
aptel
snt
XXII 2026


Prêmio APTEL Inovar
XXII
SNT 2026
aptel
snt
aptel

Autenticação de Usuários em Redes 5G Privadas para Comunicações de Missão Crítica

Defesa como Infraestrutura Crítica: abordagem *Zero Trust* para o *post-attach*

Capitão-Tenente (EN) Fernando J. de Oliveira

Marinha do Brasil

Prêmio Inovar APTEL 2026 | XXII SNT

Este projeto é parte de um trabalho desenvolvido durante o curso de Mestrado na Naval Postgradute School
Orientador da Instituição: Joffrey Xie
Orientador Técnico da MB: Capitão de Corveta (T) BRAGA



Sumário

1. OBJETIVO DO PROJETO
2. PROBLEMA A SER RESOLVIDO
3. DESCRIÇÃO DO PROJETO
4. DESAFIOS
5. SOLUÇÕES APLICADAS
6. RESULTADOS
7. BENEFÍCIOS E IMPACTOS
8. APLICABILIDADE
9. PROXIMOS PASSOS
10. AGRADECIMENTOS E PERGUNTAS



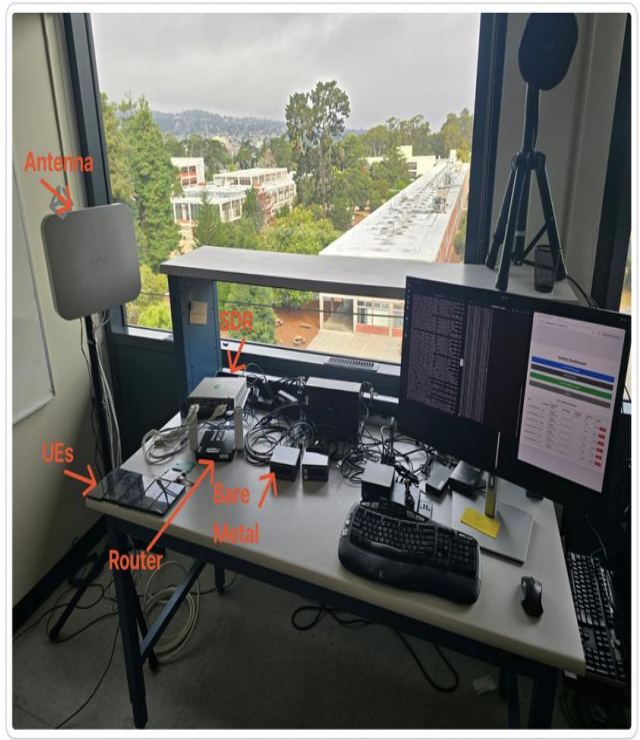
1. OBJETIVO DO PROJETO

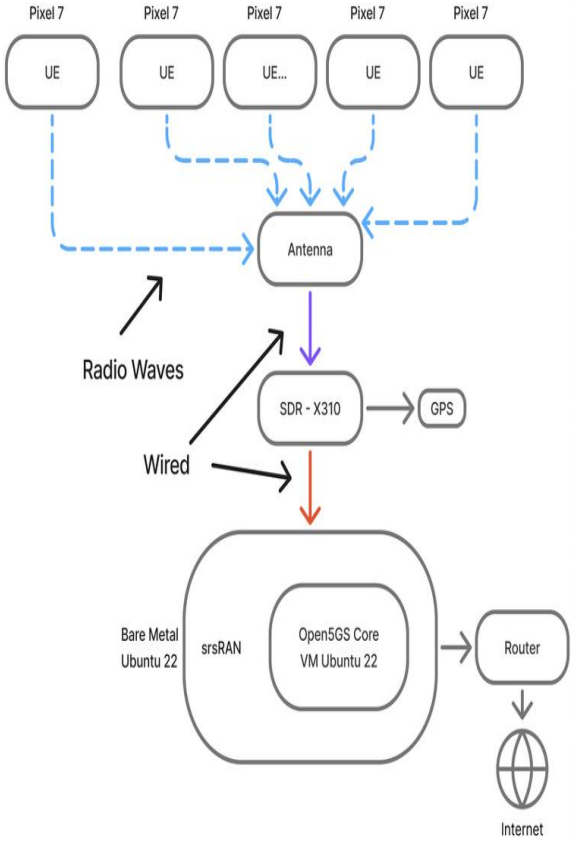
Fechar o gap *post-attach* sem alterar o 5G Core

Objetivo central

- Validar o usuário humano após o *attach 5G-AKA*, não apenas o dispositivo.
- Aplicar *Zero Trust* no plano de usuário com política por missão (*User Group Aceess* - UGA).
- Preservar interoperabilidade com solução agentless alinhada ao padrão 3GPP.

Open5Gs/srsRAN Tested



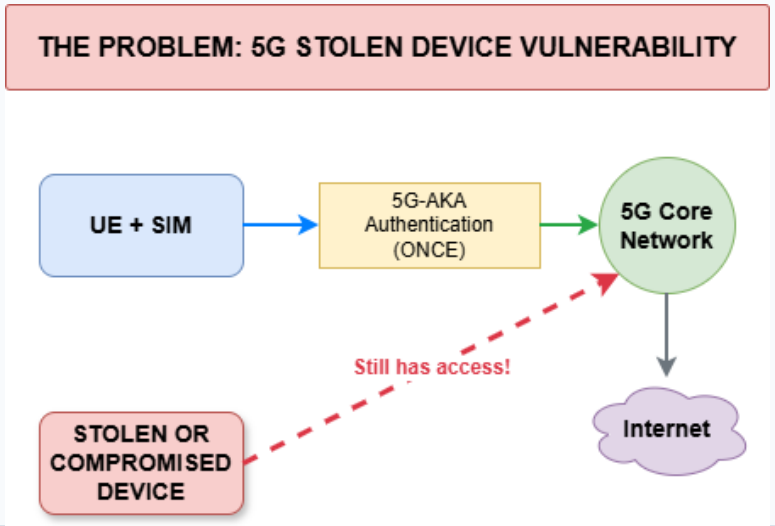


2. PROBLEMA

Por que isso é crítico para defesa e infraestrutura nacional

Risco atual

- Dispositivo comprometido pode manter sessão ativa sem revalidação humana.
- Acesso excessivo amplia impacto sobre Comando e Controle.
- Ambientes de missão exigem revogação rápida e granular.



Conexão com o XXII

SNT 2026 e para a Marinha do Brasil

- Comunicações de defesa são infraestrutura crítica do futuro.
- O problema combina segurança cibernética, continuidade operacional e soberania digital.
- A solução reduz risco sem ruptura da base instalada.
- Abre portas ao desenvolvimento de tecnologia própria .

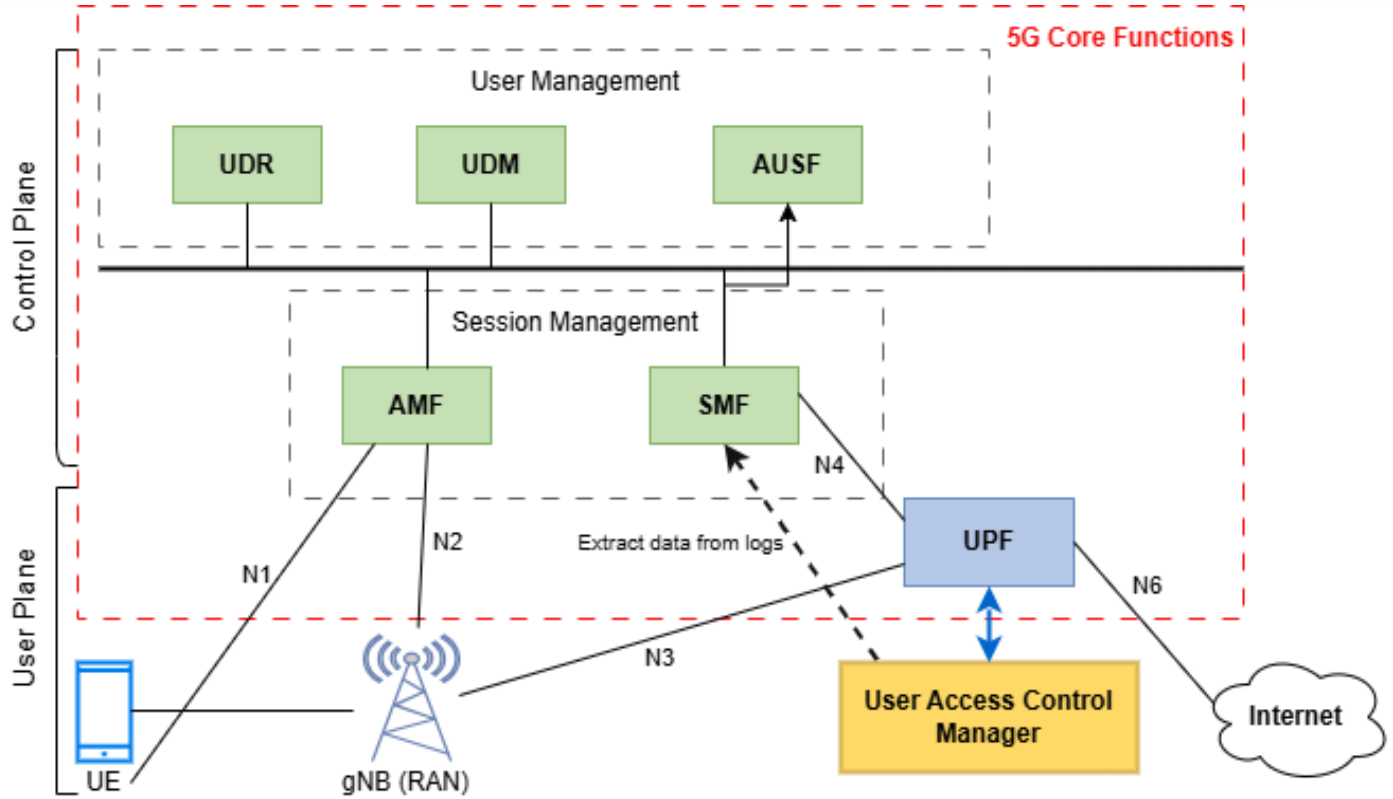
Conexão com o SNT 2026

2021: incidentes relevantes expuseram fragilidades na proteção de informações e comunicações sensíveis.

2024: Governo Federal avançou com a iniciativa de uma Rede Móvel Privativa Federal 4G (segurança e interoperabilidade).

3. DESCRIÇÃO DO PROJETO

Arquitetura UAEM em uma frase: bloquear, autenticar, liberar



Como funciona

- 1) UPF inicia em Default-Deny.
- 2) Portal web autentica o operador.
- 3) Grant assinado libera apenas o escopo da missão.
- 4) Expiração por TTL retorna ao bloqueio.

$$\text{Grant} = \text{HMAC}_K(\text{IP} \,\|\, \text{IMSI} \,\|\, \text{OpID} \,\|\, \text{UGA} \,\|\, T_{\text{exp}} \,\|\, \text{Nonce})$$

4. DESAFIOS

Quatro desafios para tornar a solução viável

Sem lock-in

- Desacoplar do controle do 5G Core.
- Evitar customização proprietária.

Tempo de missão

- Reconfigurar sem derrubar sessão PDU.
- Atualizar política em segundos.

Heterogeneidade

- Suportar múltiplos autenticadores.
- Operar com terminais COTS.

Performance

- Fiscalizar sem degradar throughput.
- Sobrecarga mínima na UPF.



5. SOLUÇÕES APLICADAS

Dashboard operacional: políticas e sessões por grupo

+ Add New Group

GROUP NAME	SECURITY TIER	DL/UL RATE	ACCESS MODE	SESSION LEASE	ACTIONS
Strategic	SSG-1	100 Mbps / 60 Mbps	WebAuthn only	60 min	Edit Delete
Tactical	SSG-2	100 Mbps / 60 Mbps	WebAuthn preferred / TOTP	60 min	Edit Delete
Confidential	SSG-3	80 Mbps / 40 Mbps	User + Password + WebAuthn	60 min	Edit Delete
Operational	SSG-4	80 Mbps / 40 Mbps	User + Password + TOTP	60 min	Edit Delete
Public-Provisional	SSG-5	50 Mbps / 20 Mbps	Express token (6-digit code)	60 min	Edit Delete

← Back

Home



5. SOLUÇÕES APLICADAS

Evidência real: fluxo de autenticação no telefone

Fluxo

- Credencial da missão -> autenticação humana -> liberação temporária por perfil (UGA).



PIN Access



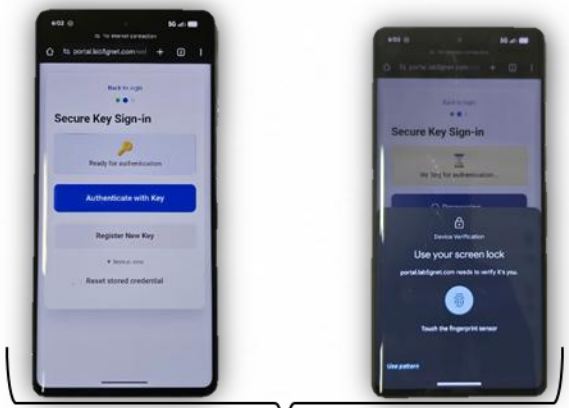
Voucher



Password



TOTP



WebAuthn

CAC



Evidência : Dashboard do Operador do Sistema

USER AUTHORIZATION AND ENFORCEMENT MANAGER

Admin Dashboard

Monitor subscriber readiness, policy tiers, and real-time attachment status.

+ Add Subscriber | + eSIM | + Bulk | Network Groups | Logout

Subscriber Status

Search by username, IMSI, or keyword...

All UGA Tiers | All Device Status | All Auth Status

Clear

user1
IMSI 001010000143841
GROUP: Command and Control - C2
UGA-1
AUTHENTICATION: WebAuthn + TOTP
WebAuthn + TOTP ready
DEVICE: Attached
AUTH STATUS: Authenticated
SESSION
10.45.0.5
Attached: 4m 10s
Auth: 3m 59s
TTL COUNTDOWN
23h 55m
Remaining
Edit | Revoke | Delete

user2
IMSI 001010000143842
GROUP: Tactical
UGA-2
AUTHENTICATION: WebAuthn only
WebAuthn ready
DEVICE: Attached
AUTH STATUS: Authenticated
SESSION
10.45.0.6
Attached: 3m 39s
Auth: 2m 38s
TTL COUNTDOWN
7h 57m
Remaining
Edit | Revoke | Delete

user3
IMSI 001010000143843
GROUP: Confidential
UGA-3
AUTHENTICATION: User + Password + WebAuthn
Password + WebAuthn ready
DEVICE: Attached
AUTH STATUS: Authenticated
SESSION
10.45.0.7
Attached: 3m 15s
Auth: 1m 40s
TTL COUNTDOWN
3h 58m
Remaining
Edit | Revoke | Delete

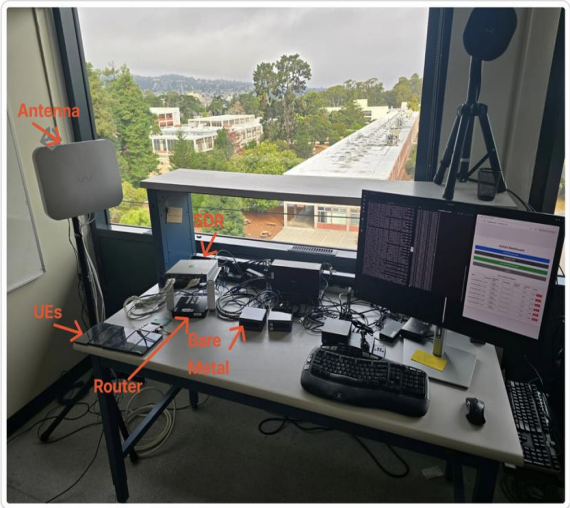


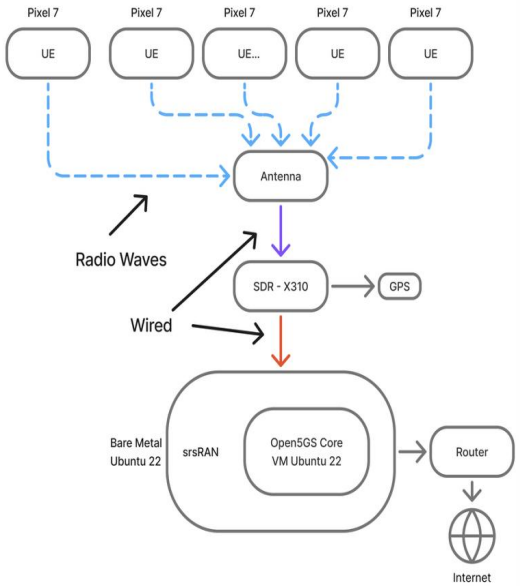
6. RESULTADOS

Eficácia defensiva validada em bancada 5G SA

100%
SP1-SP4 bloqueados

280/280
Políticas corretas

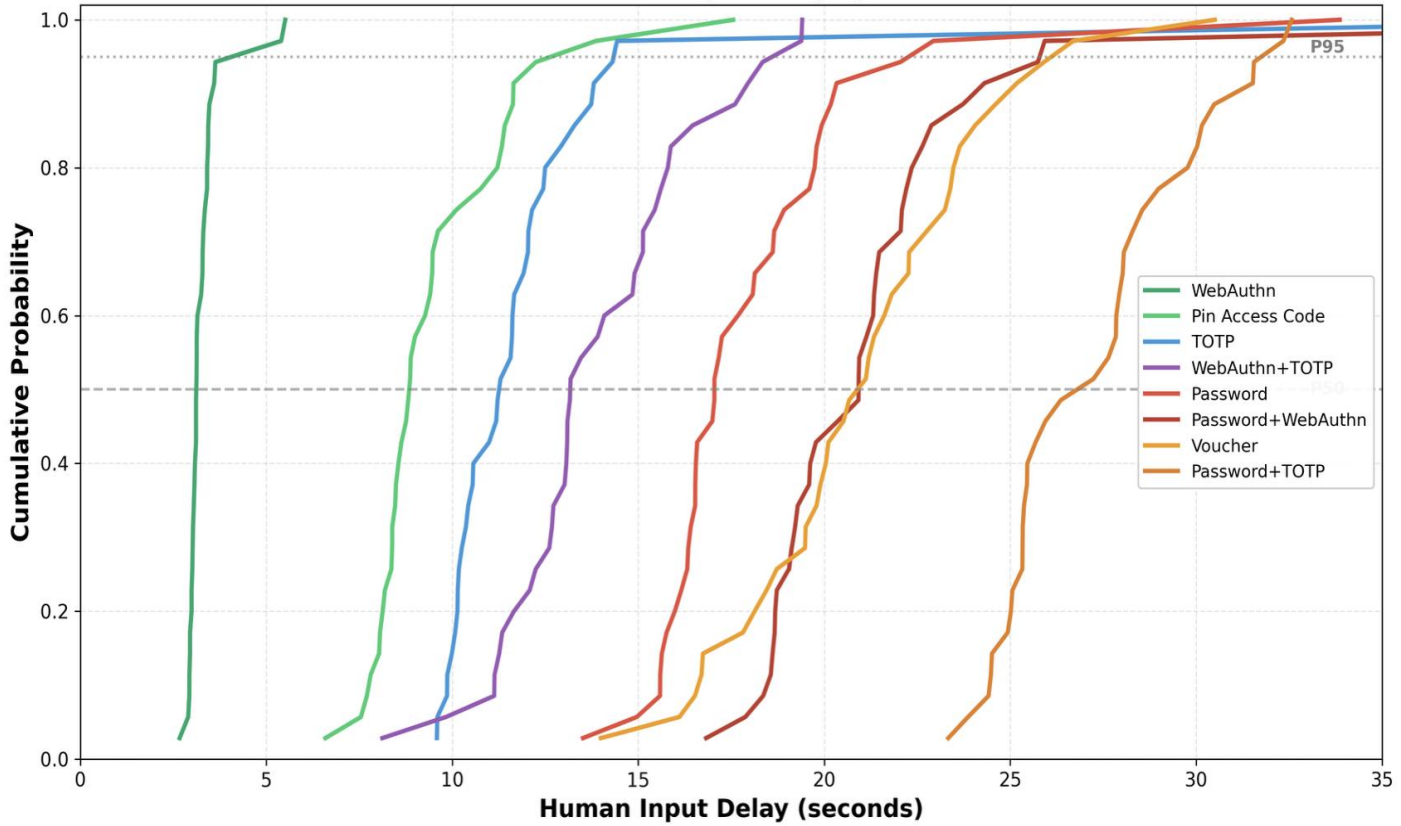




Evidências principais

- SP1: sem tráfego antes da autenticação humana.
- SP2: concessão só quando regra do grupo é satisfeita.
- SP3: expiração automática de acesso por tempo.
- SP4: isolamento entre fatias e DNNs não autorizadas.

Desempenho operacional no tempo de autenticação



High Security Applications

WebAuthn+TOTP

Best security (AAL2)
Reasonable speed

HID: 13.2s

Speed-Critical Applications

WebAuthn

Fastest method
Still AAL2 secure

HID: 3.6s

Guest/Temporary Access

Pin Access Code

Simple & fast
No account needed

HID: 8.9s



7. BENEFÍCIOS E IMPACTOS

Valor direto para o ecossistema de Telecomunicações

Segurança

- Reduz superfície de ataque *post-attach*.
- Limita movimento lateral.
- Alinha com Zero Trust.

Operação

- Mudança de perfil sem reiniciar rede.
- Gestão por missão em tempo real.
- Compatível com Commercial *Off-The-Shelf* (COTS).

Estratégia

- Soberania tecnológica.
- Escalável para múltiplos setores.
- Base para transição dual uso civil-militar.



8. APLICABILIDADE

Onde a ideia pode ser aplicada?

Algumas da Possíveis Aplicações

- Energia e óleo/gás: operação remota com controle de identidade forte.
- Portos e logística: acesso temporário para equipes terceirizadas.
- Defesa e segurança pública: continuidade de C2 em ambientes contestados.

Métricas e Implementação

- Métrica de risco e latência antes/depois.
- Sem troca do core existente.

Expansão

- Plano de expansão multi-site.
- Roadmap integração com diferentes Core 5G



9. PRÓXIMOS PASSOS

Roadmap Técnico e Institucional

Fase 1

- Ajustes do projeto ao foco ou missão específica.
- Implementação com equipamentos robustos e de mercado.
- Medir Métricas de segurança e usabilidade.

Fase 2

- Integração com IdP corporativo.
- Ampliação de métodos AAL3.
- Validação de handover inter-gNB sem perder a sessão

Fase 3

- Escala multi-planta e multi-site.
- Transferência tecnológica nacional.
- Trilha de padronização setorial.



AGRADECIMENTOS

- MARINHA DO BRASIL
- NAVAL POSTGRADUATE SCHOOL
- APTEL E PETROBRAS

PERGUNTAS?



