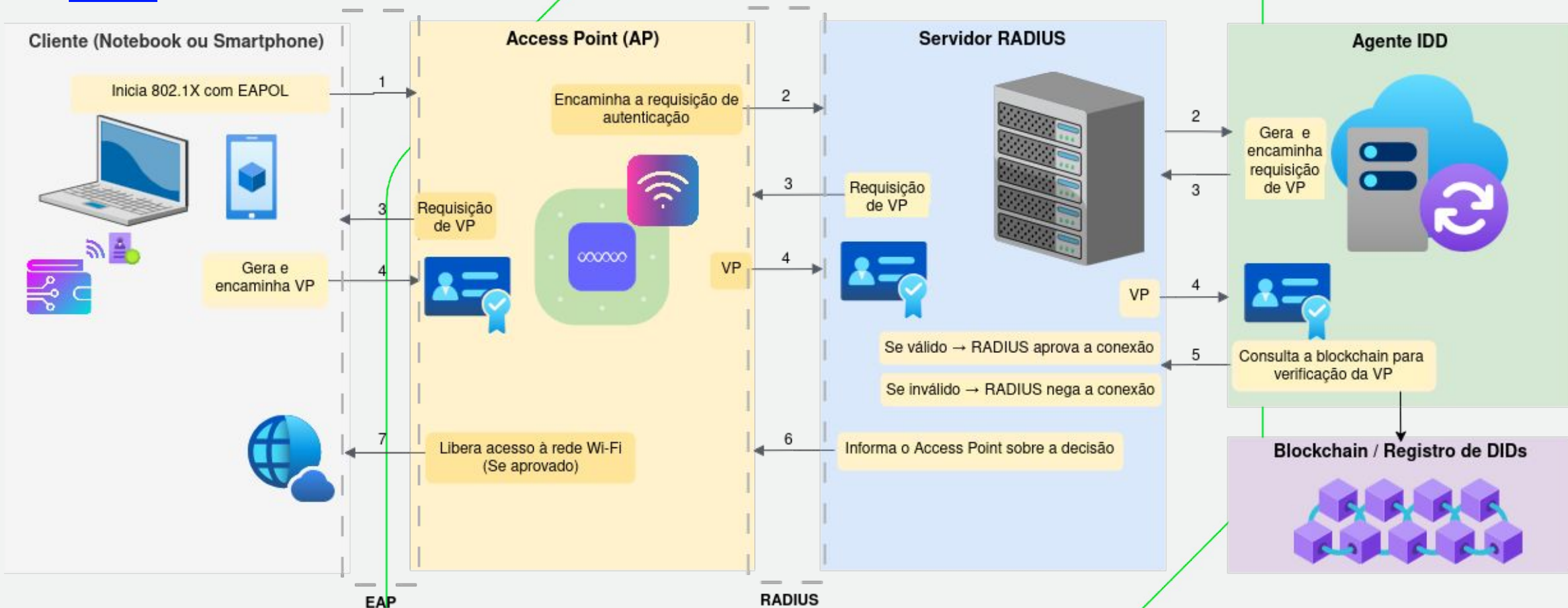


- Eduroam utiliza outer tunnel PEAP/TTLS e inner tunnel MSCHAPv2
- Proposta do projeto é criação de novo método EAP-DID para autenticação IDD

Arquitetura: Visão Geral



Arquitetura: Autenticação/Verificação de Credenciais



- Desafio técnico é a autenticação IDD segura pelos mecanismos tradicionais 802.1x
- Para isso criamos novo método EAP-DID que permite ao cliente IDD autenticar para acesso à rede quando ainda não possui IP atribuído

Arquitetura: Funcionalidades da proposta



- Emissão/Verificação de DID/VC
 - Esquemas compatíveis brEduPerson
 - Registro dos DIDs na blockchain
 - Emissão de VCs, criação e validação de VPs
- Autenticação com VPs com framework 802.1x
 - Autenticação IDD no 802.1x, para titulares de DIDs obterem acesso à rede com autenticação por VPs
 - Novo método EAP p/ encapsular mensagens do DIDCommv2 e da API IDD
- Integração da VDR com blockchain Cardano
 - VDR do IDD atua como proxy p/ blockchain e como cache para os dados
 - Integração à blockchain Cardano



Arquitetura: Softwares

Códigos abertos disponíveis

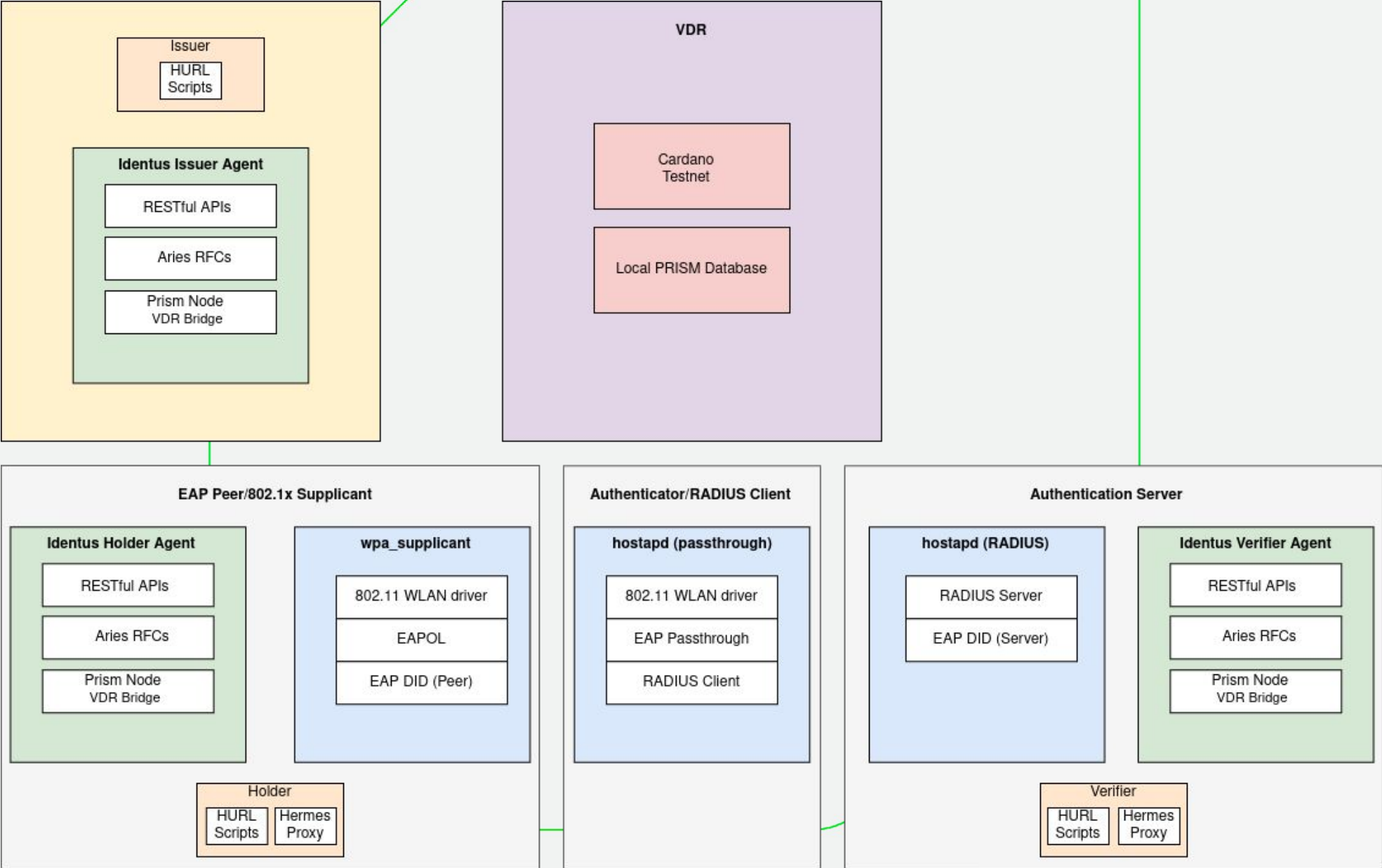
Hyperledger Identus	Framework de identidade descentralizada com desenvolvimento ativo. Agentes para Issuer, Holder, Verifier. VDR local (PRISM). Escrito em SCALA.
Cardano	Blockchain utilizada pelo Hyperledger Identus.

Códigos do SWARM - disponíveis no git da RNP

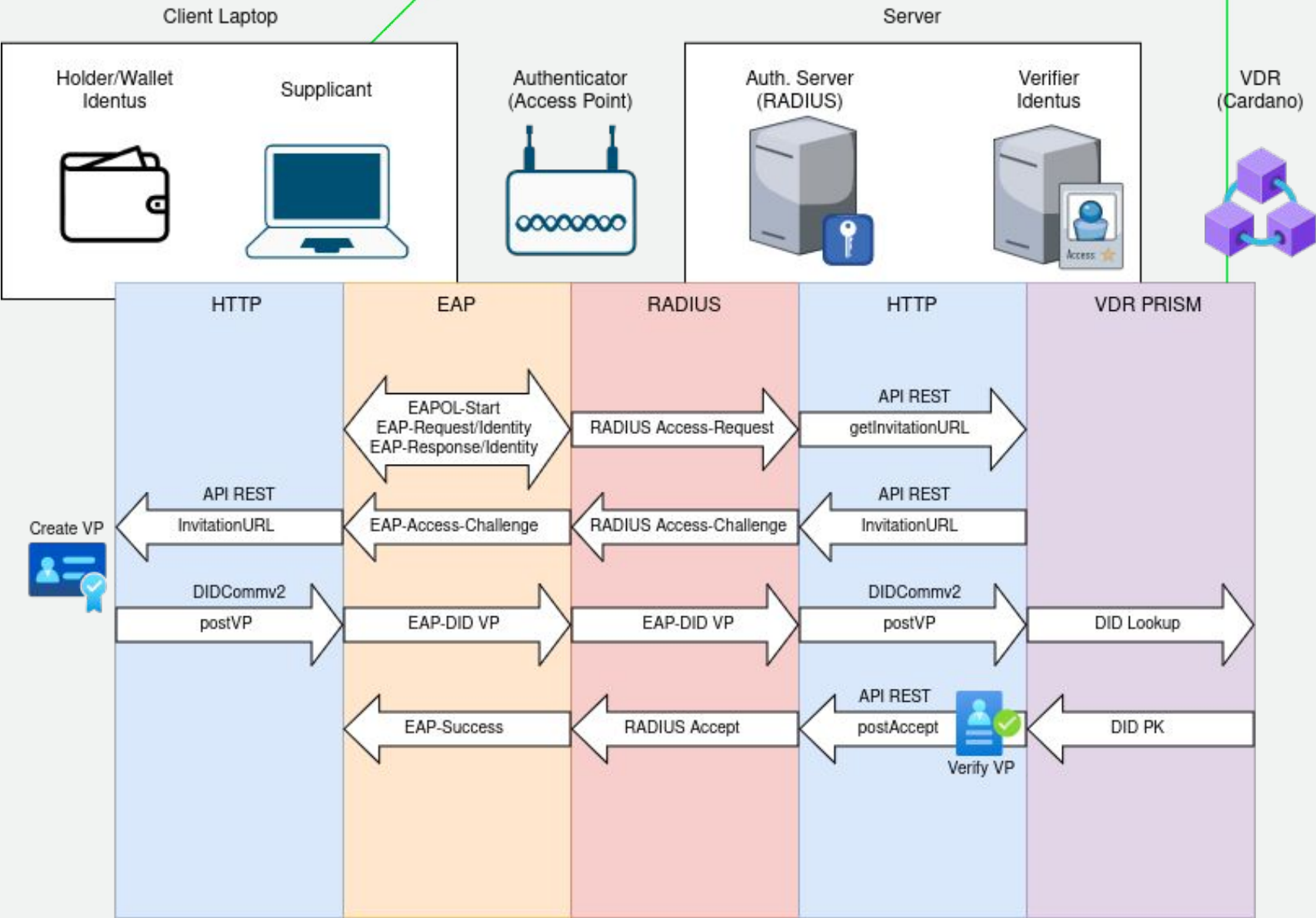
Hostap	Implementação de suplicante 802.1x open source, para implementação do método EAP-DID. Também implementa servidor RADIUS básico. Escrito em C.
Hermes	Proxy para DIDCommv2 e API REST para intermediação das mensagens de Invite OOB e de VP. Escrito em Python.



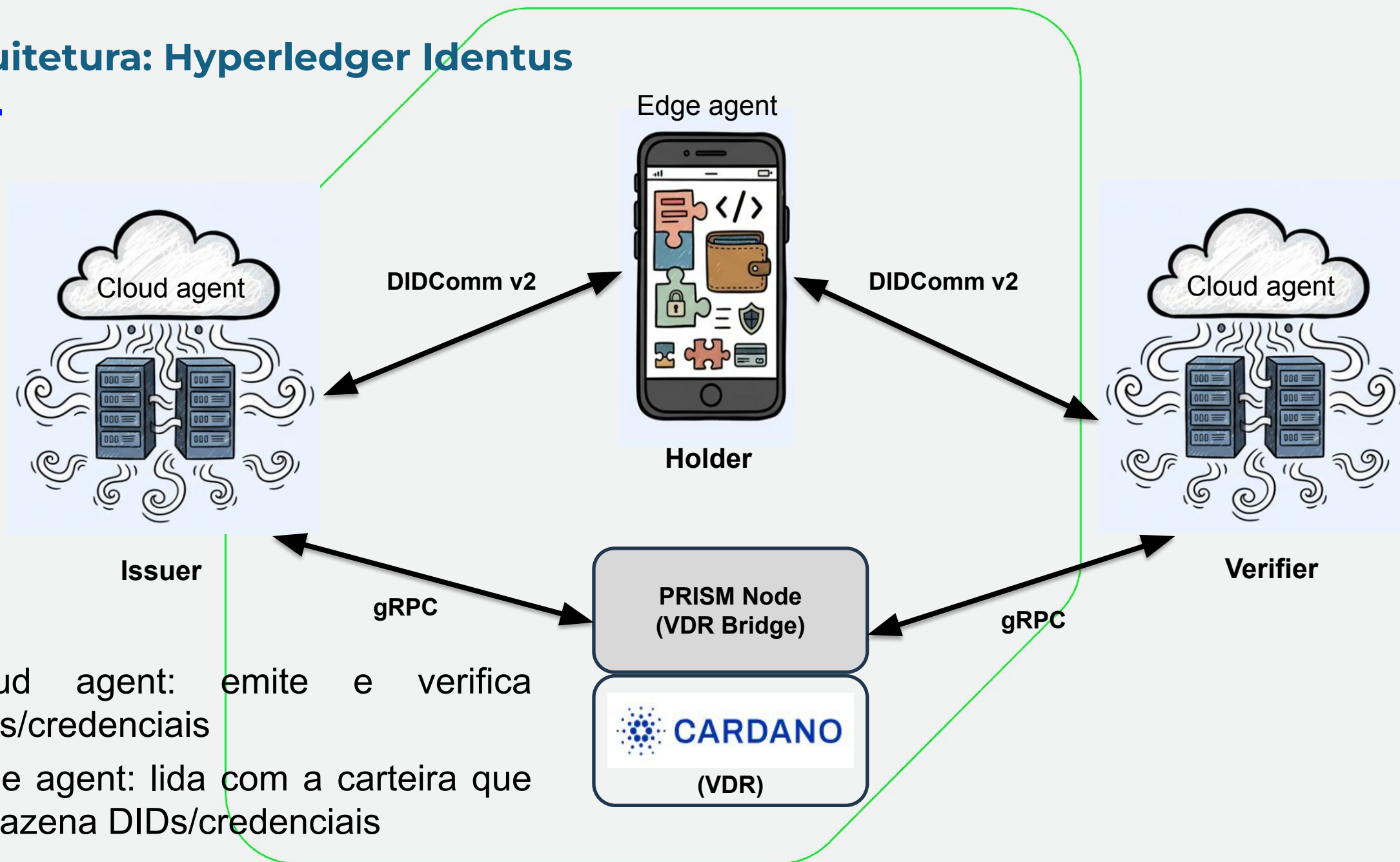
Arquitetura: Diagrama de Componentes



Arquitetura: Mensagens do EAP-DID no Caso Típico

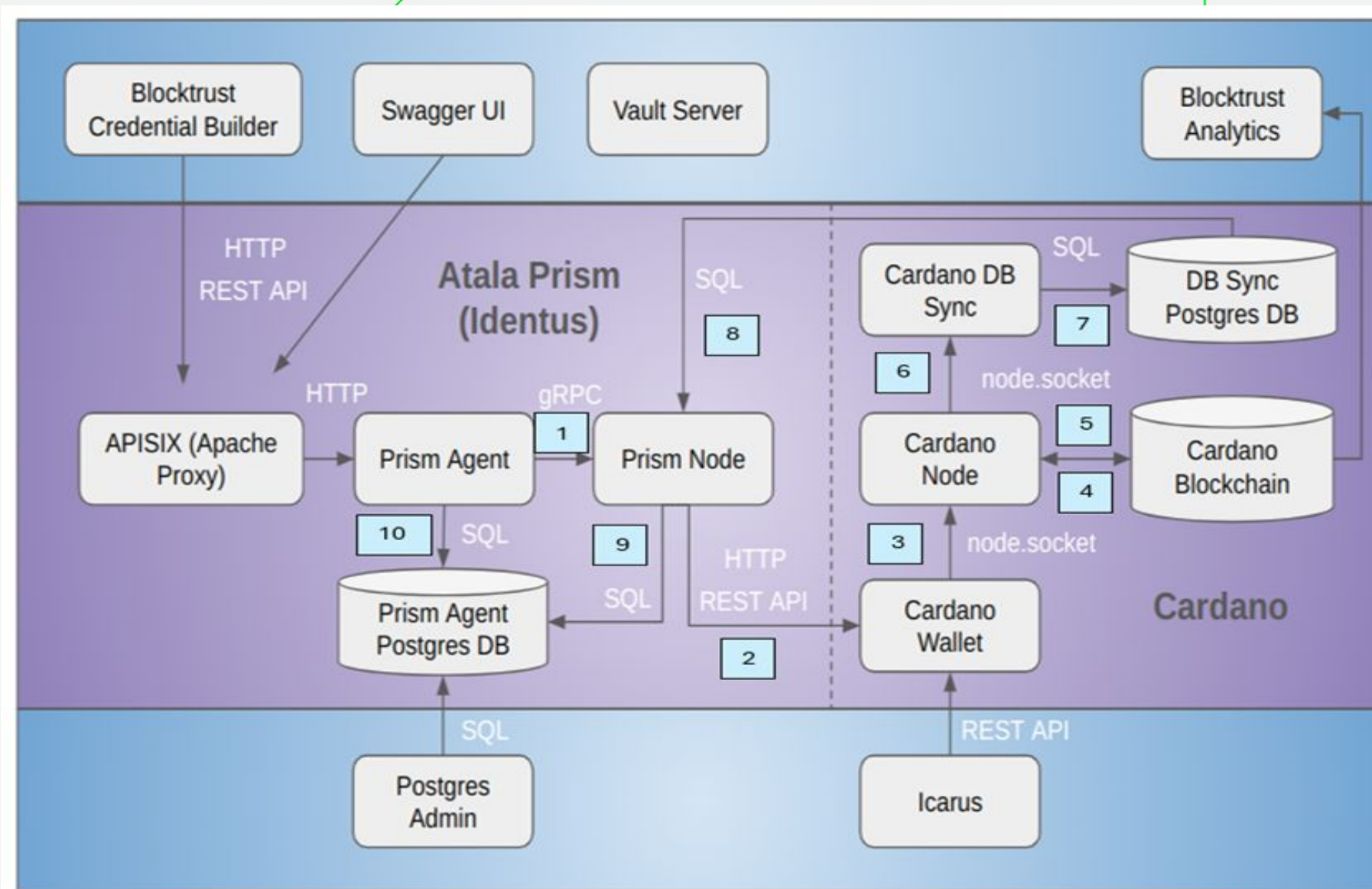


Arquitetura: Hyperledger Indentus



- Cloud agent: emite e verifica DIDs/credenciais
- Edge agent: lida com a carteira que armazena DIDs/credenciais

Arquitetura: Cardano



← → ↻ downloads.csnapshots.io/testnet/testnet-db-snapshot.json

JSON Dados brutos Cabeçalhos

Salvar Copiar Recolher tudo Expandir tudo 🔍 Filtrar JSON

▼ 0:

- db_date: "06:29 Sat, Feb 07, 2026."
- node_version: "10.5.3"
- slot: "114757189"
- epoch: "269"
- height: "4398498"
- block_hash: "'2d2935a16e041fd50fe84dabf999bc5339d4f70756dc9aa97d69b276ed27c098'"
- download_size: "4.2G"
- db_size: "17G"
- checksum: "DCFC433F83AA1FA113E24ED459C5F6562FD0304585BA79030135CF53D1018F53"
- file_name: "testnet-db-114757189.tar.zst"

```
carla@cardano:~/cardano-wallet/run/preprod/docker$ docker exec -it cardano-cardano-node-1 bash
ubuntu@c657db9c2b6e:/$ cardano-cli query tip --testnet-magic 1
{
  "block": 4121703,
  "epoch": 252,
  "era": "Conway",
  "hash": "98f2aab4d4fa364b63f2ff3632d6390001156ff426a859e0ba74255d02f42e70",
  "slot": 107433664,
  "slotInEpoch": 211264,
  "slotsToEpochEnd": 220736,
  "syncProgress": "100.00"
}ubuntu@c657db9c2b6e:/$
```

Correções feitas:

- versão cardano-node do wallet incompatível com preprod
- sem arquivo peer-snapshot.json
- snapshot.sh simplificado
- criado patch

Versões usadas no SWARM:

cardano-wallet: 2025.3.31
cardano-node: 10.5.1
cardano-db-sync: 13.6.0.5



Ambientes de testes: Carteira Cardano e saldo de tADA

Icarus: implementação de carteiras leves para a Cardano

<https://hub.docker.com/r/piotrstachyra/icarus>

Colocar tADA na carteira:

<https://docs.cardano.org/cardano-testnets/tools/faucet>

The screenshot displays the Icarus wallet interface in a web browser. The address bar shows the URL: `http://127.0.0.1:4444/wallets/60ab2bb34ec793d6cda44fc90ab7514075e948ee#`. The interface includes a navigation bar with links: "Shelley wallets", "Shared wallets", "Byron wallets", "Stake-pools", "Misc", and "Tools". Below this, there are tabs for "List All Shelley", "Management", "Transactions", "Assets", "Migrations", "Delegation", and "Co". The main content area shows details for a wallet named "carteira1".

Balance: (Total: 9992.402677 ₳ , Available: 9992.402677 ₳ , Rewards: 0.0 ₳)
Assets: N/A
ID: 60ab2bb34ec793d6cda44fc90ab7514075e948ee
Status: ready
Tip: (Height: 4254143 , Epoch: 260 , Slot: 74558)

Delegation active:
Status: not_delegating

Address pool gap: 20
Addresses:
Total: 53
Used: 33
Unused: 20
Transactions:
Total: 38
Status:
Pending: 0
Expired: 3
InLedger: 35
Direction:
Incoming: 1
Outgoing: 37

Txs in ledger:
ID: c0379c490853cab97f9d35a5adbd10685e3d0ce339dd9b8d2709761c33a64476
in_ledger **has metadata**
Inserted at:
Time: 2025-12-22T18:28:36Z
(Block: 4253871, Epoch: 260, Slot: 66516)
Status: in_ledger
Amount: 183409
Direction: outgoing
Depth: 272 blocks

Ambientes de testes: Transação de registro de DID na blockchain Cardano

```
curl --request POST 'http://10.1.2.8:8080/cloud-agent/did-  
registrar/dids/did:prism:6ef7b0450cf2ee4f33a97bba2cca687ad260908038b562fe89c04e56f9c55914/publications'  
{  
  "scheduledOperation": {  
    "id": "21b558925f7db01345a94c0798cde36e6d3ad7957167d12db2f6dfe9189b65f4",  
    "didRef": "did:prism:6ef7b0450cf2ee4f33a97bba2cca687ad260908038b562fe89c04e56f9c55914"  
  }  
}
```

<https://preprod.cardanoscan.io>

The screenshot displays the Cardanoscan (PreProd) interface. The top navigation bar includes links for Home, Governance, Blockchain, Tokens, Pools, Certificates, and Developers. A search bar is present with the text "Search transaction, address, block, epoch.slot, pool, stakeKey, policyId.assetNar". The main content area is titled "Transaction Details" and shows the following information:

Transaction Hash	Timestamp
a36216cd30059c721323be15e40cf52839fc07eaa9e8755eed6e8f8414bac3c4	Nov 24, 2025 11:35:52 PM
Block	Total Fees
4162599	0.183365 ADA
Assurance	Total Output
High 1329 confirmations	9,996.269356 ADA
Epoch / Slot	Certificates
254 / 268552	0
Absolute Slot	TTL
108354952	Nov 25, 2025 1:23:48 AM (108361428)

Ambientes de testes: Resolução de DID na blockchain Cardano

← → ↺ statistics.blocktrust.dev/resolve Entrar

statistics Register Login

Network Overview

Resolve DID

PRISM

Mainnet ⓘ

Preprod

INDY

Sovrin Mainnet ⓘ

Sovrin Staging

Sovrin Builder

IDunion Mainnet ⓘ

IDunion Testnet

Indicio Mainnet ⓘ

Indicio Testnet

did:prism:preprod:a0b06e388c98651622601c31b3b3c36207872834202db412d1c5dd408eb862b4

Resolve

Current version

a0b06e388c98651622601c31b3b3c3620787283...
25/11/2025 02:35:52

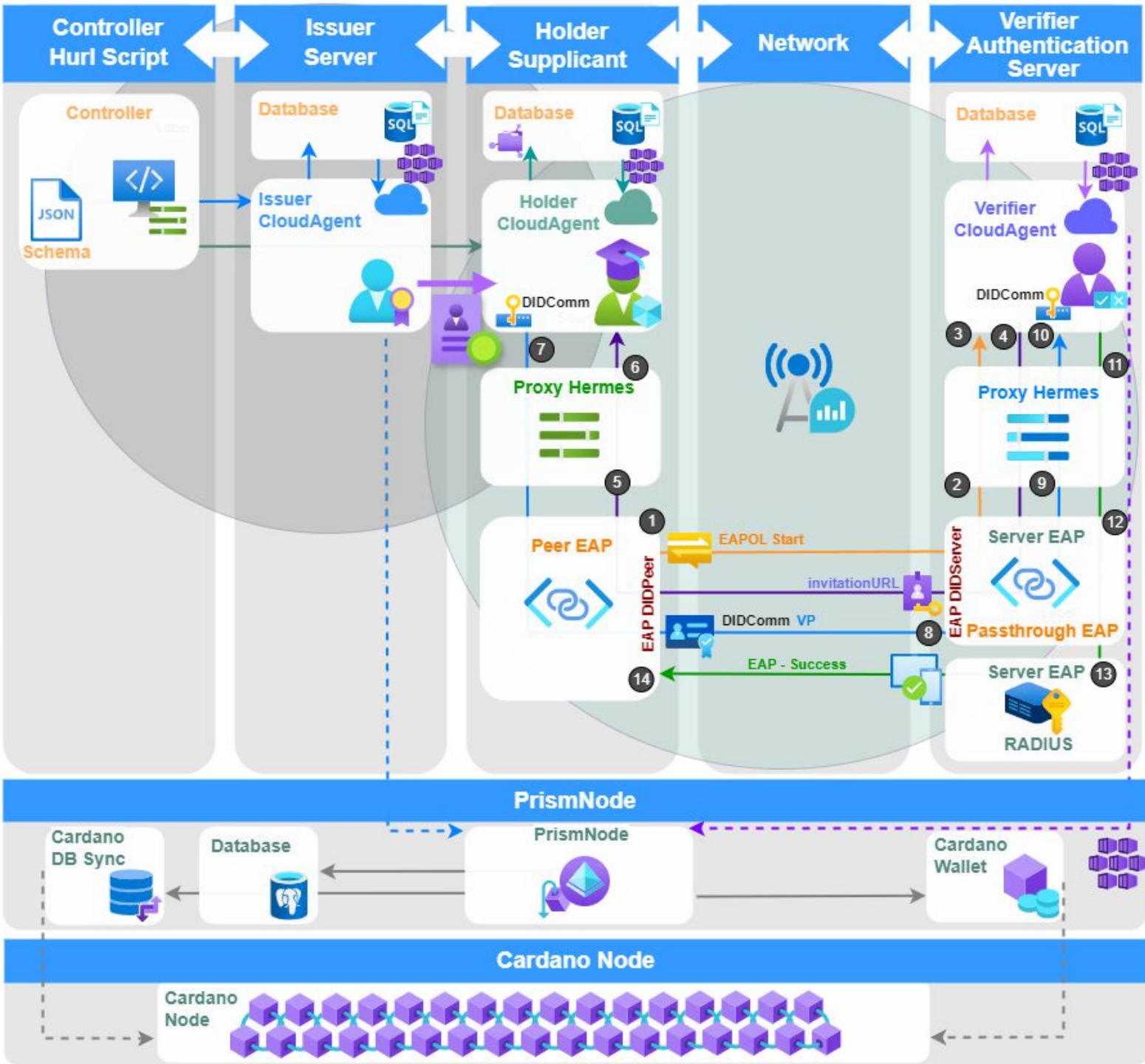
Resolution result

Version: a0b06e388c98651622601c31b3b3c36207872834202db412d1c5dd408eb862b4	✕
DID DOCUMENT	☒
JsonLd-Context https://www.w3.org/ns/did/v1	☐ ☐
JsonLd-Context https://w3id.org/security/suites/jws-2020/v1	☐ ☐
Authentication #auth-1 JsonWebKey2020 (ES256K, RS256, EdDSA)	☐
Assertion Method #issue-1 JsonWebKey2020 (ES256K, RS256, EdDSA)	☐
METADATA	☒
DID-RESOLUTION METADATA	☒
BLOCKTRUST RESOLUTION METADATA	☒

<https://statistics.blocktrust.dev/resolve>



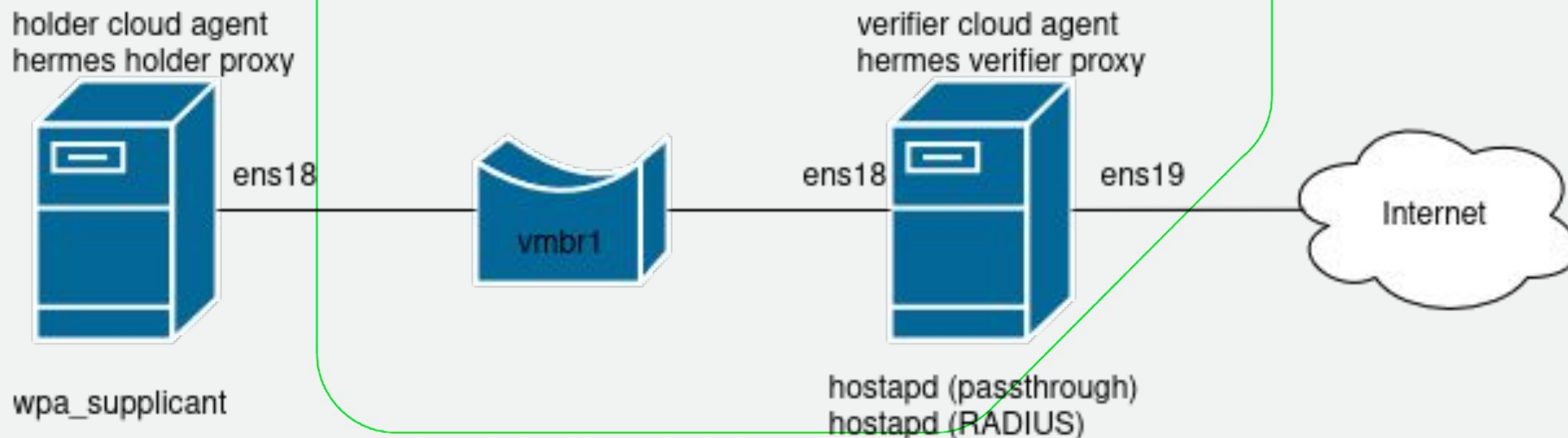
Ambientes de testes



<https://hurl.dev>¹

Testes de desempenho: Autenticação EAP-MD5 x EAP-DID

- Servidor 96 x AMD EPYC 7413 24-Core Processor (2 Sockets), 256GB RAM e 24TB Disco
- ProxMox 8.3.0
- VMs Ubuntu 24.04.3 LTS
- Habilitar EAP na bridge entre as VMs
 - `echo 8 > /sys/class/net/vmbr1/bridge/group_fwd_mask`



Ambientes de testes

```
suplicante@suplicante: ~  
suplicante@suplicante:~$ sudo docker ps  
CONTAINER ID   IMAGE                                COMMAND                  CREATED        STATUS  
PORTS  
59508028d4e3   hyperledgeridentus/identus-cloud-agent:2.0.0   "/opt/docker/bin/ide..." 2 days ago    Up 2 days  
8085/tcp, 8090/tcp  
1blae741f694   hyperledgeridentus/identus-cloud-agent:2.0.0   "/opt/docker/bin/ide..." 2 days ago    Up 2 days  
8085/tcp, 8090/tcp  
26fdcf2bea0b   ghcr.io/input-output-hk/prism-node:2.4.0       "/opt/docker/bin/node"    2 days ago    Up 2 days  
5432/tcp, 0.0.0.0:50053->50053/tcp, [::]:50053->50053/tcp  
1021b990c864   caddy:2.7.6-alpine                             "caddy run --config ..." 2 days ago    Up 2 days  
80/tcp, 443/tcp, 2019/tcp, 443/udp, 0.0.0.0:8081->8081/tcp, [::]:8081->8081/tcp  
3db072bbd499   local/didcomm-proxy-a:py                     "python -u proxy-hol..." 2 days ago    Up 2 days  
0.0.0.0:2022->2022/tcp, [::]:2022->2022/tcp  
9deld0762e28   postgres:13                                    "docker-entrypoint.s..." 2 days ago    Up 2 days (health  
y) 5432/tcp  
ddbdf37b8907   caddy:2.7.6-alpine                             "caddy run --config ..." 2 days ago    Up 2 days  
80/tcp, 443/tcp, 2019/tcp, 443/udp, 0.0.0.0:8080->8080/tcp, [::]:8080->8080/tcp  
e0667869ec59   postgres:13                                    "docker-entrypoint.s..." 2 days ago    Up 2 days (health  
y) 5432/tcp  
27488fb4b40a   postgres:13                                    "docker-entrypoint.s..." 2 days ago    Up 2 days (health  
y) 5432/tcp  
suplicante@suplicante:~$
```

```
hostapd@hostapd: ~  
hostapd@hostapd:~$ docker ps  
CONTAINER ID   IMAGE                                COMMAND                  CREATED        STATUS  
PORTS  
7b50260186f2   local/didcomm-proxy-b:py             "python -u proxy-ver..." 21 hours ago   Up 21 hours  
0.0.0.0:2020->2020/tcp, [::]:2020->2020/tcp  
ac67b66be569   postgres:13                           "docker-entrypoint.s..." 21 hours ago   Up 21 hours (health  
y) 5432/tcp  
39e6984151ed   caddy:2.7.6-alpine                   "caddy run --config ..." 21 hours ago   Up 21 hours  
80/tcp, 443/tcp, 2019/tcp, 443/udp, 0.0.0.0:8082->8082/tcp, [::]:8082->8082/tcp  
84418383454d   hyperledgeridentus/identus-cloud-agent:2.0.0   "/opt/docker/bin/ide..." 21 hours ago   Up 21 hours  
8085/tcp, 8090/tcp  
hostapd@hostapd:~$
```

Ambientes de testes - vídeos de execução

Processo de autenticação:

https://drive.google.com/file/d/10k97qPLhhtA8ZuXmcfPwobhXc5TP1jca/view?usp=drive_link

Apresentação verificável:

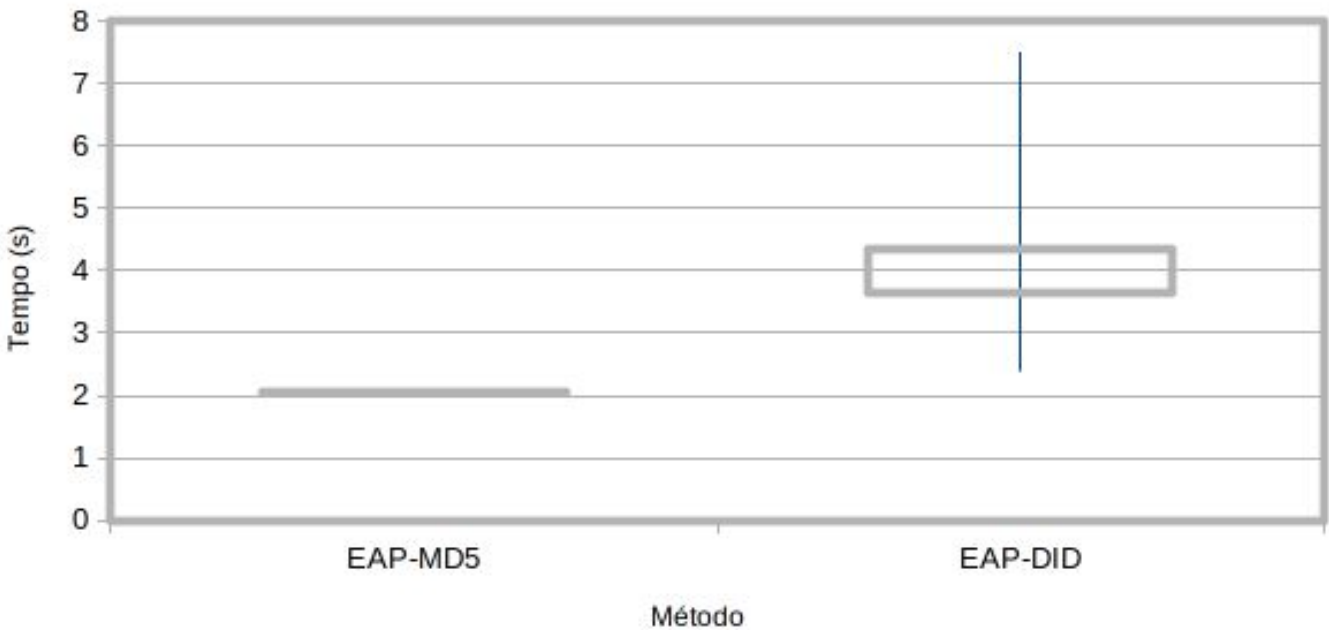
https://drive.google.com/file/d/1shVOybYE_9FhE4TBarSuCC7MMTwdbEKC/view?usp=drive_link



Testes de desempenho: Autenticação EAP-MD5 x EAP-DID

- Medição dos tempos de execução da autenticação 802.1x
 - `./wpa_supplicant -dddt -D wired -i ens18 -c ../TESTE/wpa_supplicant.conf | grep "wpa_supplicant v2.11\|EAPOL authentication completed - result=SUCCESS"`

Tempos médios de autenticação



	EAP-MD5	EAP-DID
Média	2,0634	3,9985
Variância	0,0043	0,9897
Mínimo	2,0568	2,0710
Máximo	2,3858	7,5087

* média de 30 execuções

Conclusão

- A criação e implementação do novo método EAP-DID provê encapsulamento de mensagens DIDCommv2 para realizar um fluxo completo de autenticação baseado em apresentações verificáveis (VP), mesmo antes da disponibilização de conectividade IP ao dispositivo cliente
- A implementação do protótipo validou os principais componentes:
 - geração de DIDs e credenciais verificáveis
 - funcionamento completo dos Cloud Agents do Hyperledger Indentus (Issuer, Holder, Verifier)
 - integração com o VDR em memória e com a blockchain Cardano
 - funcionamento do método EAP-DID no suplicante e servidor RADIUS
 - o papel dos proxies HERMES no tunelamento entre os ambientes 802.1X e DIDCommv2
- Segurança mantida nas mensagens OOB e DIDCommv2, já que o EAP-DID faz apenas o encapsulamento dessas mensagens



Conclusão: Posicionamento do projeto



- Iniciativas de modernização da eduroam que proporcionem maior privacidade [Petric, 2024] [Palamà et al., 2022] [Ahmed e Hussain, 2021] [Brenza et al., 2015]
- Comunidade de pesquisa em identidade digital e segurança de redes [Mazzocca et al., 2025] [Preukschat e Reed, 2021] [dos Santos, 2024] [Hoffmann et al., 2025]
- Projetos internacionais voltados a IDD, identidade descentralizada e credenciais verificáveis, como por exemplo, a iniciativa europeia eIDAS 2.0, o padrão OpenID4VC (OpenID para Credenciais Verificáveis) e plataformas do projeto Hyperledger [ONB, 2025]
- No mercado, evoluiu padrões consolidados (EAP) e tem semelhança com o projeto ROAM [MetaBlox Labs, 2025]

Trabalhos Futuros

- Suplicantes compatíveis com EAP-DID nos clientes
- Arquitetura de governança para delegação de emissão de DID/VC
- Carteiras para armazenamento seguro de credenciais
- Padronização do EAP-DID em órgãos como o IETF e IANA
- Testes de desempenho com testnet Cardano (preprod)
- Otimização da comunicação entre os proxies HERMES e os agentes Identus
- Funções `eap_did_getKey` e `eap_did_emsk` para MSK e EMSK
- Avaliação de uso em produção e testbeds da eduroam
- Exploração de recursos avançados como ZKPs e divulgação seletiva de atributos





*Blockchain
em evolução.*



Obrigado!

GT SWARM

carla.merkle.westphall@ufsc.br

caciano@cpd.ufrgs.br

eduu.hoffmann@gmail.com

cristiann.alves@gmail.com



Referências

Ahmed, F., Hussain, S. A. "A Privacy-Preserving Cross-domain Network access Services Using Sovrin Identifier," 2021 International Conference on Cyber Warfare and Security (ICCWS 2021).

Brenza, S., Pawlowski, A., Pöpper, C.: A practical investigation of identity theft vulnerabilities in Eudroam. In: Proceedings of the 8th ACM Conference on Security and Privacy in Wireless and Mobile Networks. ACM, 2015.

dos Santos, Cristian Alves. Uma abordagem para a integridade dos dados na preservação de evidências forenses usando identidades autossobranas. 2024. Dissertação (Programa de Pós-Graduação em Ciência da Computação) - Universidade Federal de Santa Catarina. <https://repositorio.ufsc.br/handle/123456789/257692>

Hoffmann, Eduardo Freitas; Machado, Caciano; Westphall, Carla Merkle. RadChain Connect: Integration Between Blockchain and FreeRADIUS for Secure Authentication in Wi-Fi Networks/Web Environment In: 2025 International Conference on Information Networking (ICOIN), 2025, Chiang Mai. 2025 International Conference on Information Networking (ICOIN)IEEE, 2025, v.1, p.431 - 436.

Referências

Mazzocca, C., Acar, A., Uluagac, S., Montanari, R., Bellavista, R. and Conti, M. A Survey on Decentralized Identifiers and Verifiable Credentials. IEEE Communications Surveys & Tutorials, doi: 10.1109/COMST.2025.3543197.

MetaBlox Labs. Roam: Decentralized OpenRoaming WiFi Networks. <https://weroam.xyz/whitepaper/>

ONB (Observatório Nacional de Blockchain). META A5.1 – Prospecção tecnológica, padronização e aspectos legais em identidade digital descentralizada. Projeto Ilíada - Fase 1. Relatório da Meta Física 5: A6.3 – Pesquisa e Desenvolvimento em Identidade Digital Descentralizada. Maio de 2025.

Palamà, I., Amici, A., Gringoli, F., Bianchi, G.: “Careful with that Roam, Edu” :experimental analysis of Eduroam credential stealing attacks. In: 17th Wireless On-Demand Network Systems and Services Conference, IEEE, 2022.

Petric, R. (2024). Specifying SSI over EAP: Towards an Even Better Eduroam in the Future. In: Barolli, L. (eds) Advanced Information Networking and Applications. AINA 2024. Lecture Notes on Data Engineering and Communications Technologies, vol 202. Springer, Cham. https://doi.org/10.1007/978-3-031-57916-5_6

Preukschat, Alex; Reed, Drummond. Self-Sovereign Identity. Manning Publications, July 2021.

