Identidade Descentralizada em Open RAN: Governança descentralizada de xApps/rApps via Credenciais Verificáveis

Bruno Evaristo[1,2], **Antonio Gomes Abelem**[1]

[1]Instituto de Computação – Universidade Federal do Pará(UFPA)
Belem – PA – Brasil

[2]Centro de Pesquisa e Desenvolvimento em Telecomunicações(CPQD)
Campinas – SP – Brasil

elderb@cpqd.com.br, abelem@ufpa.br

Resumo. *A desagregação da Open RAN expõe o RAN Intelligent Controller (RIC) a aplicações de terceiros (xApps, rApps, dApps), hoje autenticadas via certificados X.509 e um repositório centralizado (XRF). Propomos tratar cada aplicação como* sujeito soberano de identidade*, com Identificador Descentralizado (DID) e Credenciais Verificáveis (VCs) de capacidade, em arquitetura de seis camadas na qual a autorização é decisão de política* off-chain *ancorada em* ledger *permissionado (Hyperledger Besu), viabilizando admissão Zero-Trust às interfaces E2/A1 e à* Shared Data Layer *sem raiz de confiança central.*

1. Introducao

A Open RAN desagrega a estação base em unidades abertas (O-CU, O-DU, O-RU) e introduz os *RAN Intelligent Controllers* (RICs), que hospedam aplicações de terceiros: xApps no near-RT RIC (E2, 10–1000 ms), rApps no non-RT RIC (A1, $>$1000 ms) e dApps distribuídos, ampliando a superfície de ataque sobre o plano de controle da RAN. O modelo de segurança vigente é *centrado no operador*: a WG11 da O-RAN Alliance exige que o identificador de cada xApp seja associado às credenciais de autenticação (REQ-SEC-XAPP-3), hoje certificados X.509 validados via TLS 1.3. O *xApp Repository Function* (XRF) [Atalay et al. 2023] e extensões hierárquicas [Fernando et al. 2025] proveem autenticação, autorização e descoberta escaláveis, porém sob raiz de confiança centralizada.

Este trabalho investiga: *é possível admitir xApps/rApps/dApps no RIC sem autoridade central, de forma auditável e revogável?* Nossa hipótese é que tratar cada aplicação como *sujeito soberano de identidade*, com DID e Credenciais Verificáveis (VCs) de capacidade, ancorada em *ledger* substitui a raiz centralizada por um modelo Zero-Trust descentralizado. A contribuição é uma arquitetura de seis camadas e seu fluxo de integração, como trabalho em andamento. O tema alinha-se ao contexto nacional: a Open RAN é vetor de soberania sobre infraestrutura crítica, dialogando com as diretrizes brasileiras de identidade digital e proteção de dados (LGPD).

2. Referencial Teórico e Trabalhos Relacionados

2.1. Identidade Auto-Soberana e Trabalhos Relacionados

Um *Decentralized Identifier* (DID) é um identificador único e verificável, independente de autoridade central, que resolve para um *DID Document* com as chaves públicas do sujeito; uma *Verifiable Credential* (VC) associa atributos ao DID, padronizada como *Verifiable Credentials Data Model* 2.0 [Verifiable Credentials Working Group 2025] (Rec. W3C, 2025), com proteção via *Data Integrity*/JOSE/COSE e divulgação seletiva via SD-JWT. Um *Verifiable Data Registry* (VDR) ancora chaves e revogação via *Bitstring Status*

List 1.0: a trinca DID–VC–VDR fundamenta a Identidade Auto-Soberana (SSI), substrato da governança do RIC.

Na literatura, o XRF [Atalay et al. 2023] e extensões hierárquicas [Fernando et al. 2025] resolvem autenticação/autorização de xApps sob confiança centralizada no operador (PKI X.509), sem auditabilidade independente; o BE-RAN [Xu et al. 2024] descentraliza identidade via DLT, mas para NEs e UEs, não aplicações do RIC. Em paralelo, cresce o movimento de equipar agentes de IA com DID e VCs [Evaristo et al. 2025] — precisamente o que são xApps/rApps de IA, atuando sobre o plano de controle da RAN.

2.2. Lacuna e Posicionamento

Identifica-se, assim, uma lacuna: nenhuma abordagem trata xApps/rApps/dApps como *sujeitos soberanos de identidade*, com credenciais de capacidade emitidas e verificadas de forma descentralizada e auditável (Tabela 1). O diferencial não é "usar *blockchain* em RAN" (já proposto pelo BE-RAN), mas deslocar o sujeito da identidade para a aplicação do RIC e tornar a decisão de admissão função de uma prova on-chain, não de autoridade central.

Tabela 1. Posicionamento frente ao estado da arte.

Dimensão	XRF	Hier.	BE-RAN	Proposta
Raiz de confiança	central	central	DLT	DLT (VDR+Besu)
Sujeito de identidade	xApp	xApp	NE/UE	xApp/rApp/dApp
Mecanismo de credencial	token	X.509	DID	DID+Capability VC
Auditabilidade on-chain	não	não	parcial	sim (hash ancorado)
Revogação independente	não	não	sim	sim (status list)
Atribuição forense	não	não	parcial	sim (registro imutável)

3. Proposta da Arquitetura

A arquitetura (Figura 1) organiza-se em seis camadas de comunicação, percorridas por uma sequência de integração de provisionamento (P1) e de tempo de execução (1–10).

(1) Identity & Trust (VDR/SSI). O *vendor*/operador atua como *Trusted Issuer*, assinando VCs de capacidade; um *Authorized-Issuer Registry*, ancorado no mesmo DLT da camada 5, torna a legitimidade de cada emissor um fato multipartes e auditável pelo consórcio, não uma configuração bilateral por RIC como em X.509; o *App Catalogue* (SMO/O-RAN App Store) publica o DID e o *schema* de cada aplicação; um VDR (besu, `did:besu`) ancora chaves públicas e *status list* de revogação.

(2) RIC Apps como sujeitos DID. Cada xApp, rApp e dApp possui um *app-DID* e uma *Capability* VC (RIC alvo, funções, escopo de *Input Control Parameters*, interfaces E2/A1), custodiada por uma *App Identity Wallet* (agente ACA-Py). Adota-se `did:besu` para identidade persistente e `did:web`/`did:key` para instâncias efêmeras; a credencial é emitida em formato SD-JWT VC, habilitando divulgação seletiva.

(3) Verification & Onboarding Agent. Um *Verifier* acoplado ao RIC recebe a *Verifiable Presentation* (VP) via OpenID4VP 1.0 [Hauck et al. 2025] e a processa em *pipeline*: resolução de DID, verificação criptográfica (assinatura, emissor, *status list*), extração de capacidade e canonicalização (RFC 8785, JCS) do contexto de decisão. A prova de posse (*holder binding*) garante que só o detentor legítimo do *app-DID* apresente a credencial.

(4) Governança / Decisão de Política. Um *Policy Engine* ABAC avalia uma função de decisão $G(app) \in \{0, 1\}$ sobre o contexto canônico recebido do Verifier, combinando o resultado da verificação de capacidade com as regras de acesso vigentes para o RIC alvo; a decisão gera um *commitment_hash* determinístico, que sela de forma reprodutível o contexto exato sobre o qual a política foi avaliada.

(5) Semantic Anchoring (DLT). O contrato `AppGovernanceRegistry.sol` (Besu) registra `AppAuthAnchored` e persiste um `AppGovRecord` (⟨`app_did_ref`, `capability_ref`, `ric_target`, `commitment_hash`, `status`, `timestamp`⟩) — sem dado proprietário ou *telemetria* on-chain, apenas o compromisso criptográfico. A DLT *permissionada* (Besu) cabe a operadores/fornecedores conhecidos e governáveis, com finalidade determinística e sem custos de *gas* públicos.
(6) Enforcement. O RIC (near/non-RT + SMO) admite a aplicação a E2/A1 e à *Shared Data Layer se e somente se* a decisão estiver ancorada e validada no contrato: *onboarding* Zero-Trust em que X.509 e o token XRF cedem lugar a *app-DID + Capability VC*.

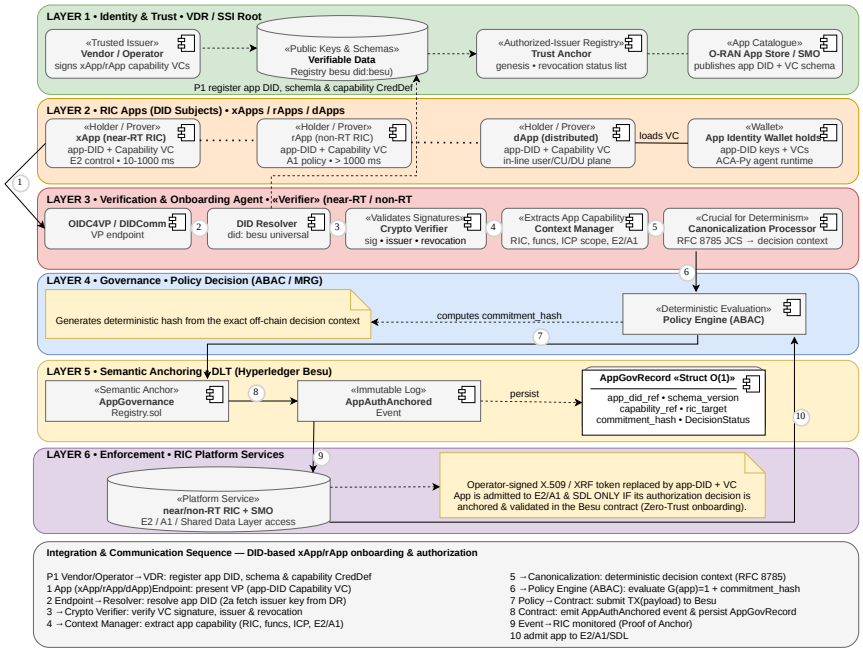

Figura 1. Arquitetura de governança descentralizada para xApps/rApps, com a sequência de integração de provisionamento (P1) e de onboarding/autorização (1–10).

3.1. Sequência de Integração e Comunicação

O fluxo fim-a-fim (Figura 1): **P1** registro de app-DID, *schema* e *CredDef* no VDR; **1** apresentação da VP; **2** resolução do DID (**2a** chave do emissor); **3** verificação de assinatura, emissor e revogação; **4** extração de capacidade; **5** canonicalização do contexto; **6** avaliação ABAC ($G(app) = 1$) e *hash*; **7** submissão da transação; **8** emissão do evento e persistência do `AppGovRecord`; **9** monitoramento (*Proof of Anchor*); **10** admissão ao E2/A1/SDL via *capability token*.

3.2. Propriedades de Segurança e Privacidade

A proposta oferece três garantias: *autenticação sem autoridade central* (a chave do *app-DID* e a VP substituem o segredo compartilhado e o certificado do operador); *auditabilidade e não-repúdio* (cada admissão deixa compromisso imutável e verificável no *ledger*); e *revogação e divulgação seletiva* (a *status list* revoga independentemente do emissor, e a VC revela só os atributos necessários).

3.3. Modelo de Ameaça e Escopo

Distinguimos ataques ao *quem* (identidade), cobertos integralmente, dos ataques ao *como* (comportamento em execução), delimitados explicitamente.

Identidade forjada. A admissão (passo 3) exige *Capability* VC assinada por emissor autorizado; forjá-la demanda a chave privada do emissor, o mesmo obstáculo de um certificado X.509. A proposta não elimina essa confiança no emissor — ela descentraliza a governança de quem é um emissor legítimo (via o *Authorized-Issuer Registry*) e a auditoria das decisões de admissão (via o *ledger*), mantendo a integridade do emissor como pressuposto, como em qualquer PKI.
Credencial roubada. O furto do documento não basta: a VP (passo 1) exige a chave do *app-DID* vinculado (*holder binding*). O comprometimento dessa chave é tratado por revogação via *status list*.
Aplicação legitimamente credenciada, porém maliciosa. Uma aplicação pode, uma vez admitida, agir fora do declarado (e.g., *eavesdropping* de KPIs), limite também de XRF, hierárquicas e BE-RAN, cabendo ao monitoramento de anomalias do RIC (WG11). A arquitetura contribui com *menor privilégio* (VC confina o escopo) e *atribuição forense* (`AppGovRecord` imutável e independente do emissor), tornando a detecção posterior verificável.

4. Conclusão e Trabalhos Futuros

Defendemos o tratamento de xApps, rApps e dApps como sujeitos soberanos de identidade, admitidos ao RIC mediante prova de governança ancorada em *ledger*. Frente ao XRF e ao BE-RAN, a contribuição deste resumo estendido é um passo descentralizado e auditável, materializado nesta arquitetura ainda sem validação empírica. Trabalho futuro: protótipo com ACA-Py e *ledger* Besu; e análise de ameaças estruturada (*VC replay*, *DID spoofing*, comprometimento do *Verifier*).

Agradecimentos

Este trabalho foi parcialmente financiado pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), sob os processos nº 403539/2020-0, nº 302951/2023-7 e nº 400111/2023-3; e pela Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), sob os processos nº 2023/00811-0, nº 2023/00673-7, nº 2021/00199-8 (CPE SMARTNESS), nº 2020/04031-1 e nº 2018/23097-3. Este trabalho também contou com o apoio da PROPESP/UFPA (Pró-Reitoria de Pesquisa e Pós-Graduação da Universidade Federal do Pará).

Referências

Atalay, T. O., Maitra, S., Stojadinovic, D., Stavrou, A., and Wang, H. (2023). Securing 5g openran with a scalable authorization framework for xapps. In *IEEE INFOCOM 2023-IEEE Conference on Computer Communications*, pages 1–10. IEEE.

Evaristo, B., Celeiro, J., and Abelém, A. (2025). Estrutura de governança orientada por regras programáveis com suporte de identidade digital descentralizada. In *Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg)*, pages 119–122. SBC.

Fernando, P., Porambage, P., Liyanage, M., Steenhaut, K., and Braeken, A. (2025). Securing xapps in open ran: A hierarchical approach to authentication and authorisation. In *2025 IEEE Conference on Communications and Network Security (CNS)*, pages 1–9. IEEE.

Hauck, F., Hosseyni, P., Küsters, R., and Würtele, T. (2025). Formal security analysis of the openid for verifiable presentations specification. IACR Cryptology ePrint Archive.

Verifiable Credentials Working Group (2025). Verifiable credentials data model 2.0. Technical report, World Wide Web Consortium (W3C). W3C Recommendation. URL: https://www.w3.org/TR/vc-data-model-2.0.

Xu, H., Zhou, Z., Zhang, L., Sun, Y., et al. (2024). Be-ran: Blockchain-enabled open ran for 6g with did and privacy-preserving communication. In *2024 IEEE Globecom Workshops (GC Wkshps)*, pages 1015–1021. IEEE.