PROJETO ILIADA

Blockchain
em evolução.

GT-SWARM
Self-sovereign Wi-Fi Authentication Roaming

Carla Merkle, Caciano Machado,
Cristian Alves, Eduardo Hoffmann

Março/2025

UFSC - Laboratório de Redes e Gerência
LRG

UFSC

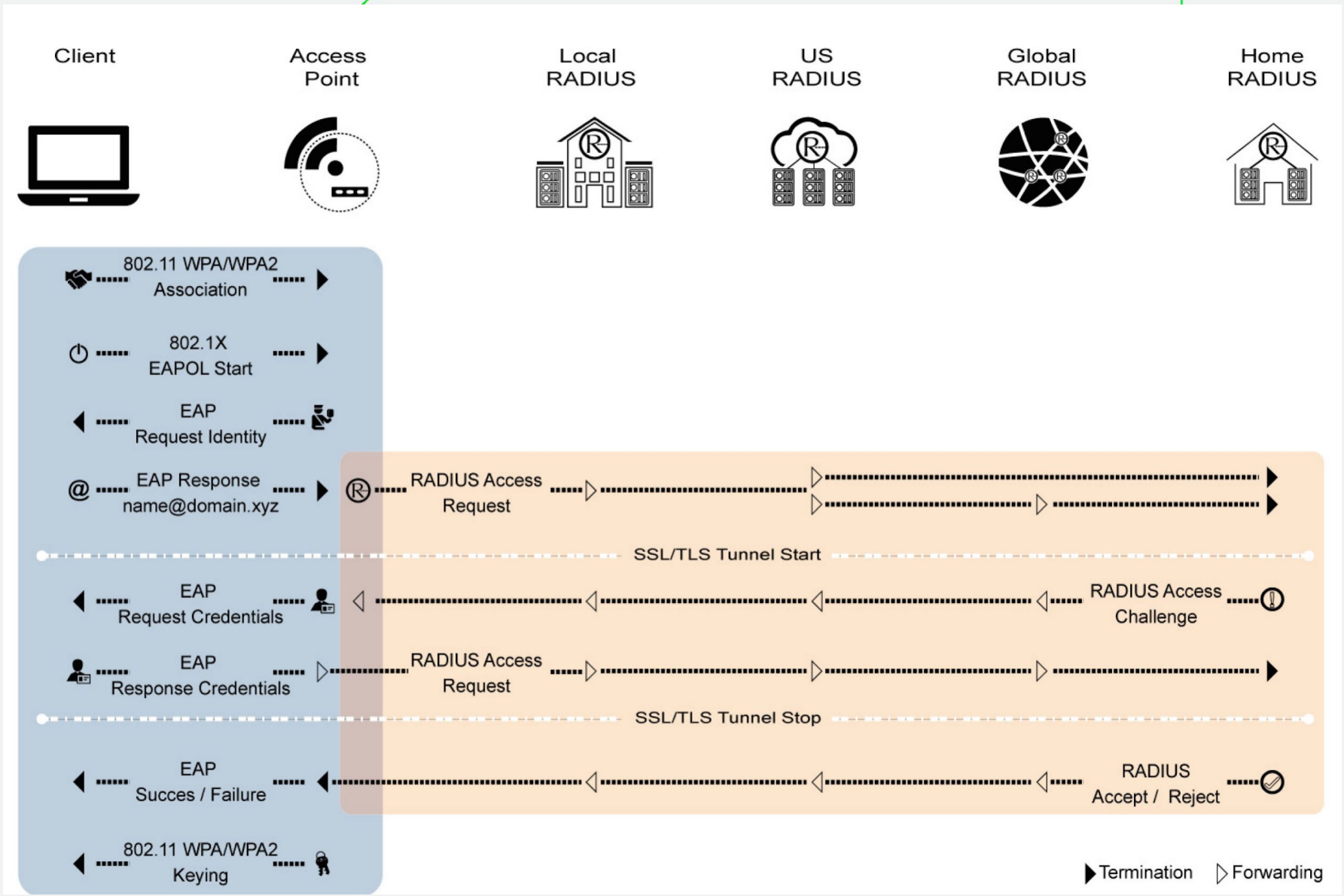
Sumário

Introdução

SWARM - Self-sovereign Wi-Fi Authentication Roaming

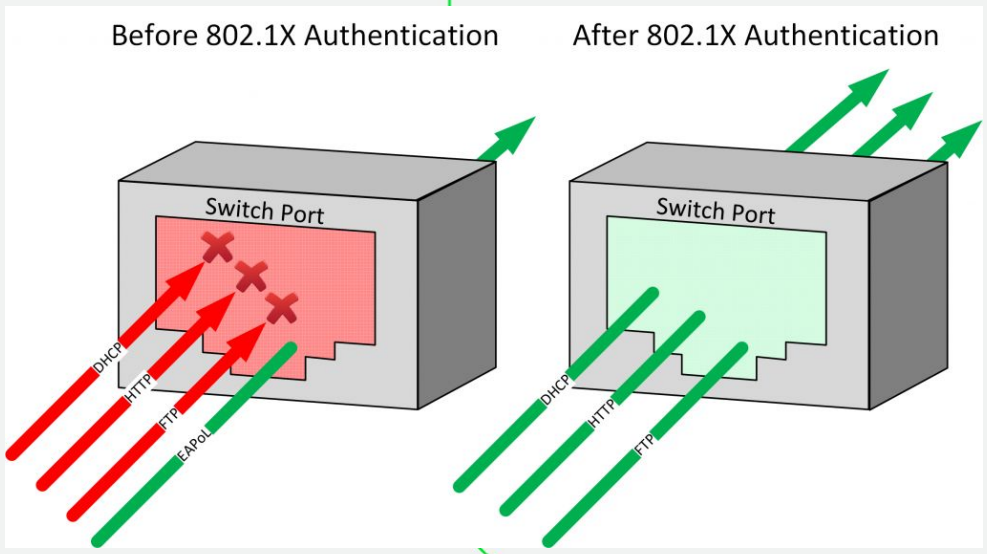
- Integração do 802.1x ao modelo DID/VC/VDR
- Plataforma de emissão de VC para autenticação WiFi

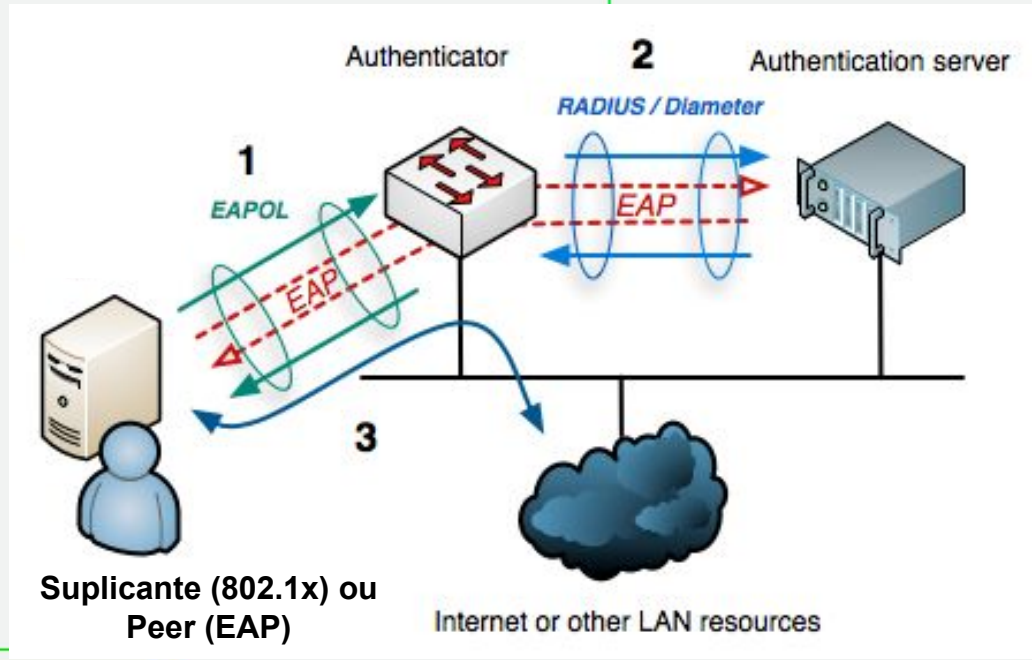
Introdução: Eduroam



Introdução: 802.1x e EAP

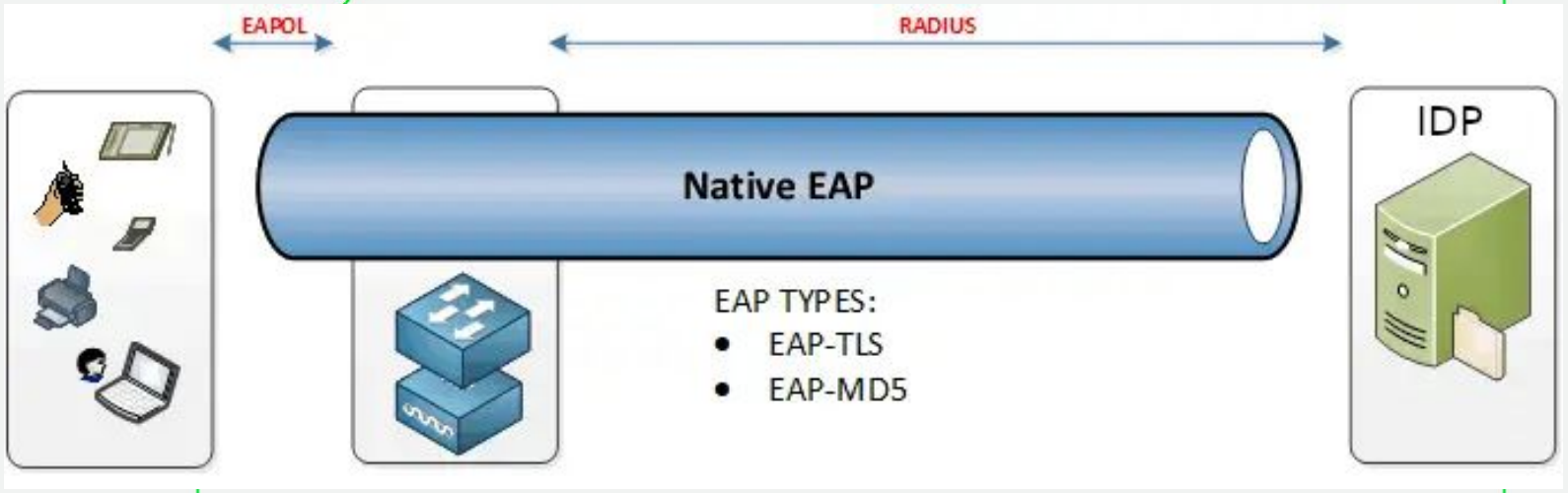
- *Extensible Authentication Protocol* - RFC 3748
- Framework de autenticação para acesso à rede utilizado pelo 802.1x
- Agentes
  - **Peer (EAP) / suplicante (802.1x)** – Dispositivo sendo autenticado
  - **Autenticador / Cliente RADIUS** – Switch/Access Point de acesso
  - **Servidor de Autenticação** – RADIUS com acesso à base de usuários





Introdução: Métodos EAP

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

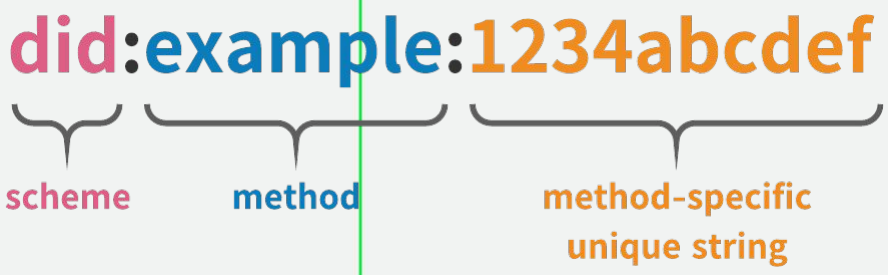


- Eduroam utiliza outer tunnel PEAP/TTLS e inner tunnel MSCHAPv2

Introdução: Padrões técnicos que dão suporte à SSI

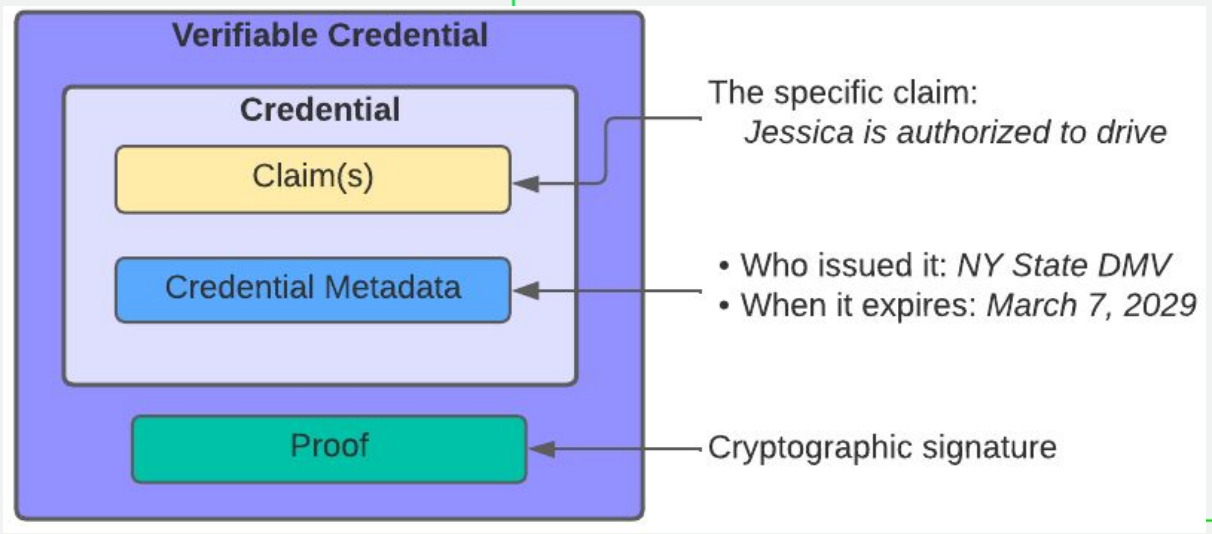
DIDs (Decentralized Identifiers):

- Identificadores únicos e descentralizados, armazenados em blockchains ou VDRs
- ex: `did:v1:nym:BcNkgGmGEpCGSJSMPB4BvWvwVM6YeTR52BSWcZTbzU23`



VCs (Verifiable Credentials):

- Credenciais digitais criptograficamente verificáveis
- Exemplo: diploma universitário, carteira de motorista digital

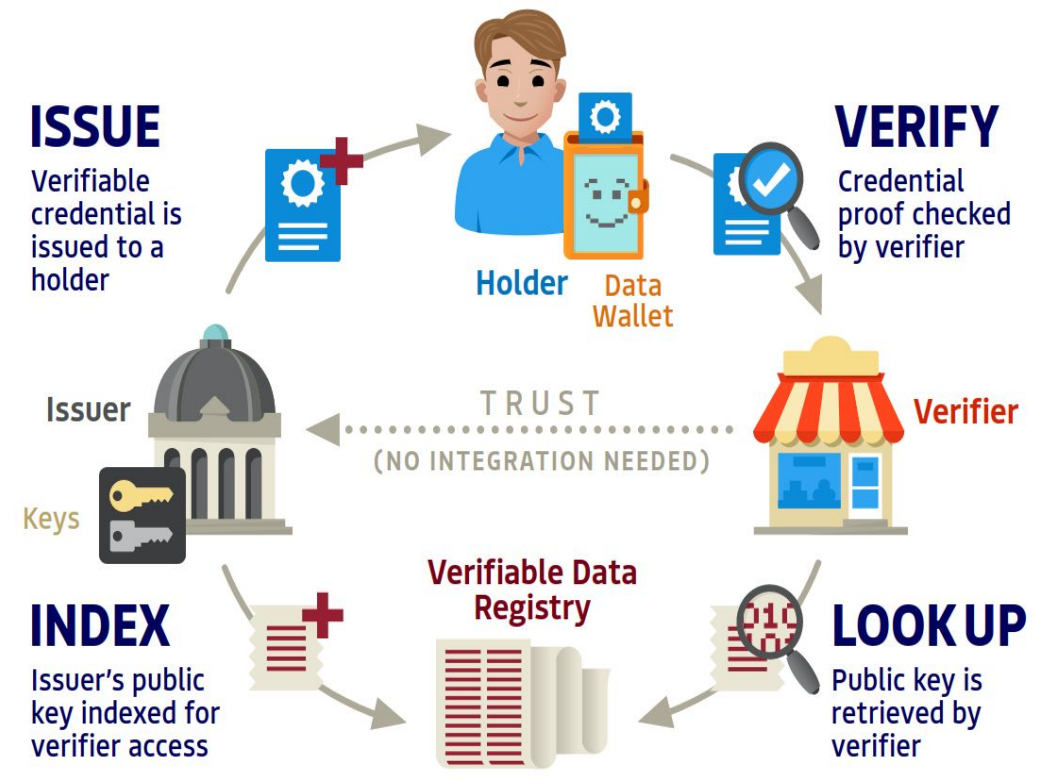



```
{
  "id": "did:example:aluno123",
  "nome": "João Silva",
  "curso": "Ciência da Computação",
  "data_conclusao": "2023-10-01",
  "nota_final": "9.5"
}
```

Introdução: Padrões técnicos que dão suporte à SSI

Blockchain e VDRs (Verifiable Data Registries):

- Infraestrutura descentralizada para registrar/verificar DIDs e VCs
- Ex. de blockchains: Ethereum, Hyperledger Indy, Sovrin



https://trustoverip.org/

Blockchain em evolução.

Introdução: Soluções e seu papel na SSI

Hyperledger INDY

- Ferramentas para DIDs, VCs e VDRs

Hyperledger IDENTUS

- Componentes para soluções de IDD em SSI

Hyperledger ARIES

- Framework para credenciais e comunicação segura

Hyperledger ANONCREDS

- Formato de VC mais comum

ACA-Py

- Aries Cloud Agent Python
- Agente leve para implementar SSI

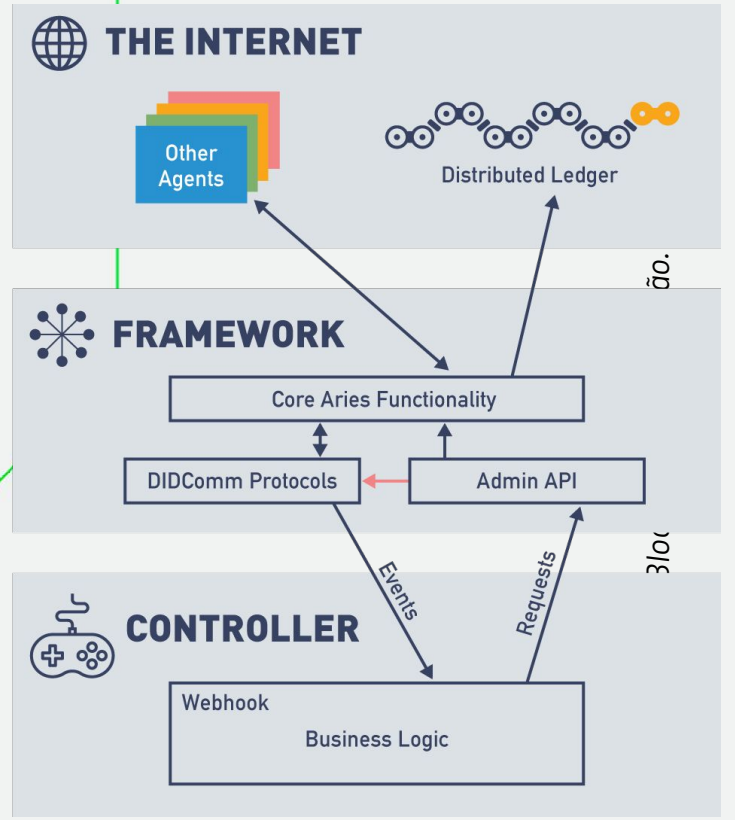
Outras soluções possíveis:

- Hyperledger Fabric
- Hyperledger Besu
- uPort
- Veramo

OpenWallet FOUNDATION

TRUST Over IP

CREDEBL



Problema: Limitações do eduroam

- Senhas para autenticação WiFi -> mecanismo de segurança fraco
  - Necessário lembrar senhas complexas
- Necessidade de identificar usuário na autenticação -> problema de privacidade
- CA desconhecida para o 802.1x nos dispositivos dos clientes
  - Dificuldade de instalar certificados para servidores RADIUS nos clientes que torna a autenticação suscetível a ataques MitM, com quebra da integridade e confidencialidade do outer tunnel [1][2]
- Pontos de falha na infraestrutura da federação RADIUS do eduroam

[1] Brenza, S., Pawlowski, A., P¨opper, C.: A practical investigation of identity theft vulnerabilities in Eduroam. In: Proceedings of the 8th ACM Conference on Security and Privacy in Wireless and Mobile Networks. ACM, 2015

[2] Palam`a, 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

Problema: Referencial teórico sobre eduroam + SSI [3] [4]

- Maior controle do usuário sobre seus dados
- Autenticação sem senhas, baseada em VC
- Privacidade aprimorada (ZKP)
- Maior dependabilidade, não depende de toda uma infraestrutura de RADIUS, com utilização de VDR em blockchain

[3] 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)

[4] Petrlic, 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

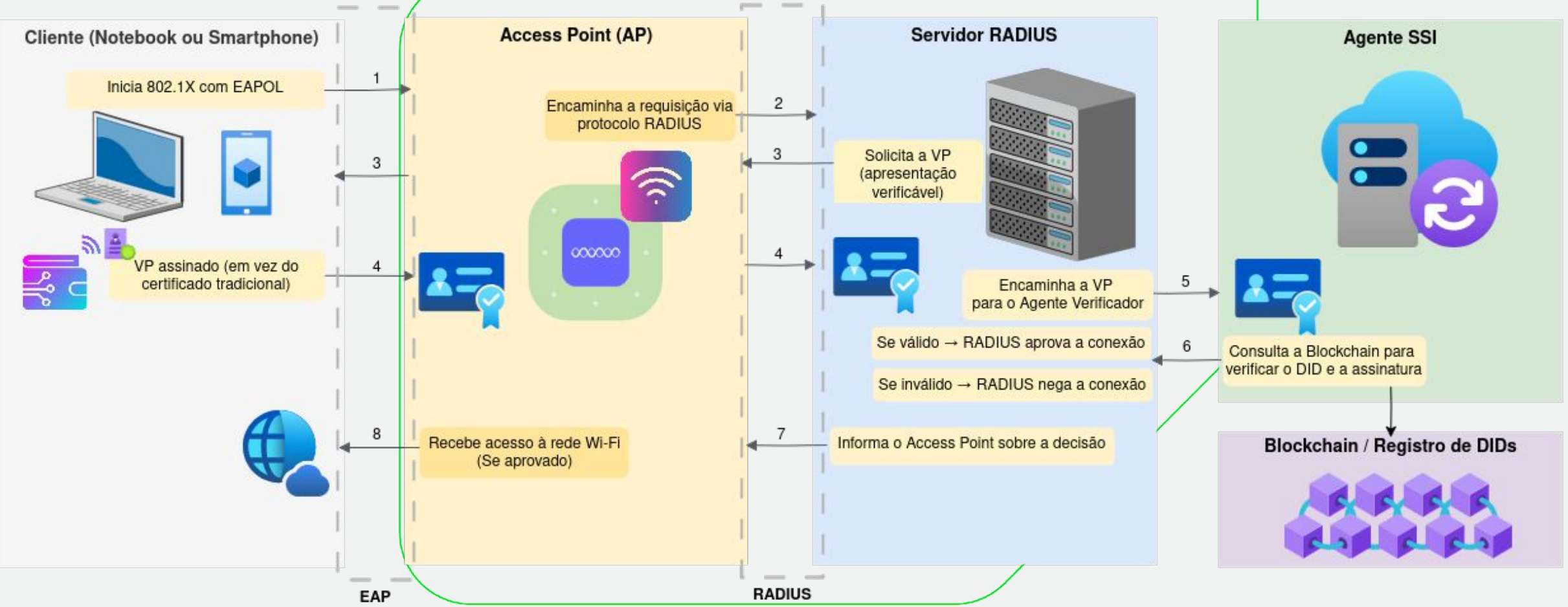
Blockchain em evolução.

Objetivo

- Permitir autenticação de redes federadas como o eduroam com identificadores descentralizados (DDI) utilizando a infraestrutura padrão *de facto* do 802.1x

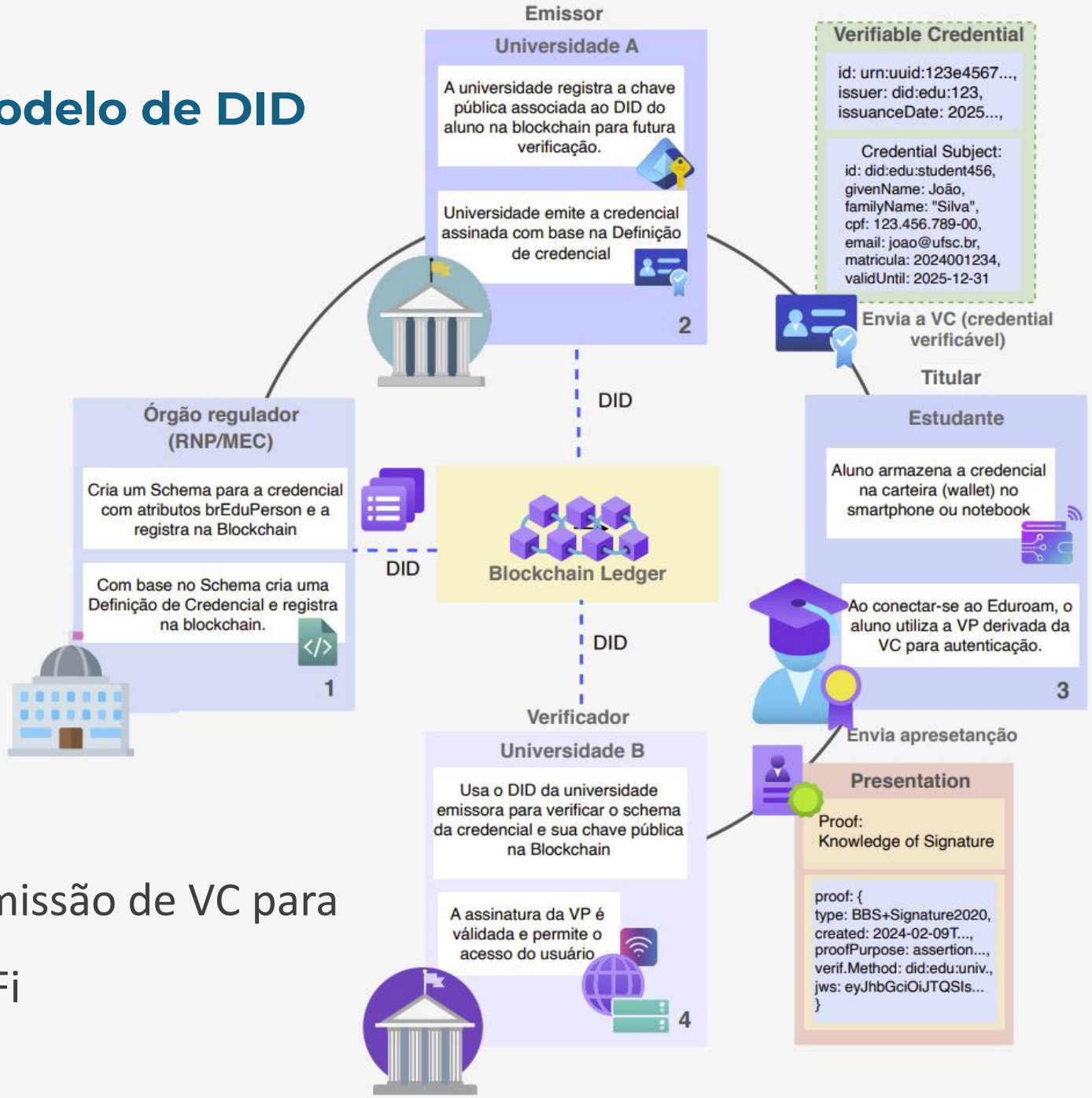
Proposta - Autenticação

- Adequação do 802.1x ao modelo VC/DID/VDR
- Integração de novos métodos EAP aos padrões de autenticação de facto de redes WiFi



Blockchain em evolução.

Proposta - Modelo de DID



- Plataforma de emissão de VC para autenticação WiFi

Proposta: Objetivos Específicos e Atividades

- Levantar abordagens apropriadas para autenticação DID/VC, retrocompatíveis com redes WiFi convencionais 802.1x (introduzir novo método EAP)
- Elaborar os mecanismos de DID/VC e especificar abordagens apropriadas para armazenamento de VCs para a autenticação
- Integrar proposta do GT na rede eduroam, utilizando TestBed da RNP, caso seja possível e apropriado, para gerar um produto mínimo viável

A. Revisão sistemática de métodos 802.1x
B. Revisão sistemática de autenticação WIFi com SSI
C. Modelagem e adequação da autenticação DID/VC com 802.1x
D. Protótipo de integração do Radius para autenticação de usuários na blockchain
E. Modelagem da plataforma para emissão de VC para DID
F. Protótipo da plataforma para emissão de VC para DID
G. Desenvolvimento do MVP para emissão de VC para DID
H. Publicação de artigos científicos
I. Elaboração de relatórios técnicos

ATIVIDADES	MESES											
	1º Mês	2º Mês	3º Mês	4º Mês	5º Mês	6º Mês	7º Mês	8º Mês	9º Mês	10º Mês	11º Mês	12º Mês
	Mar/ 2025	Abr/ 2025	Mai/ 2025	Jun/ 2025	Jul/ 2025	Ago/ 2025	Set/ 2025	Out/ 2025	Nov/ 2025			
Atividade A	x	x										
Atividade B		x	x									
Atividade C			x	x	x							
Atividade D					x	x	x	x				
Atividade E	x	x	x	x								
Atividade F				x	x							
Atividade G					x	x	x	x				
Atividade H									x			

Blockchain em evolução.

Resultados Esperados

- Complementar métodos tradicionais de autenticação com as credenciais verificáveis no contexto do eduroam da RNP
- Elaborar formato piloto de emissão de DID/VC para usuários da RNP usando plataformas de SSI disponíveis
- Preparar servidores Radius para autenticar usuários usando esse novo formato de DID/VC
- Montar estrutura de rede de teste e blockchain apropriada
- Integrar implementações usando testbeds da RNP (se possível) para gerar um produto mínimo viável (MVP)

PROJETO ILIADA

Blockchain
em evolução.

Obrigado!

GT SWARM

carla.merkle.westphall@ufsc.br
caciano@cpd.ufrgs.br
eduu.hoffmann@gmail.com
cristiann.alves@gmail.com

RNP

SWARM

UFSC

UFSC - Laboratório de Redes e Gerência
LRG