RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 30/09/2026 | aceito: 03/10/2026 | publicação: 06/10/2026

Roaming internacional em redes 5g standalone

International roaming in 5 G standalone networks

Roaming internacional en redes 5G independientes

Danyell Teixeira Soares

Engenheiro de telecomunicações com 16 anos de experiência. MBA em Gestão Empresarial pela Fundação Getulio Vargas (FGV-SP, 2015). Graduado em Engenharia Elétrica com ênfase em Telecomunicações pela Pontifícia Universidade Católica de São Paulo (PUC-SP, 2008).

Resumo

Este artigo investiga os mecanismos arquiteturais, protocolos de segurança e requisitos de governança necessários para garantir a continuidade internacional de serviços em redes 5G Standalone (5G SA). Examina-se a diferenciação entre as topologias Home Routed (HR) e Local Breakout (LBO), o papel do Security Edge Protection Proxy (SEPP) na borda inter-PLMN e a proteção da interface N32 via especificações 3GPP TS 29.573. Analisa-se também o esquema de privacidade de identidade do assinante baseado na cifragem do SUPI em SUCI, mitigando vulnerabilidades históricas de rastreamento. A metodologia baseia-se em uma revisão analítica de normas do 3GPP (Release 18), especificações GSMA (NG.113), relatórios ENISA e artigos científicos revisados por pares. Conclui-se que o sucesso operacional do roaming 5G depende de uma cadeia de confiança ponto a ponto rigorosamente validada por testes bilaterais e observabilidade segmentada por parceiro.

Palavras-chave: Roaming 5G. Home Routed. Local Breakout. SEPP. Interface N32. SUCI.

Abstract

This paper investigates the architectural mechanisms, security protocols, and governance frameworks required to ensure international service continuity in 5G Standalone (5G SA) networks. It details the operational differences between Home Routed (HR) and Local Breakout (LBO) topologies, the role of the Security Edge Protection Proxy (SEPP) at the inter-PLMN boundary, and the protection of the N32 interface according to 3GPP TS 29.573 specifications. It also analyzes subscriber identity privacy mechanisms based on encrypting the SUPI into a SUCI, mitigating legacy tracking vulnerabilities. The methodology relies on an analytical review of 3GPP Release 18 standards, GSMA guidelines (NG.113), ENISA threat reports, and peer-reviewed scientific literature. The study concludes that operational success in 5G roaming depends on an end-to-end chain of trust validated by bilateral testing and partner-segmented observability.

Keywords: 5G Roaming. Home Routed. Local Breakout. SEPP. N32 Interface. SUCI.

1 Introdução

O roaming internacional em redes de telecomunicações móveis é o pilar que possibilita a continuidade global de serviços de voz, mensagens e dados para usuários em deslocamento fora de suas redes de origem (Home Public Land Mobile Network - HPLMN). Nas gerações de redes legadas (2G, 3G e 4G), a sinalização entre redes parceiras apoiava-se fortemente nos protocolos SS7 e Diameter, transportados por redes de troca de tráfego conhecidas como IPX (IP Exchange) (BASIN et al., 2018; ENISA, 2020).

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 30/09/2026 | aceito: 03/10/2026 | publicação: 06/10/2026

Entretanto, as arquiteturas legadas de sinalização sofriam de vulnerabilidades estruturais graves. Os protocolos SS7 e Diameter foram originalmente concebidos sob a premissa ingênua de que a rede de transporte IPX era um ambiente implicitamente confiável. Essa brecha permitiu que malfeitores executassem ataques de falsificação de origem (*spoofing*), interceptação não autorizada de chamadas e mensagens SMS, e o rastreamento em tempo real da localização geográfica dos assinantes (ENISA, 2020).

A introdução do 5G Standalone (5G SA) altera radicalmente esse cenário ao substituir os protocolos legados pela Arquitetura Baseada em Serviços (SBA). No 5G SA, toda a comunicação do plano de controle entre a rede visitada (Visited PLMN - VPLMN) e a rede doméstica (HPLMN) passa a ser tratada através de chamadas de API RESTful sob HTTP/2, exigindo novos paradigmas para a proteção das fronteiras inter-operadoras (3GPP, 2024c; GSMA, 2024).

Para garantir a segurança do ecossistema de roaming inter-PLMN, a norma 3GPP TS 29.573 define o Security Edge Protection Proxy (SEPP) como a função obrigatória de borda. O SEPP atua como o único ponto de entrada e saída para a sinalização do plano de controle, protegendo a topologia interna da operadora e gerenciando a criptografia das mensagens transmitidas através da interface N32 (3GPP, 2024c).

A interface N32 implementa o protocolo PRINS (Protocol-specific Application Layer Security), uma inovação crucial que resolve o impasse entre cifragem ponto a ponto e a necessidade de intermediários da rede IPX alterarem determinados cabeçalhos de transporte. Dessa forma, garante-se a integridade e confidencialidade dos dados do usuário, permitindo apenas modificações explicitamente autorizadas por contratos de sinalização.

O objetivo deste artigo é examinar minuciosamente a arquitetura de roaming no 5G SA, analisando as topologias de transporte de dados, o papel do SEPP na interface N32, o esquema criptográfico de privacidade de identidade (SUPI/SUCI), a interoperabilidade multi-vendor e os modelos de governança bilateral. A análise apoia-se estritamente nas especificações oficiais do 3GPP, orientações da GSMA e literatura científica de alto impacto.

2 Metodologia

A condução deste estudo fundamenta-se na revisão analítica e sistemática da literatura técnica, normativa e científica especializada em segurança de redes móveis e arquitetura de telecomunicações. O processo de seleção do corpus documental orientou-se pelo rigor metodológico e pela verificação de autoridade das fontes.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 30/09/2026 | aceito: 03/10/2026 | publicação: 06/10/2026

O primeiro eixo do levantamento abrange as especificações normativas primárias publicadas pelo 3GPP (Release 18). Foram analisados em profundidade os documentos TS 23.501 (arquitetura geral), TS 23.502 (fluxos de procedimentos), TS 29.573 (interconexão de redes PLMN via SEPP) e TS 33.501 (arquitetura e procedimentos de segurança do 5G).

O segundo eixo metodológico engloba as diretrizes e orientações operacionais consolidadas pela associação internacional de operadoras (GSMA). O foco recaiu sobre a norma GSMA NG.113 (5GS Roaming Guidelines), que estabelece os requisitos práticos para a implementação de acordos bilaterais de roaming em redes de quinta geração.

O terceiro eixo contempla relatórios técnicos de avaliação de ameaças e frameworks de cibersegurança emitidos por órgãos governamentais e internacionais, com destaque para as publicações da Agência da União Europeia para a Cibersegurança (ENISA - *5G Threat Landscape*) e do NIST (Cybersecurity Framework 2.0).

O quarto eixo compreende artigos científicos revisados por pares e apresentados em conferências de referência na área de segurança da informação e redes móveis, como o ACM SIGSAC Conference on Computer and Communications Security (CCS) e periódicos da IEEE/Elsevier, selecionados mediante validação direta do DOI.

A síntese das informações foi organizada em uma matriz analítica focada em quatro dimensões operacionais: topologia de plano de usuário, segurança do plano de controle na interface N32, criptografia de privacidade do assinante e requisitos de governança bilateral. O texto final foi totalmente padronizado segundo as diretrizes de redação científica e citações da ABNT.

3 Modelos Arquiteturais do Roaming 5G

O estabelecimento de uma sessão de roaming no 5G SA requer a coordenação precisa entre as funções de controle e transporte localizadas na rede visitada (VPLMN) e na rede de origem do assinante (HPLMN). O 3GPP padroniza dois modelos arquiteturais para o tratamento do tráfego de dados de usuário: Home Routed (HR) e Local Breakout (LBO) (3GPP, 2024a; GSMA, 2024).

No modelo Home Routed (HR), a ancoragem principal do plano de usuário permanece na rede de origem através da H-UPF (Home UPF). Quando o usuário acessa a rede na VPLMN, o tráfego de dados é recebido pela V-UPF local e encapsulado em um túnel GTP-U que atravessa a interface N9 inter-PLMN via rede IPX até atingir a H-UPF no país de origem, de onde o tráfego finalmente é roteado para a Internet (3GPP, 2024a).

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS - Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 30/09/2026 | aceito: 03/10/2026 | publicação: 06/10/2026

Figura 1 – Arquitetura de Interconexão e Segurança de Roaming 5G SA com SEPP

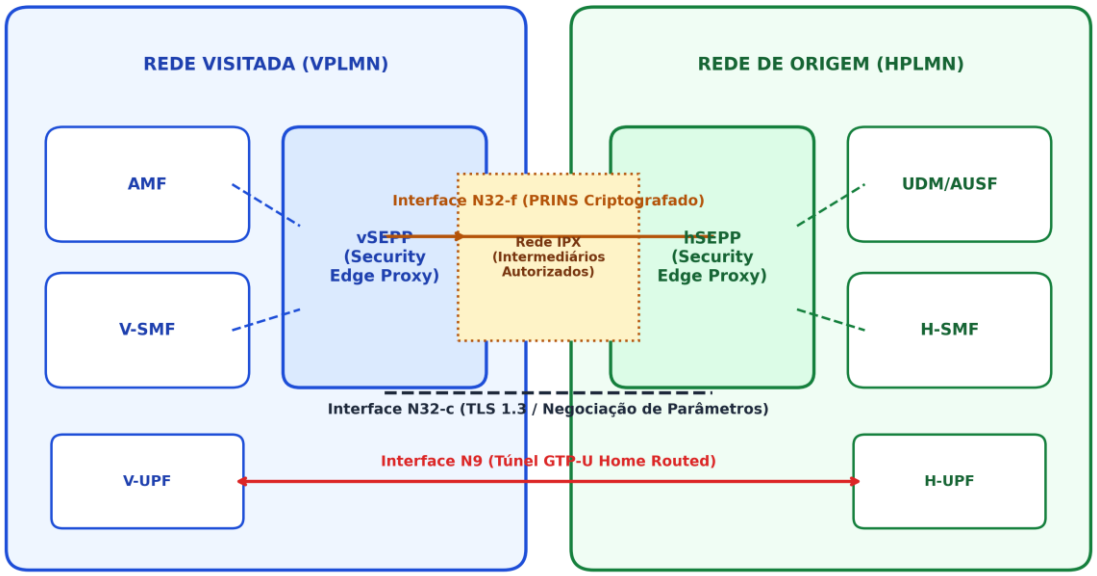

Figura 1 – Arquitetura de Interconexão e Segurança de Roaming 5G SA com SEPP. Fonte: Elaborado com base em 3GPP TS 29.573 (2024).

A arquitetura HR é a escolha amplamente preferida pelas operadoras de telecomunicações para serviços de dados convencionais. A centralização do plano de usuário na HPLMN garante controle absoluto sobre a aplicação de políticas de tarifação em tempo real, auditoria de consumo e cumprimento rigoroso de exigências regulatórias locais de interceptação legal (*lawful interception*), sem depender das políticas do parceiro visitado.

Contudo, a principal desvantagem do modelo Home Routed é a latência adicional introduzida pelo roteamento circular (*tromboning*). O tráfego de dados é forçado a viajar geograficamente até o país de origem e retornar ao destino, o que pode inviabilizar aplicações de tempo real que demandam baixíssima latência (URLLC), como automação industrial avançada e telemedicina (GSMA, 2024).

Para contornar essa limitação, o 3GPP define o modelo Local Breakout (LBO). No LBO, o tráfego de dados da sessão PDU é descarregado diretamente para a rede de dados de destino a partir da V-UPF localizada na VPLMN, eliminando a viagem do tráfego até o país de origem. A HPLMN mantém apenas o controle sobre as regras de política e autorização de sessão via H-PCF e H-SMF (3GPP, 2024a).

Apesar da superioridade técnica em latência, o modelo LBO apresenta grande complexidade operacional e comercial. Ele exige acordos bilaterais de bilhetagem altamente complexos para faturamento cruzado entre operadoras e impõe desafios regulatórios sobre a responsabilidade do tráfego descarregado na rede visitada, razão pela qual sua adoção inicial é restrita a serviços corporativos específicos (GSMA, 2024).

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 30/09/2026 | aceito: 03/10/2026 | publicação: 06/10/2026

4 SEPP, Interface N32 e Segurança da Interconexão

Para eliminar as vulnerabilidades históricas das redes de sinalização SS7 e Diameter, o 3GPP TS 29.573 estabelece o Security Edge Protection Proxy (SEPP) como a função obrigatória de fronteira no 5G SA. Todo e qualquer fluxo de sinalização do plano de controle entre a VPLMN e a HPLMN deve transitar obrigatoriamente através dos SEPPs das duas redes (vSEPP e hSEPP) (3GPP, 2024c; ENISA, 2020).

O SEPP desempenha funções vitais de segurança cibernética na borda inter-PLMN. Ele atua como um firewall de aplicação de sinalização, realizando a ocultação da topologia interna da rede (*topology hiding*), a filtragem de mensagens não autorizadas, o controle de taxa para prevenção de ataques de negação de serviço (DoS) e a validação estrita do formato dos esquemas JSON (3GPP, 2024c).

A interconexão entre o vSEPP e o hSEPP ocorre através da interface N32, que é logicamente subdividida em dois canais operacionais com papéis complementares: a interface N32-c (Control Plane) e a interface N32-f (Forwarding Plane) (3GPP, 2024c).

A interface N32-c é utilizada para a fase inicial de controle. Através dela, os dois SEPPs realizam a autenticação mútua via TLS 1.3 utilizando certificados digitais x.509, negociam as capacidades criptográficas suportadas, trocam chaves de sessão e estabelecem os parâmetros da Associação de Segurança (Security Association - SA) que governará a troca de mensagens de aplicação.

A interface N32-f é dedicada ao transporte efetivo das mensagens de sinalização das NFs internas (como chamadas entre V-SMF e H-SMF ou AMF e UDM). Para proteger essas mensagens enquanto transitam pela rede IPX, a N32-f implementa o protocolo PRINS (Protocol-specific Application Layer Security) (3GPP, 2024c; BASIN et al., 2018).

O protocolo PRINS soluciona de forma elegante o dilema do transporte em roaming. Como provedores de rede IPX intermediários frequentemente precisam modificar determinados cabeçalhos HTTP/2 para roteamento, o PRINS divide a mensagem em blocos: os dados sensíveis do assinante permanecem totalmente cifrados e inacessíveis, enquanto os cabeçalhos modificáveis podem ser alterados por nós autorizados e reassinados criptograficamente, garantindo auditabilidade total (BASIN et al., 2018).

5 Identidade, Autenticação e Privacidade do Assinante

Uma das fragilidades mais severas das redes móveis de segunda, terceira e quarta gerações era a transmissão da identidade permanente do assinante (IMSI) em texto claro sobre o canal de rádio

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 30/09/2026 | aceito: 03/10/2026 | publicação: 06/10/2026

durante os procedimentos iniciais de anexo à rede. Essa limitação facilitou a proliferação de equipamentos maliciosos de interceptação conhecidos como *IMSI Catchers* (Stingrays) (BASIN et al., 2018; ENISA, 2020).

No 5G Standalone, a especificação 3GPP TS 33.501 elimina essa vulnerabilidade ao redefinir a estrutura de identidade do usuário. A identidade permanente do assinante passa a ser denominada SUPI (Subscription Permanent Identifier). A norma proíbe expressamente que o SUPI seja transmitido em texto claro em qualquer interface de rádio (3GPP, 2024d).

Em substituição ao envio direto do SUPI, o cartão SIM/eSIM do terminal do usuário gera uma identidade temporária e cifrada denominada SUCI (Subscription Concealed Identifier). A geração do SUCI apoia-se em um esquema de criptografia de chave pública assimétrica baseado em curvas elípticas (ECIES - Elliptic Curve Integrated Encryption Scheme) (BASIN et al., 2018).

O cartão SIM possui gravada em sua memória segura a chave pública da sua rede de origem (HPLMN). Ao solicitar o acesso à rede visitada (VPLMN), o terminal utiliza a chave pública para cifrar o SUPI, produzindo o SUCI. Como a chave privada correspondente é mantida exclusivamente no interior do UDM da HPLMN, nem a rede de rádio nem o AMF da VPLMN conseguem decifrar a identidade real do usuário.

Ao receber o SUCI enviado pelo terminal, o AMF na VPLMN repassa essa identidade cifrada ao hSEPP da HPLMN através da interface N32. O UDM da HPLMN utiliza sua chave privada para decifrar o SUCI, recupera o SUPI original e inicia o procedimento de autenticação mútua 5G-AKA (ou EAP-AKA') (3GPP, 2024d).

Esse mecanismo garante que a privacidade do assinante permaneça preservada ponta a ponta. Mesmo que a rede de rádio visitada ou a infraestrutura do parceiro de roaming seja comprometida por escuta maliciosa, a identidade permanente do usuário permanece totalmente protegida contra rastreamentos indevidos (BASIN et al., 2018).

6 Interoperabilidade e Sinalização entre Operadores

A viabilização do roaming internacional em redes 5G SA exige a estrita conformidade técnica e semântica entre as funções de rede desenvolvidas por diferentes fornecedores de tecnologia (*multi-vendor*). As chamadas de API trocadas no SBA devem respeitar rigorosamente os schemas OpenAPI 3.0 padronizados pelo 3GPP na série TS 29.500 (3GPP, 2024c; GSMA, 2024).

Em cenários operacionais reais, pequenas divergências na interpretação de parâmetros opcionais nos documentos JSON ou no tratamento de cabeçalhos HTTP/2 específicos podem causar a rejeição de

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 30/09/2026 | aceito: 03/10/2026 | publicação: 06/10/2026

solicitações no SEPP de borda. Isso resulta no encerramento prematuro da tentativa de conexão e na perda de conectividade para o assinante em roaming.

Para mitigar esses riscos de interoperabilidade, a norma GSMA NG.113 estabelece um protocolo detalhado para a realização de testes bilaterais contínuos (*IREG Testing*) antes da liberação comercial de rotas de roaming entre duas operadoras (GSMA, 2024).

Os testes bilaterais englobam a validação sintática e semântica no SEPP, verificando se as regras de *firewall* de sinalização estão configuradas para permitir a passagem das APIs autorizadas sem alterar indevidamente o payload das mensagens cifradas via PRINS.

Outro aspecto crítico é o mapeamento padronizado de códigos de causa de erro (*cause codes*). Quando uma solicitação de sessão PDU falha na HPLMN, o H-SMF deve retornar um código de erro HTTP padronizado (ex: `403 Forbidden` ou `504 Gateway Timeout`) acompanhado do código de causa 5GSM correspondente segundo a TS 24.501, permitindo que o AMF na VPLMN oriente o terminal corretamente (GSMA, 2024).

Por fim, as equipes de engenharia de redes devem realizar o ajuste fino dos temporizadores de reconexão TCP e das chamadas de verificação de integridade (*PING*) do barramento HTTP/2 na interface N32. Essa medida evita que pequenas oscilações de latência na rede IPX provoquem a derrubada em massa de associações de segurança entre os SEPPs (GSMA, 2024).

7 Qualidade, Continuidade e Experiência em Roaming

A experiência percebida pelo usuário em roaming internacional depende diretamente da qualidade técnica mantida em ambas as redes envolvidas (VPLMN e HPLMN) e no segmento de transporte interconectado via IPX. A monitoração contínua dessa experiência exige o acompanhamento de Indicadores de Nível de Serviço (SLIs) altamente específicos (ITU, 2024; GSMA, 2024).

A avaliação da qualidade divide-se entre as métricas do plano de controle e as métricas do plano de usuário. No plano de controle, o principal indicador é a taxa de sucesso nos procedimentos de autenticação 5G-AKA e o tempo de resposta total para o estabelecimento de sessões de dados PDU na topologia Home Routed.

No plano de usuário, as métricas concentram-se na latência de ida e volta (RTT) do túnel GTP-U na interface N9, na taxa de variação do atraso de pacotes (*jitter*) e na porcentagem de perda acidental de pacotes durante a transmissão transfronteiriça.

A identificação de gargalos de desempenho em redes internacionais exige a capacidade de segmentar os dados de observabilidade por parceiro de roaming (identificado pelo PLMN-ID). Uma elevação atípica na latência observada exclusivamente na interface N32 associada a uma determinada

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 30/09/2026 | aceito: 03/10/2026 | publicação: 06/10/2026

operadora parceira indica saturação no SEPP remoto ou degradação na rota da rede IPX contratada (GSMA, 2024).

A utilização de sistemas automatizados de monitoramento de experiência em tempo real permite que a operadora de origem execute a comutação proativa de tráfego (*steering of roaming*). Caso a qualidade de uma VPLMN parceira caia abaixo dos limites aceitáveis de SLO, a HPLMN orienta dinamicamente os terminais de seus assinantes a se conectarem a outra rede parceira disponível na mesma região.

Dessa forma, a integração de métricas de qualidade do plano de controle e do plano de dados assegura a continuidade transparente dos serviços, minimizando interrupções de navegação e garantindo o cumprimento dos acordos de nível de serviço (SLA) comerciais (ITU, 2024).

8 Governança Bilateral, Fraude e Resposta a Incidentes

A operação confiável de acordos de roaming no 5G SA transcende a implantação de soluções puramente tecnológicas. Ela requer uma estrutura organizacional e contratual de governança bilateral altamente disciplinada entre as operadoras parceiras, alinhada aos princípios do NIST Cybersecurity Framework 2.0 e recomendações da GSMA (GSMA, 2024; NIST, 2024).

Os contratos operacionais de roaming devem definir com precisão uma matriz de responsabilidades (RACI) cobrindo todos os pontos de contato técnicos, janelas de manutenção programada e procedimentos padronizados para notificação prévia de alterações de software na borda inter-PLMN.

Um dos pilares da governança técnica é o gerenciamento contínuo do ciclo de vida dos certificados digitais x.509 utilizados para criptografia TLS na interface N32-c e assinatura PRINS na N32-f. A falta de acompanhamento rigoroso dos prazos de expiração de chaves ou falhas na rotação de certificados da PKI podem resultar na interrupção total e imediata do tráfego de roaming entre duas redes.

No âmbito da prevenção de fraudes, a migração para o 5G SA exige novos mecanismos de monitoramento no SEPP. O tráfego de sinalização deve ser continuamente analisado por algoritmos de detecção de anomalias para identificar tentativas de bypass de cobrança, chamadas fantasma ou ataques de exploração de APIs visando o consumo não autorizado de dados.

Adicionalmente, a troca mútua de registros de tarifação e uso deve ocorrer em prazos reduzidos através do formato padronizado SDR (Standard Data Record), permitindo a conciliação rápida do faturamento inter-operadoras e a contenção ágil de incidentes financeiros (GSMA, 2024).

Por fim, a governança exige o estabelecimento de canais de comunicação direta de resposta a incidentes de segurança cibernética (CSIRT). Em caso de comprometimento de chaves privadas ou

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 30/09/2026 | aceito: 03/10/2026 | publicação: 06/10/2026

identificação de padrões de ataque originados na rede parceira, os protocolos de contenção emergencial e isolamento de rotas devem ser acionados com prazos de resposta medidos em minutos (NIST, 2024).

Considerações Finais

A viabilização do roaming internacional em redes 5G Standalone representa uma transição histórica no nível de segurança, privacidade e eficiência oferecido aos usuários em mobilidade global. A substituição definitiva das redes legadas SS7 e Diameter por uma infraestrutura baseada em microsserviços e chamadas de API sob o protocolo HTTP/2 resolve vulnerabilidades estruturais de sinalização que afetavam o setor de telecomunicações há décadas.

Conforme demonstrado nesta pesquisa, a presença obrigatória do Security Edge Protection Proxy (SEPP) na borda inter-PLMN constitui a pedra angular da segurança no 5G SA. Ao atuar como firewall de aplicação e gerenciar o protocolo PRINS na interface N32, o SEPP garante a integridade e confidencialidade das mensagens do plano de controle mesmo diante da presença de intermediários na rede de transporte IPX.

A análise das topologias de plano de usuário evidencia que a arquitetura Home Routed (HR) permanece como a escolha predominante para as operadoras na prestação de serviços de dados convencionais. A capacidade de reter a ancoragem da UPF na HPLMN assegura a auditoria de tarifação e o cumprimento das regulamentações locais sem depender do parceiro visitado.

Por sua vez, o modelo Local Breakout (LBO) consolida-se como uma opção estratégica indispensável para viabilizar serviços de altíssima velocidade e ultra-baixa latência (URLLC). O descarregamento do tráfego diretamente na rede visitada elimina os atrasos inerentes ao roteamento circular, abrindo caminho para aplicações industriais e corporativas transfronteiriças.

No que tange à privacidade do usuário, o avanço proporcionado pelo esquema de criptografia assintótica SUPI/SUCI elimina permanentemente a exposição do identificador do assinante no canal de rádio. O fato de o SUCI ser decifrado exclusivamente pela chave privada mantida no UDM da rede de origem protege os assinantes contra varreduras maliciosas e rastreamento indevido por dispositivos *IMSI Catchers*.

A garantia de interoperabilidade contínua em ambientes compostos por múltiplos fornecedores reforça a importância do cumprimento estrito dos schemas OpenAPI 3.0 e das rotinas de testes bilaterais preconizadas pela GSMA NG.113. O ajuste de temporizadores do barramento HTTP/2 e a padronização dos códigos de causa de erro são indispensáveis para evitar falhas de sinalização intermitentes.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 30/09/2026 | aceito: 03/10/2026 | publicação: 06/10/2026

Em paralelo, a governança operacional e contratual reafirma-se como elemento inseparável da arquitetura de rede. A gestão disciplinada do ciclo de vida de certificados PKI, o monitoramento preventivo de fraudes no SEPP e a coordenação de incidentes cibernéticos em tempo real são as condições que asseguram a estabilidade das parcerias internacionais.

Em conclusão, o sucesso do roaming no 5G SA depende da construção de uma cadeia de confiança técnica e institucional ponta a ponto. A integração harmoniosa entre os mecanismos de criptografia na borda, a observabilidade segmentada por parceiro e a governança bilateral contínua é o que garante a entrega de uma experiência de conectividade internacional verdadeiramente robusta, segura e resiliente.

Referências

3GPP. TS 23.501: System architecture for the 5G System; Stage 2 (Release 18). Sophia Antipolis: 3GPP, 2024a. Disponível em: https://www.3gpp.org/dynareport/23501.htm.

3GPP. TS 23.502: Procedures for the 5G System; Stage 2 (Release 18). Sophia Antipolis: 3GPP, 2024b. Disponível em: https://www.3gpp.org/dynareport/23502.htm.

3GPP. TS 29.573: Public Land Mobile Network (PLMN) interconnection; Stage 3 (Release 18). Sophia Antipolis: 3GPP, 2024c. Disponível em: https://www.3gpp.org/dynareport/29573.htm.

3GPP. TS 33.501: Security architecture and procedures for 5G System (Release 18). Sophia Antipolis: 3GPP, 2024d. Disponível em: https://www.3gpp.org/dynareport/23501.htm.

BASIN, D. et al. A formal analysis of 5G authentication. In: PROCEEDINGS OF THE 2018 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY (CCS '18), 2018, Toronto. Anais [...]. New York: ACM, 2018. p. 1383-1396. DOI: https://doi.org/10.1145/3243734.3243846.

ENISA. ENISA threat landscape for 5G networks. Athens: European Union Agency for Cybersecurity, 2020. DOI: https://doi.org/10.2824/49299.

GSMA. NG.113: 5GS roaming guidelines. Version 10.0. London: GSMA, 2024. Disponível em: https://www.gsma.com/newsroom/wp-content/uploads/NG.113-v10.0.pdf. Acesso em: 10 set. 2026.

ITU. Measuring digital development: Facts and Figures 2024. Geneva: International Telecommunication Union, 2024. Disponível em: https://www.itu.int/itu-d/reports/statistics/facts-figures-2024/.

NIST. Cybersecurity Framework 2.0. Gaithersburg: NIST, 2024. DOI: https://doi.org/10.6028/NIST.CSWP.29.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.