STIR/SHAKEN EM SIP

Autenticação e verificação
AS / VS · interconexão e intrarrede

A1–A7 · V1–V7 · API · SIP · RCD · políticas de bloqueio



Whitepaper técnico-comercial · versão 1.4 · 14/10/2026

Whitepaper técnico-comercial — versão 1.4 ZICTEC | 14 de outubro de 2026 Público: operadoras, prestadoras de voz, equipes de engenharia, tecnologia, regulação e compras.

AS e VS são duas metades de uma mesma arquitetura de confiança: o AS autentica a originação; o VS verifica o que chega e entrega evidência para uma política explícita de completar, sinalizar ou rejeitar a chamada.

Resumo executivo

A versão 1.0 descreveu sete formas A1–A7 de disponibilizar o **Authentication Service (AS)**. Esta revisão preserva esses cenários e acrescenta seus equivalentes **V1–V7 para o Verification Service (VS)**, bem como operação **AS/VS intrarrede (on-net)** pela API ZICTEC em uma chamada `samestep` ou em duas operações independentes.

O mesmo ponto SIP — ProSBC dedicado, SBC de interconexão ou SIP AS/VS SERVICE Cloud ZICTEC — pode integrar autenticação e verificação por API, SIP in-band, resposta de decisão ou consulta out-of-band. A diferença essencial está no resultado:

- o **AS** produz a identidade autenticada correspondente à requisição de saída;
- o **VS** verifica `Identity`/PASSporT, credenciais, temporalidade, autoridade e perfis aplicáveis;
- o **policy engine** decide completar, sinalizar, adaptar para legado ou bloquear;
- o **RCD** pode trazer nome, motivo e imagem validados quando a origem aderiu à Origem Verificada e a rede/terminal suportam sua apresentação.

Uma falha de autenticação e uma falha técnica não são a mesma coisa. Em especial, uma chamada reprovada por política **não deve prosseguir por rota de failover**; o failover serve à indisponibilidade do serviço de consulta, conforme política homologada. A decisão ocorre no SBC/softswitch mesmo quando o terminal STFC, analógico, TDM, 2G/3G ou legado não consegue exibir os dados enriquecidos.

No Brasil, o RGST prevê implantação abrangente de autenticação, com transição e possíveis exceções. Cautelares específicas disciplinam grandes chamadores, chamadas abusivas e tráfego irregular. Isso não equivale a um comando universal e imediato para descartar toda chamada sem `Identity`, nem torna RCD obrigatório para todas as chamadas. Cada política de bloqueio deve ser rastreável à regra aplicável e às salvaguardas de exceção e contestação.

1. Quatro camadas que não devem ser confundidas

Identidade autenticada — STIR/SHAKEN

O cabeçalho SIP `Identity` carrega um PASSporT assinado. O **AS** assina; o **VS** verifica. Atestação e assinatura não comprovam consentimento de marketing, conteúdo da conversa ou reputação positiva.

Autorização e política de chamadas

A verificação produz fatos técnicos. A decisão de permitir, sinalizar, desviar ou rejeitar é uma camada separada, capaz de combinar regulação, perfil do cliente, exceções, DNO, reputação e listas estáticas/dinâmicas.

Origem Verificada e RCD

RCD pode incluir:

- nome em `rcd.nam`;
- imagem/logomarca por `rcd.icn` ou jCard;
- motivo da chamada no claim `crn`, fora do objeto `rcd`;
- mecanismos de integridade para conteúdo referenciado.

Nome tende a ser aproveitável por mais terminais; motivo e imagem dependem mais fortemente de perfil, rede, sistema operacional e aparelho compatíveis. Ausência de exibição não elimina a verificação na rede.

Antispam e checagens complementares

A API ZICTEC pode, conforme contratação, agregar checagens de DNO, numeração impossível/não atribuída, blacklist estática e dinâmica, reputação, consentimento/opt-out e consistência. Essas funções não substituem AS/VS e não devem ser tratadas como uma única “lista de fraude”.

2. Componentes e fronteiras de responsabilidade

- **OSP / origem:** rede que inicia a chamada e apresenta a identidade declarada.
- **AS — Authentication Service:** produz o PASSporT e a assinatura para a requisição de saída.
- **VS — Verification Service:** valida a identidade recebida e retorna um resultado estruturado.
- **SBC de interconexão:** preserva ou reconstrói corretamente os elementos protegidos, aplica política e faz interworking.
- **Softswitch:** correlaciona chamadas, interpreta resultados, seleciona rota e impede bypass por failover quando há reprovação.
- **SIP AS/VS SERVICE Cloud ZICTEC:** ponto SIP gerenciado para decisão e integração sem exigir suporte nativo no SBC legado.
- **API ZICTEC/STFC Tools:** orquestração, auditoria, relatórios e políticas opcionais.
- **Fornecedor/ecossistema autorizado:** função tecnológica aplicável — por exemplo, Neustar/TransUnion — sujeita a contrato, credenciais e homologação.

Um B2BUA que altera origem, destino, `iat` ou outra informação protegida não deve copiar cegamente um `Identity` antigo. A perna de saída precisa de identidade correspondente ao novo pedido.

3. Arquiteturas de integração

Arquitetura A — ProSBC dedicado com módulo protegido em memória

O módulo proprietário ZICTEC é carregado em runtime no ProSBC do cliente. Pode consultar diretamente o serviço autorizado ou consumir a API ZICTEC, aplicar AS, VS e políticas no ponto de roteamento, sem expor código-fonte. É adequado a alto volume, controle local e aproveitamento de infraestrutura já amortizada.

Arquitetura B — API direta

SBCs e softswitches modernos podem consumir a API oficial para autenticar, verificar ou executar AS+VS `samestep`. Operações separadas continuam disponíveis quando a arquitetura exige evidências, latências ou políticas distintas.

Arquitetura C — SIP 302 para entrega de dados

No modelo AS, o serviço pode devolver `302` com `Identity` e `Date` em integração homologada; a origem escolhe o destino e gera seu novo `INVITE`. No modelo VS, `302` só deve ser usado como envelope contratual de decisão quando o UAC/SBC conseguir distinguir claramente aprovação, reprovação e falha técnica. Não confundir esse uso homologado com semântica universal do SIP.

Arquitetura D — OOB por resposta SIP e failover controlado

Uma tentativa de consulta chega ao iSBC Cloud e recebe códigos distintos:

- **sucesso da consulta:** o softswitch prossegue para a rota real e aplica o resultado recebido;
- **reprovação/bloqueio:** a chamada é rejeitada e não avança para outra rota;
- **erro técnico/timeout:** aplica-se a contingência homologada, que pode incluir outra instância, API, fail-open limitado ou fail-closed.

Os códigos de controle desta integração precisam ser reservados, documentados e não ambíguos. Códigos STIR/SHAKEN padronizados permanecem destinados às condições definidas pela RFC 8224.

Arquitetura E — SIP AS/VS SERVICE Cloud ZICTEC

Para SBCs legados, a consulta ocorre em SIP diretamente contra a nuvem ZICTEC. O cliente não precisa implementar a API nem suportar nativamente todo o conjunto de códigos e claims. A plataforma pode atuar apenas como plano de decisão/OOB ou permanecer no caminho SIP, conforme o contrato.

4. Códigos SIP e tradução para redes legadas

Código/resultado	Significado técnico	Tratamento recomendado no SBC/softswitch	Compatibilidade legado
`428 Use Identity Header`	Política exige identidade suportada, mas ela não foi recebida	Rejeitar ou aplicar regra de transição explicitamente definida; não rotular automaticamente como fraude	Traduzir para código legado homologado, preservando internamente o motivo 428
`436 Bad Identity Info`	VS não conseguiu obter as credenciais necessárias	Distinguir falha de aquisição/infraestrutura; tentar fonte alternativa quando aplicável	Pode mapear para indisponibilidade temporária, sem perder a causa original
`437 Unsupported Credential`	Credencial obtida, porém não aceita/suportada	Bloquear ou tratar conforme trust store e política; não confundir com reputação	Mapear para rejeição compatível e registrar causa 437
`438 Invalid Identity Header`	Nenhum Identity válido e suportado foi verificado	Rejeitar quando a política local assim determinar; considerar a única repetição permitida para PASSporT completo no caso previsto	Mapear para rejeição legada, sem permitir bypass por rota alternativa
`607 Unwanted`	O próprio destinatário indica comunicação indesejada	Usar como feedback do usuário; evitar banimento global sem identidade autenticada e controles contra falso positivo	Converter em evento de feedback e resposta compatível
`608 Rejected`	Intermediário rejeita a comunicação como indesejada em nome do usuário	Rejeição global; incluir informação de remediação quando exigida e segura	Elemento de rede deve oferecer mecanismo compatível de anúncio/remediação ao originador legado
`verified/pass`	Identidade verificada e política permite	Completar a chamada e disponibilizar dados verificados aos elementos seguintes	Entregar número/nome suportado; motivo/logo podem não aparecer
`failed/block`	Falha criptográfica, de autoridade ou política que exige bloqueio	Encerrar a chamada; nunca tratar como “próxima rota”	Código tradicional configurado, anúncio ou causa PSTN, mantendo trilha auditável
`unavailable/error`	Timeout ou indisponibilidade técnica da consulta	Aplicar contingência separada, com limites e alarmes	Failover técnico permitido apenas nesta classe, conforme política

Os códigos `428`, `436`, `437` e `438` descrevem falhas de identidade. `607` é feedback do destinatário; `608` é rejeição por intermediário. Não se deve mapear blacklist, DNO ou falta de consentimento genericamente para `438`, nem usar `607` como resultado automático do motor antispam.

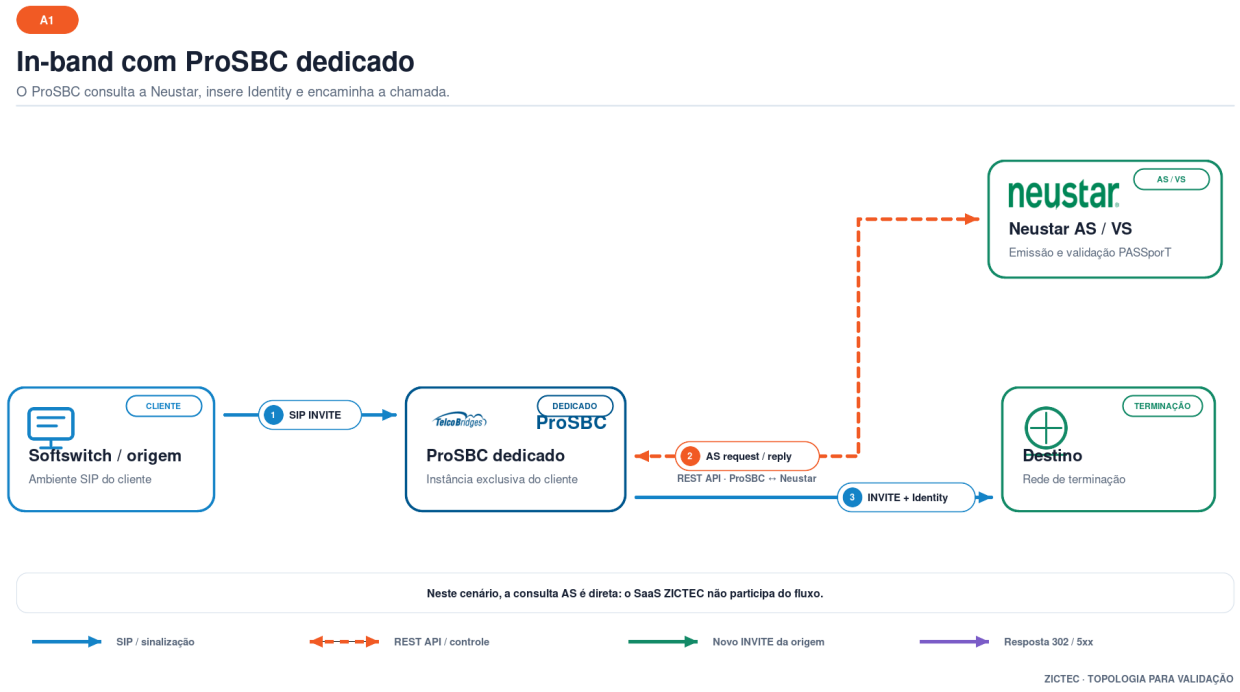
5. Sete cenários de Authentication Service — A1–A7

Os cenários A permanecem válidos. A função AS autentica a originação e devolve o `Identity` correspondente à perna de saída.

Cenário	Ponto de entrada	Consulta AS	Entrega/continuidade
A1 — In-band dedicado padrão	ProSBC dedicado	AS autorizado direto	`INVITE` de saída com `Identity`
A2 — Dedicado com policer	ProSBC dedicado	Políticas ZICTEC e AS direto	`INVITE` autenticado após checagens
A3 — Dedicado com SaaS	ProSBC dedicado	Orquestração API ZICTEC	`INVITE` autenticado

Cenário	Ponto de entrada	Consulta AS	Entrega/continuidade
A4 — 302 dedicado	ProSBC dedicado	AS autorizado	`302` com `Identity`/`Date`; novo `INVITE` pela origem
A5 — OOB dedicado	ProSBC dedicado	AS autorizado	Resposta SIP de controle; origem avança à rota real
A6 — 302 Cloud	SIP AS SERVICE ZICTEC	AS autorizado via nuvem	`302` homologado; chamada final fora da plataforma
A7 — OOB Cloud	SIP AS SERVICE ZICTEC	AS autorizado via nuvem	Resultado por SIP; rota final controlada pela origem

A1 — In-band dedicado padrão



Topologia técnica — cenário A1. Fluxos, componentes e integrações do cenário.

Origem → ProSBC dedicado → AS autorizado → destino. A identidade é produzida para o `INVITE` de saída.

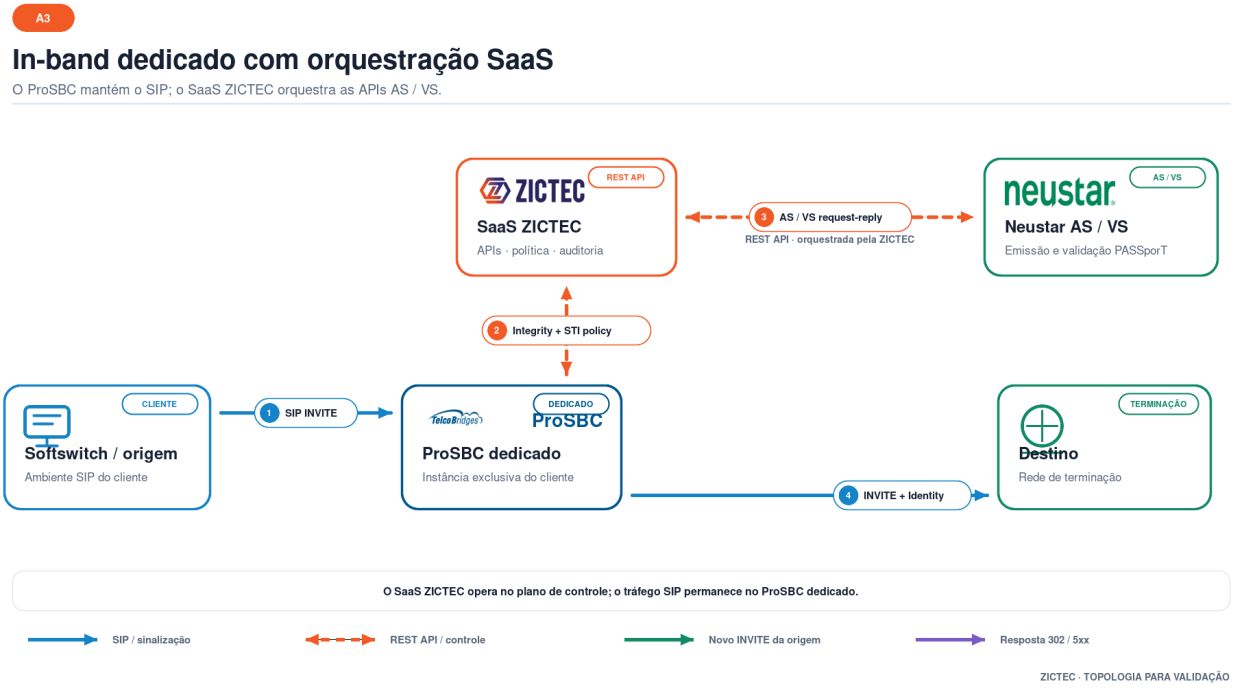
A2 — In-band dedicado com policer/auditoria



Topologia técnica — cenário A2. Fluxos, componentes e integrações do cenário.

Antes da assinatura, a camada ZICTEC executa as verificações contratadas. O AS autorizado continua responsável pelo PASSporT.

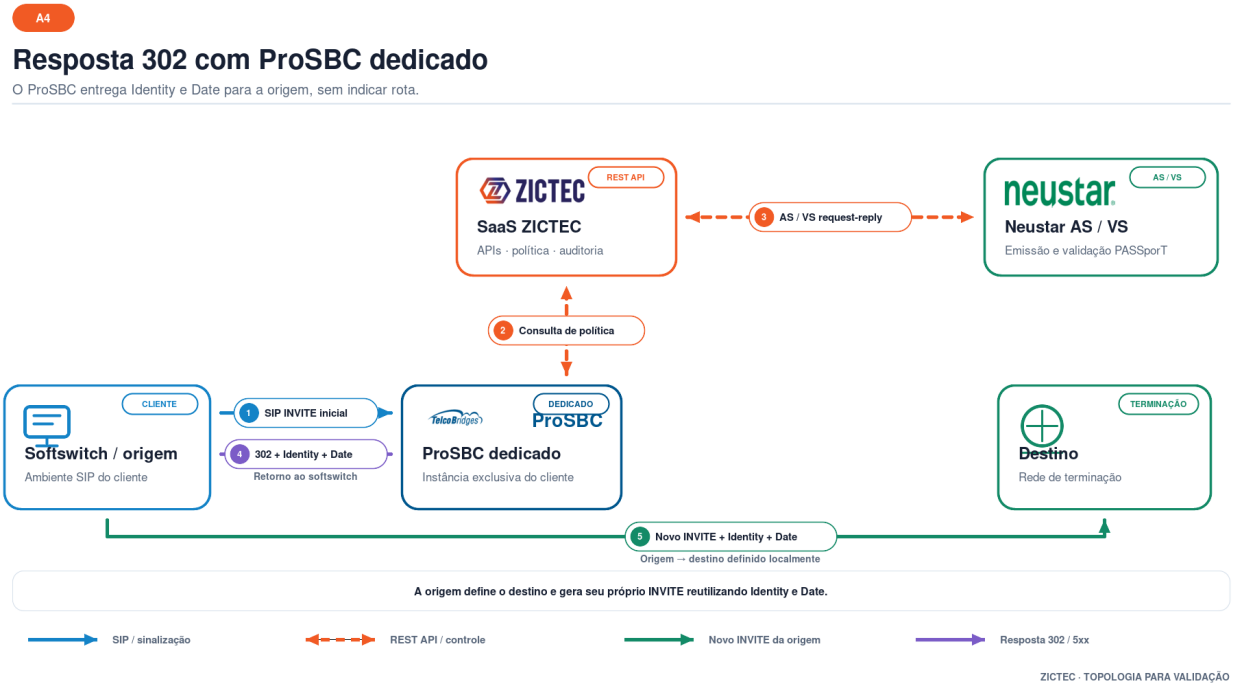
A3 — In-band dedicado com orquestração SaaS



Topologia técnica — cenário A3. Fluxos, componentes e integrações do cenário.

O ProSBC permanece no caminho da chamada e usa a API ZICTEC para políticas e integração com o AS.

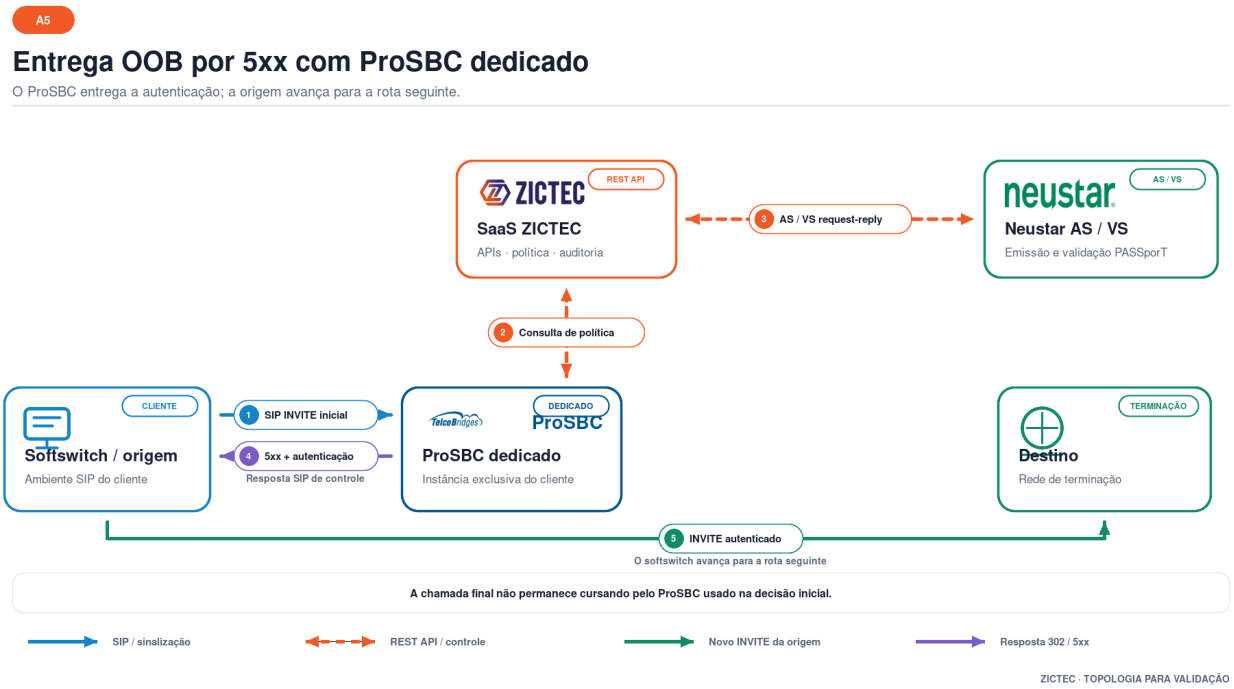
A4 — Resposta 302 pelo ProSBC dedicado



Topologia técnica — cenário A4. Fluxos, componentes e integrações do cenário.

O ProSBC devolve `302` com `Identity` e `Date`; a origem seleciona o destino e cria o novo `INVITE` conforme homologação.

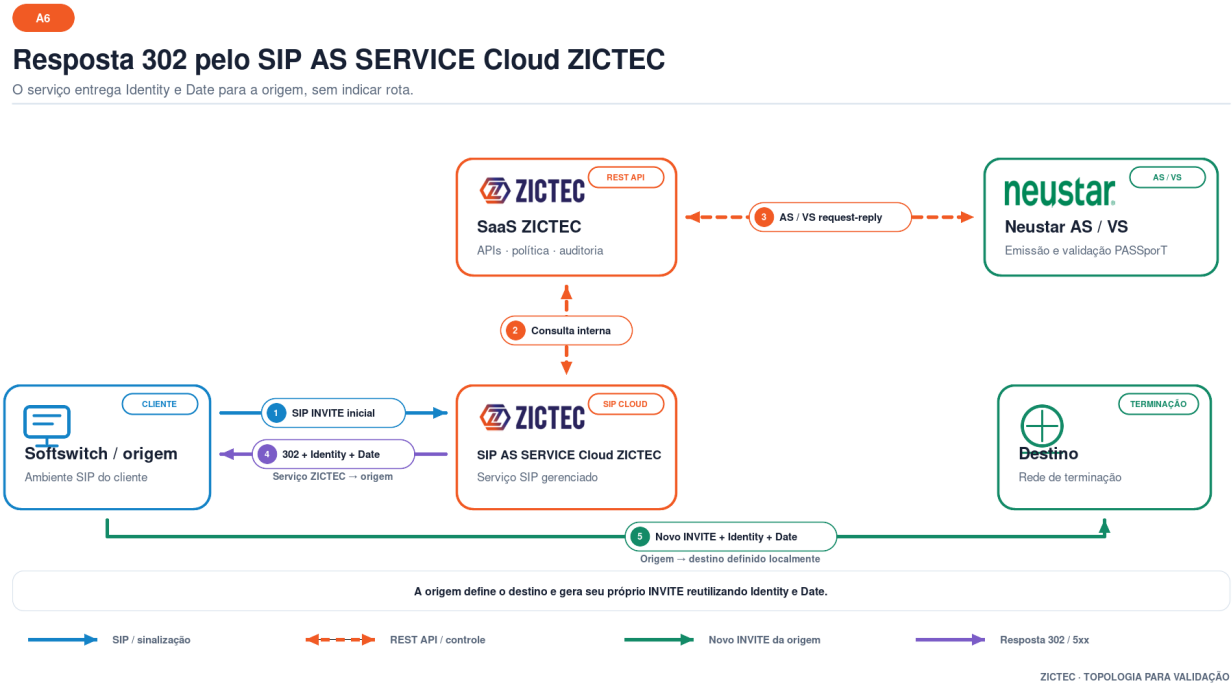
A5 — Entrega OOB pelo ProSBC dedicado



Topologia técnica — cenário A5. Fluxos, componentes e integrações do cenário.

A primeira tentativa é de decisão. A resposta SIP carrega o resultado; a origem só avança à rota real quando a autenticação foi bem-sucedida.

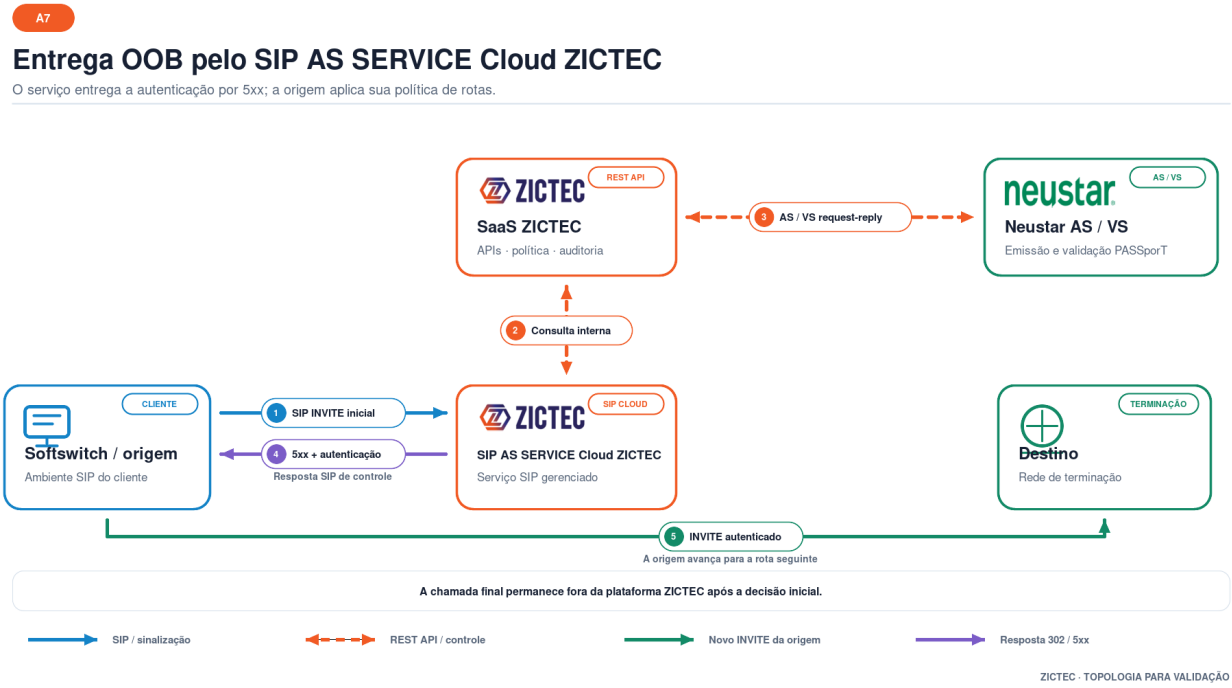
A6 — Resposta 302 pelo SIP AS SERVICE Cloud ZICTEC



Topologia técnica — cenário A6. Fluxos, componentes e integrações do cenário.

A primeira tentativa vai à nuvem ZICTEC; o resultado de AS volta em `302` homologado, sem manter a chamada final no serviço.

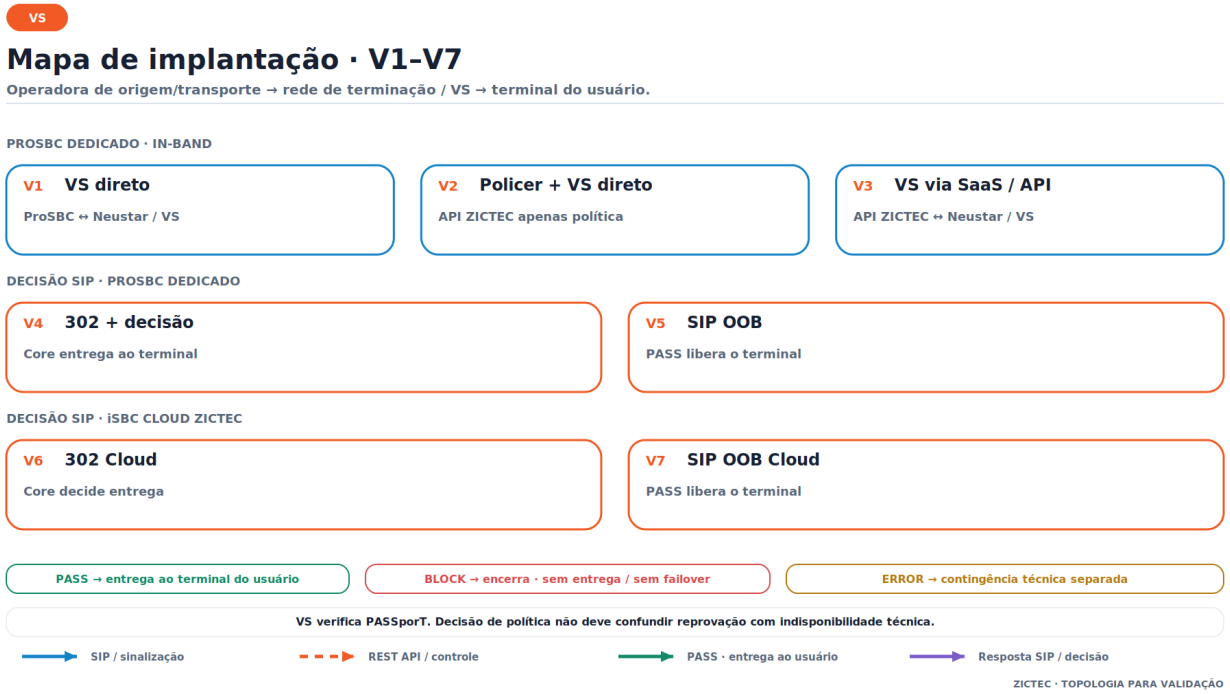
A7 — Entrega OOB pelo SIP AS SERVICE Cloud ZICTEC



Topologia técnica — cenário A7. Fluxos, componentes e integrações do cenário.

A nuvem recebe uma tentativa de consulta e devolve sucesso, falha ou indisponibilidade por códigos distintos. Apenas sucesso autoriza a rota real.

6. Sete cenários de Verification Service — V1–V7

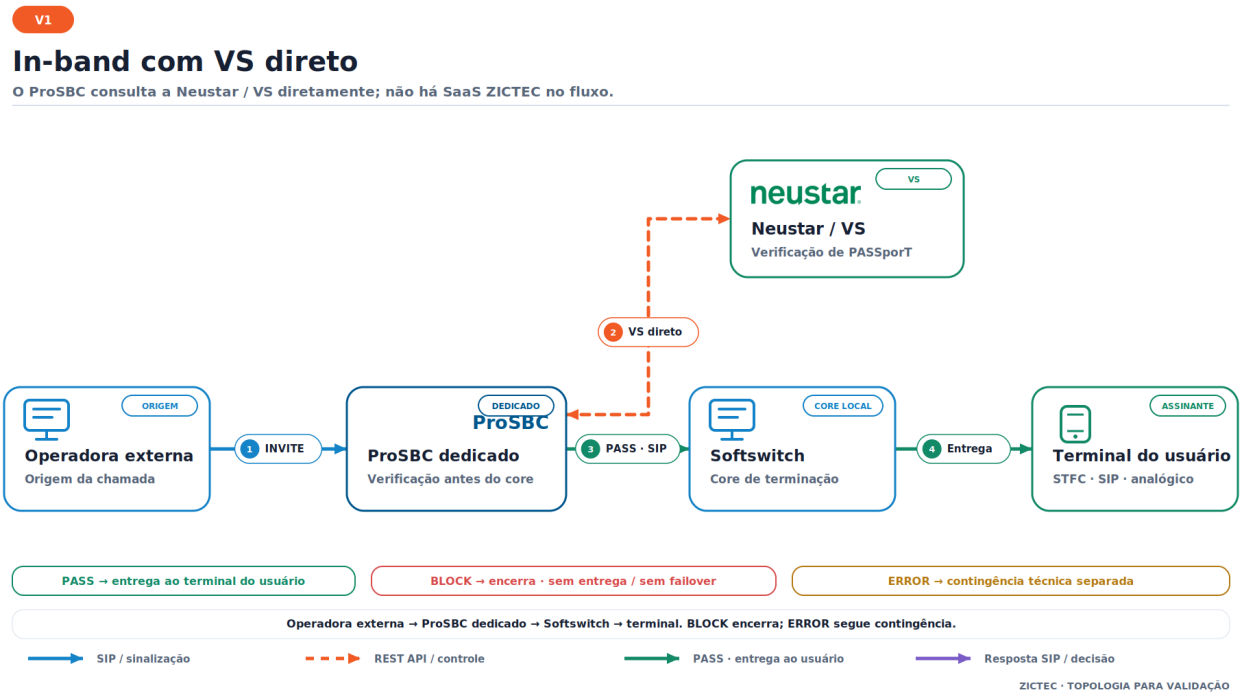


Os cenários V reutilizam os modelos de integração A, mas representam a **recepção e terminação de uma chamada**: **operadora de origem ou de transporte** → **rede de terminação (SBC/softswitch e VS)** → **terminal do usuário**. A operadora externa entrega a chamada na interconexão; o SBC/softswitch é um elemento intermediário da rede receptora, não a origem externa. O VS verifica a identidade recebida, não cria uma nova identidade. A entrega ao terminal só ocorre quando a decisão permitir, independentemente de o terminal ser SIP, STFC, analógico ou legado.

Nos modelos redirect e OOB, é o **core da rede de terminação** que consulta o serviço de verificação e interpreta o retorno. Em PASS, ele continua a entrega ao usuário; em BLOCK, encerra sem entrega e sem failover; erro técnico segue contingência homologada. O retorno do serviço não determina que a operadora externa refaça a chamada.

Cenário	Ponto de verificação	Consulta VS	Resultado operacional
V1 — In-band dedicado padrão	ProSBC de interconexão	VS autorizado direto	Completa, sinaliza ou rejeita segundo política
V2 — Dedicado com políticas	ProSBC de interconexão	VS direto + policy engine ZICTEC	STIR + DNO/blacklist/reputação contratados
V3 — Dedicado com SaaS	ProSBC de interconexão	API ZICTEC orquestra VS	Resultado estruturado e auditoria centralizada
V4 — Decisão 302 dedicada	ProSBC/iSBC dedicado	VS autorizado	Resultado devolvido em 302 homologado; semântica de controle contratual
V5 — VS OOB dedicado	ProSBC/iSBC dedicado	VS autorizado	Código distinto para pass, block e erro técnico
V6 — Decisão 302 Cloud	SIP VS SERVICE ZICTEC	VS pela nuvem	Resposta de decisão; core de terminação entrega ao terminal fora da plataforma
V7 — VS OOB Cloud	SIP VS SERVICE ZICTEC	VS pela nuvem	Core legado consulta por SIP; só pass entrega ao terminal

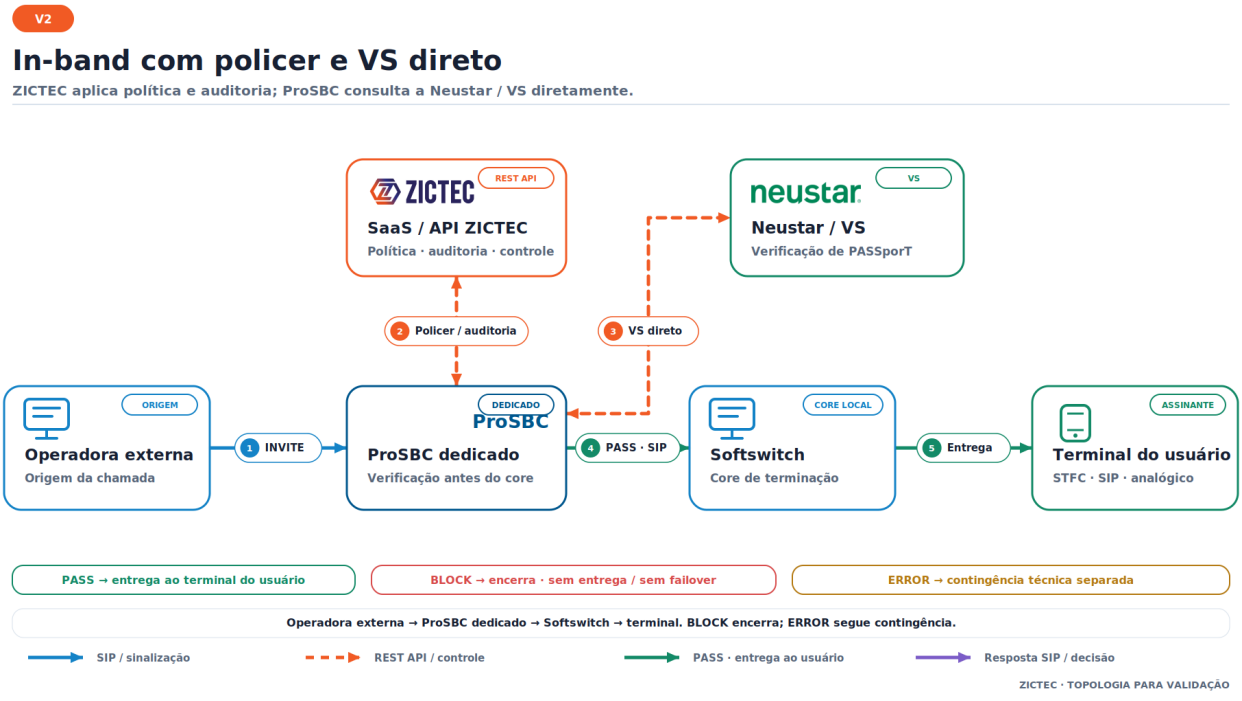
V1 — Verificação in-band dedicada padrão



Topologia técnica — cenário V1. Fluxos, componentes e integrações do cenário.

O `INVITE` recebido da operadora externa segue pelo ProSBC dedicado, que consulta o VS autorizado, preserva o resultado e aplica a política. Quando permitido, a chamada segue ao Softswitch e, somente depois, ao terminal do usuário: **operadora externa** → **ProSBC dedicado** → **Softswitch** → **terminal do usuário**. O Softswitch sempre antecede a entrega ao terminal; quando não há ProSBC dedicado, a chamada ingressa no Softswitch.

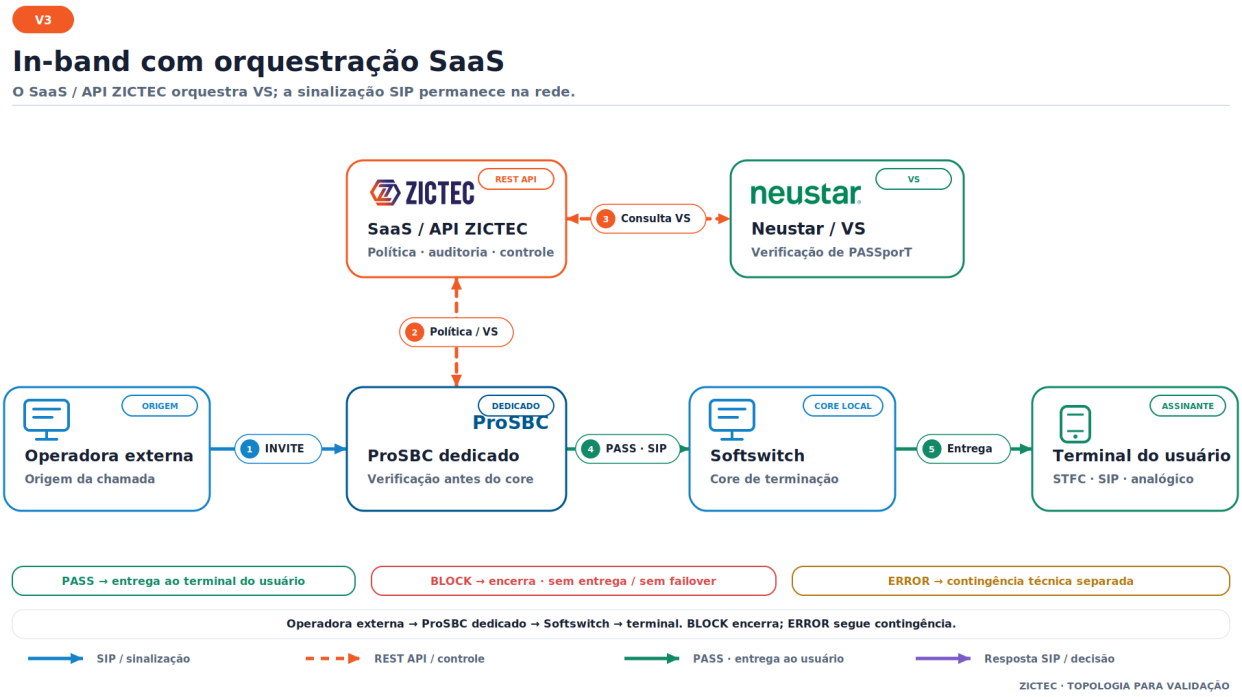
V2 — Verificação dedicada com policer/auditoria



Topologia técnica — cenário V2. Fluxos, componentes e integrações do cenário.

Além da validação criptográfica, a camada ZICTEC executa checagens opcionais de DNO, numeração, blacklist e reputação. Cada motivo permanece separado no log e na decisão.

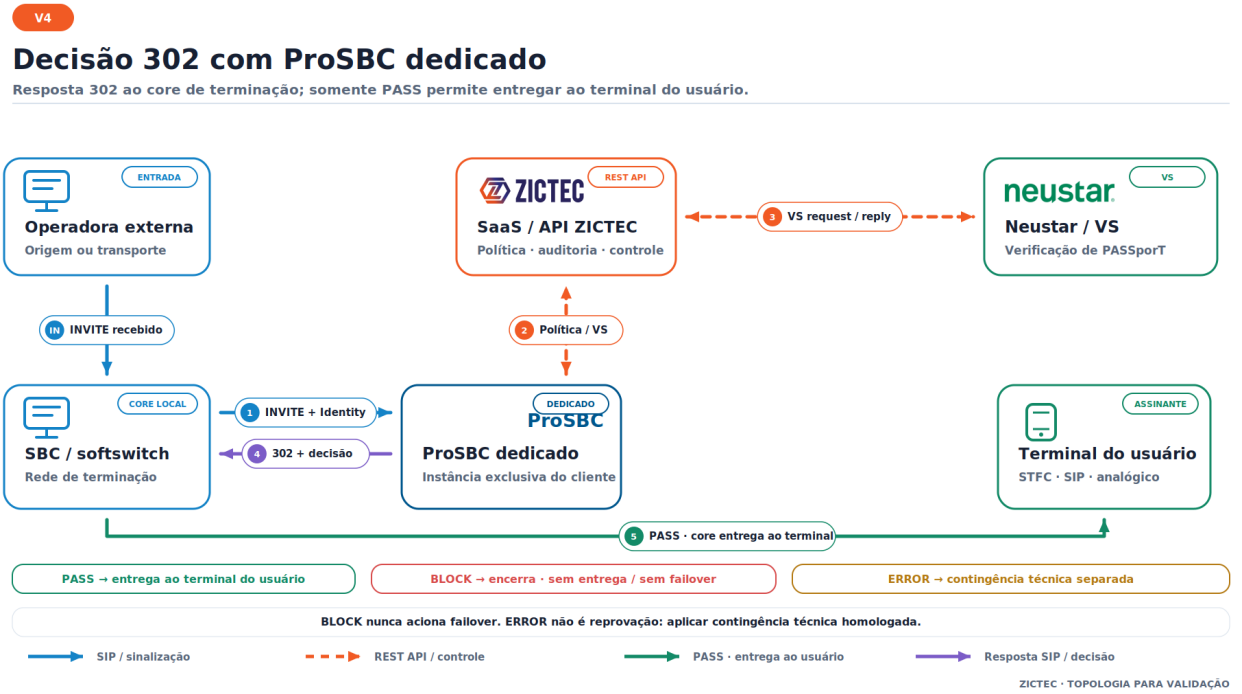
V3 — Verificação dedicada com orquestração SaaS



Topologia técnica — cenário V3. Fluxos, componentes e integrações do cenário.

O ProSBC consome a API ZICTEC; a nuvem coordena VS, auditoria e políticas. O tráfego pode permanecer local, com apenas o plano de decisão na nuvem.

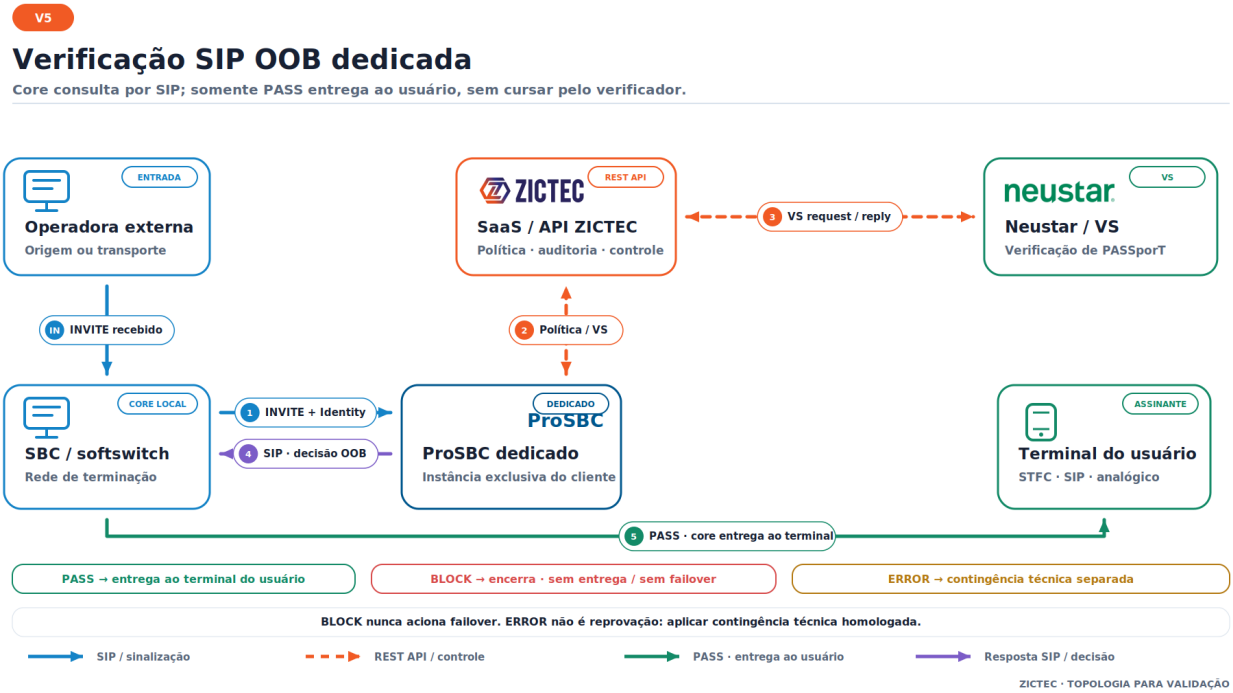
V4 — Resultado VS em 302 pelo iSBC dedicado



Topologia técnica — cenário V4. Fluxos, componentes e integrações do cenário.

O `302` atua como envelope de integração homologado, não como código STIR universal. O SBC/softswitch da rede de terminação extrai o estado de verificação e prossegue com a entrega ao terminal do usuário somente em caso permitido.

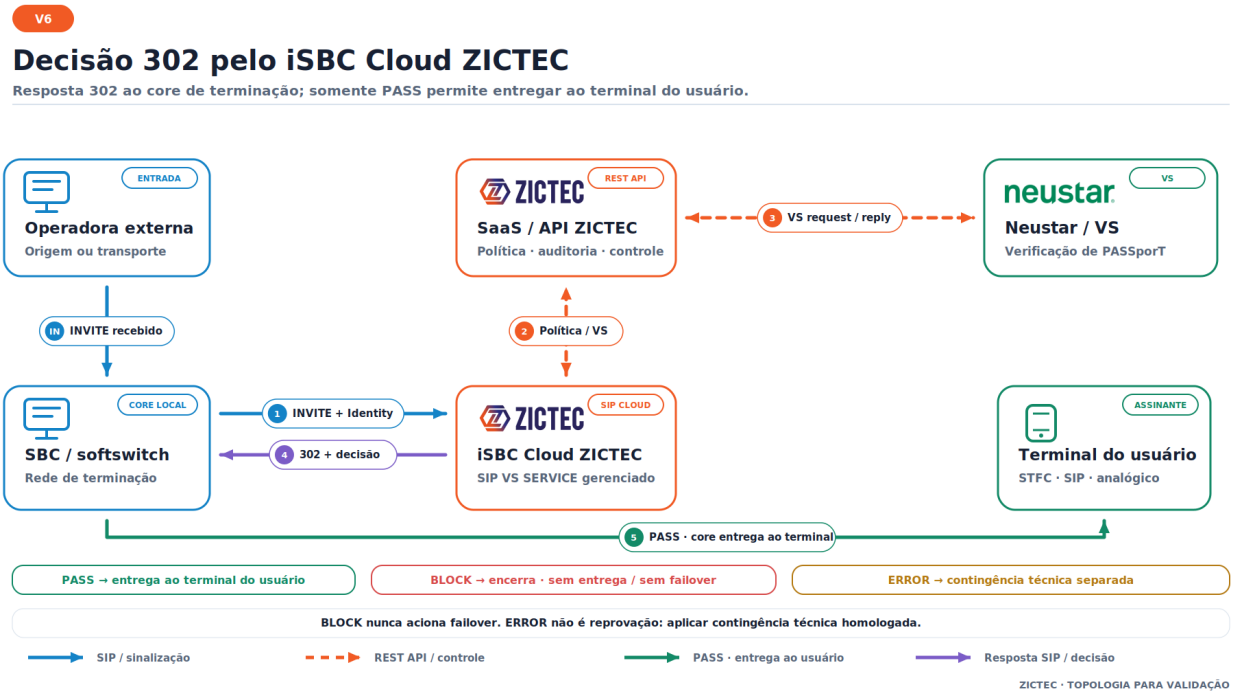
V5 — Verificação OOB pelo iSBC dedicado



Topologia técnica — cenário V5. Fluxos, componentes e integrações do cenário.

Adequado quando o SBC/softswitch da rede de terminação trata continuação por código SIP. `pass` encaminha à rota de entrega ao terminal do usuário; `block` encerra; `error` aciona contingência. Nunca configurar `block` como condição de failover.

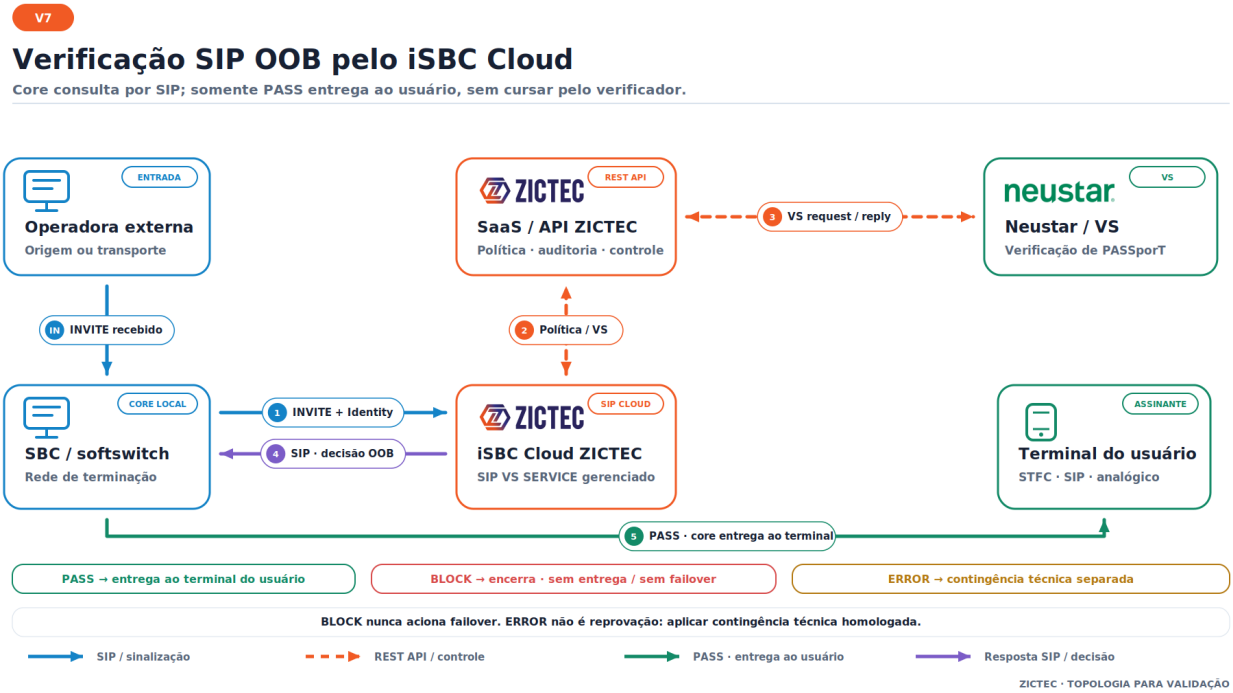
V6 — Resultado VS em 302 pelo SIP VS SERVICE Cloud ZICTEC



Topologia técnica — cenário V6. Fluxos, componentes e integrações do cenário.

Após receber a chamada da operadora externa, o core da rede de terminação consulta a nuvem por SIP. Ele recebe decisão e metadados e, se autorizado, entrega ao terminal do usuário sem manter a chamada final cursando pelo serviço.

V7 — Verificação OOB pelo SIP VS SERVICE Cloud ZICTEC



Topologia técnica — cenário V7. Fluxos, componentes e integrações do cenário.

O SBC ou softswitch legado da rede de terminação recebe a chamada da operadora de origem/transporte e envia uma tentativa de consulta ao iSBC Cloud. Somente PASS permite a entrega ao terminal do usuário. Códigos SIP distintos identificam sucesso, reprovação e falha técnica. A implementação legada precisa de uma tabela de tradução e testes de ausência de bypass.

7. RCD: nome, motivo e logomarca

Quando a origem empresarial possui Origem Verificada/RCD habilitada e os dados foram autenticados, o VS pode disponibilizar:

- nome validado para apresentação e registro;
- motivo da chamada para terminais compatíveis;
- logomarca/imagem por referência HTTPS ou jCard, com controles de integridade;
- estado de verificação e proveniência para o SBC/softswitch.

O SBC deve remover ou reclassificar dados não verificados, impedir que um chamador injete `verified` por conta própria e preservar a distinção entre informação assinada, informação consultada e display local. Mesmo quando o telefone analógico recebe apenas número — ou número e nome via mecanismos tradicionais —, o core continua responsável por verificar e aplicar a política.

8. AS/VS intrarrede — on-net

Em chamadas em que a mesma rede controla originação e terminação, AS e VS podem ser executados no mesmo domínio administrativo sem perder sua separação lógica. Há outros cenários possíveis para ON-NET, cuja viabilidade geralmente depende do suporte do Softswitch ou do posicionamento de um ProSBC como front-end antes do Softswitch, utilizando as APIs ZICTEC. Os modelos abaixo são exemplos de integração, não um catálogo exaustivo de topologias.

API `samestep`

Uma única transação de API solicita autenticação da perna originada, verificação da identidade relevante e políticas complementares. A resposta deve manter campos distintos para:

- resultado AS e `Identity` emitido;
- resultado VS e causa técnica;
- resultado de DNO/blacklist/reputação;
- decisão final de política;
- RCD validado;
- identificadores de auditoria e correlação.

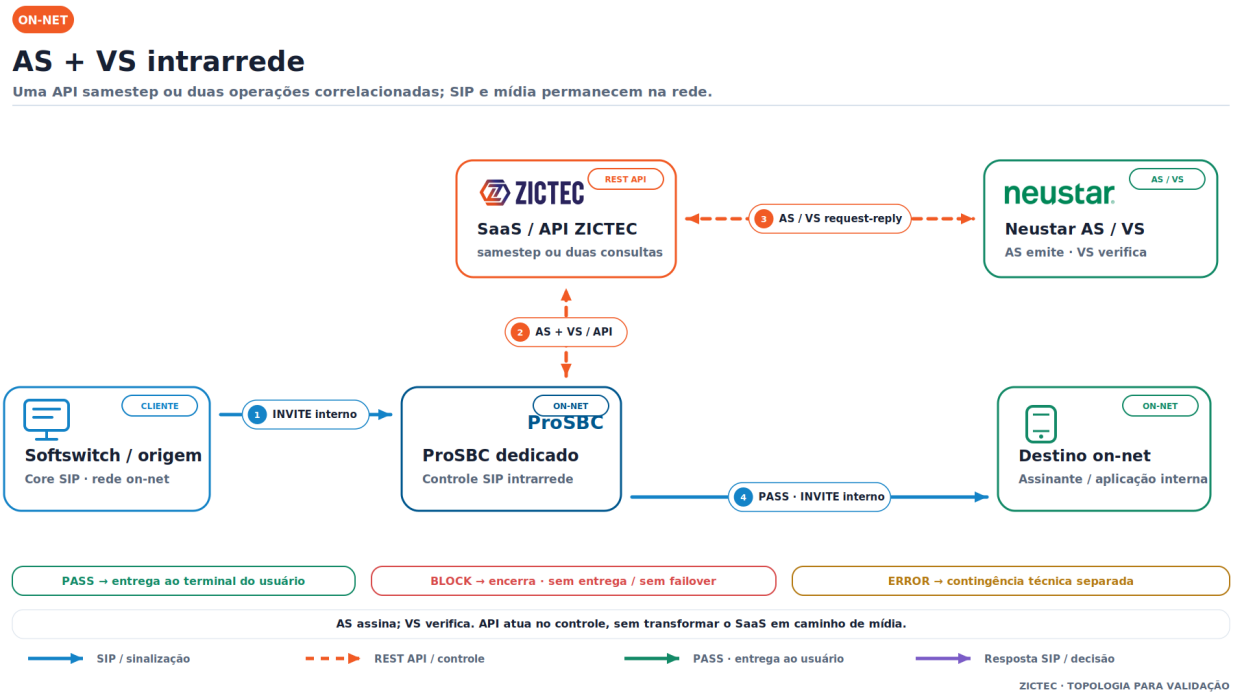
Duas chamadas de API

AS e VS são chamados separadamente quando há pernas, credenciais, equipes, tempos ou trilhas de auditoria diferentes. Esse modelo facilita troubleshooting granular e retry seletivo.

Regras on-net

- “Mesma rede” não significa dispensar assinatura/verificação quando a política ou regulação exigir evidência.
- O `Identity` deve corresponder à perna protegida; mudanças feitas pelo B2BUA podem exigir nova autenticação.
- A decisão antispam permanece independente da validade criptográfica.
- A indisponibilidade parcial de AS ou VS deve gerar estados separados, nunca um “sucesso genérico”.

9. AS/VS intrarrede — topologia e operação



A arquitetura on-net pode ser centralizada na API ZICTEC sem obrigar o tráfego RTP a sair da rede. O softswitch/ProSBC envia uma transação `samestep` ou duas consultas, recebe os resultados e executa a chamada internamente. STFC Tools agrega auditoria, relatórios e controles contratados.

A topologia é ilustrativa. Outros cenários ON-NET dependem do suporte do Softswitch ou de um ProSBC antes dele, como front-end integrado às APIs ZICTEC. Não são detalhados aqui porque variam conforme a operação.

10. DNO, antispam e blacklists

DNO

DNO (*Do Not Originate*) identifica números que, por autoridade do titular ou fonte confiável, não devem aparecer como origem. Não é a lista de destinatários “Não Me Perturbe” e não equivale a reputação negativa.

Blacklist estática e dinâmica

- **estática:** entrada administrada, com fonte, motivo, validade, autor e remoção auditáveis;
- **dinâmica:** inferida por analytics, com confiança, janela temporal, expiração, salvaguardas e contestação;
- **allowlist/exceções:** emergência, utilidade pública, saúde e outras classes aplicáveis devem ser protegidas conforme a regra vigente.

Limitação de consulta por CNPJ

Enquanto não houver fonte pública confiável para consulta em tempo real de todos os vínculos entre CNPJ e grupos de números, a funcionalidade pode ficar limitada à análise do terminal individual. Recursos por grupo/CNPJ dependem de integrações adicionais, dados autorizados e governança de atualização. O whitepaper não presume uma base nacional DNO universal que não foi confirmada.

11. Política regulatória e bloqueio

A **Medida Provisória nº 1.396, de 9 de outubro de 2026**, publicada no DOU de 13/10/2026, estabelece deveres para as prestadoras de interesse coletivo que utilizam numeração pública: a origem autentica, o trânsito preserva e a terminação verifica a autenticação antes da entrega (art. 2º). Prevê bloqueio de chamadas não autenticadas na terminação, ressalvadas as hipóteses da Anatel (art. 3º, I), identificação de chamadas empresariais autenticadas com nome e logotipo, se houver (art. 4º), e base centralizada com vínculos de numeração, titular e CNPJ (art. 5º).

Vigência não se confunde com exigibilidade operacional. A MP vigora desde a publicação (art. 10), mas autenticação, verificação, bloqueio por ausência de autenticação, identificação e base de dados tornam-se exigíveis conforme a regulamentação da Anatel e seus prazos de implementação (art. 8º, § 2º). O prazo de sessenta dias é para regulamentação; o prazo de trinta dias do § 1º alcança apenas as obrigações ali indicadas. A MP não especifica STIR/SHAKEN nem impõe um modelo de integração AS/VS.

Para uso abusivo, o art. 6º combina volume diário por acesso ou conjunto de acessos do usuário com proporção de chamadas curtas, prevê bloqueio de originação por quinze dias e ressalvas para atividades essenciais. A apuração por grupo exige vínculo autorizado e atualizado entre usuário e terminais; a previsão legal da base não comprova disponibilidade pública de consulta em tempo real. Checagem de terminal único não deve ser apresentada como apuração integral por CNPJ.

O art. 60 do RGST determina autenticação abrangente para prestadoras de serviços coletivos que usam numeração E.164, com prazo de três anos da entrada em vigor para atuais STFC/SMP e possibilidade de exceções ou prazos adicionais pelo Conselho Diretor.

Para grandes chamadores, o Despacho 787/2025 alcança volume superior a 500.000 chamadas por serviço e prestadora em mês civil, com notificação, prazo de regularização, exceções e eventual bloqueio da capacidade de originação. Isso difere de rejeitar instantaneamente cada chamada sem assinatura.

O Despacho 82/2026, conforme comunicado oficial da Anatel, estabelece salvaguardas quando a prestadora adota antispam próprio: ativação padrão gratuita, opt-out, proporcionalidade, proteção de serviços essenciais e contestação. A política técnica deve refletir exatamente o ato aplicável ao caso e sua vigência.

Regra de engenharia: quando a política aplicável exigir bloqueio e a chamada for efetivamente reprovada, o bloqueio deve ocorrer no SBC/softswitch antes da entrega ao assinante, mesmo que o terminal não suporte STIR/SHAKEN ou RCD. Isso não autoriza transformar toda ausência de `Identity` em fraude ou bloqueio universal.

12. Matriz de decisão

Necessidade	Caminho preferencial	Controle essencial
ProSBC existente e alto volume	Módulo AS/VS local	Capacidade, certificados, failover e rollback
Core moderno e integração nativa	API direta	Schema, correlação, timeout e estados separados
SBC legado sem API	SIP OOB via iSBC Cloud	Códigos distintos para pass/block/error
Chamada recebida com RCD	VS + policy engine	Proveniência, integridade e apresentação compatível
Originação e terminação na mesma rede	API AS+VS `samestep`	Resultados independentes e auditoria comum
Políticas complexas por CNPJ/grupo	Integrações adicionais	Fonte autorizada, atualização e recurso
Redução da operação interna	SaaS + STFC Tools	SLA, conectividade, contingência e governança

13. Segurança, disponibilidade e aceite

Antes da produção, registrar e testar:

- executor de AS, VS e policy engine;
- chaves, certificados, trust stores, rotação e revogação;
- PASSporT compacto/completo e tratamento de retry previsto;
- skew temporal, `Date`, `iat`, replay e correlação;
- políticas independentes para `pass`, `block`, `no_identity`, `invalid`, `credential_error` e `service_unavailable`;
- códigos SIP externos e traduções legadas internas;
- garantia de que `block` não aciona failover;
- contingência de indisponibilidade e limites de fail-open;
- CPS, sessões e latência P95/P99;
- RCD, integridade de imagem, cache e remoção de dados não verificados;
- exceções regulatórias, opt-out e contestação quando aplicáveis;
- logs sem chaves nem dados pessoais excessivos;
- testes em SIP moderno, STFC/analógico/TDM e terminais incompatíveis;
- rollback e critérios formais de aceite.

14. Oferta ZICTEC e próximos passos

A ZICTEC pode entregar AS e VS por módulo em ProSBC dedicado, API oficial, integração SIP OOB/redirect, SIP AS/VS SERVICE Cloud ou SBC on-premises dedicado conectado às APIs. STFC Tools pode agregar auditoria, relatórios e checagens complementares conforme o pacote contratado.

A nomenclatura comercial pública ainda contém SKUs originalmente orientados a STI-AS. O enquadramento de VS, RCD e políticas adicionais deve ser confirmado na proposta e no escopo técnico, sem presumir inclusão automática em licença antiga.

Prepare sua rede para a Chamada Verificada

Converse com a ZICTEC sobre AS, VS, RCD e a integração mais adequada ao seu ambiente.

Site https://www.chamadaverificada.com.br

E-mail suporte@zictec.com.br

WhatsApp https://wa.me/554732300435

Referências técnicas e regulatórias

- RFC 3261 — SIP: https://www.rfc-editor.org/rfc/rfc3261
- RFC 8224 — Authenticated Identity Management in SIP: https://www.rfc-editor.org/rfc/rfc8224
- RFC 8225 — PASSporT: https://www.rfc-editor.org/rfc/rfc8225
- RFC 8588 — SHAKEN PASSporT: https://www.rfc-editor.org/rfc/rfc8588
- RFC 8197 — SIP 607 Unwanted: https://www.rfc-editor.org/rfc/rfc8197
- RFC 8688 — SIP 608 Rejected: https://www.rfc-editor.org/rfc/rfc8688
- RFC 8816 — STIR Out-of-Band Architecture: https://www.rfc-editor.org/rfc/rfc8816
- RFC 9795 — PASSporT Extension for Rich Call Data: https://www.rfc-editor.org/rfc/rfc9795
- RFC 9796 — SIP Call-Info Parameters for Rich Call Data: https://www.rfc-editor.org/rfc/rfc9796
- Anatel — Autenticação e Identificação de Chamadas: https://www.gov.br/anatel/pt-br/regulado/acompanhamento-e-controle/autenticacao-e-identificacao-de-chamadas
- Medida Provisória nº 1.396, de 9/10/2026 — DOU de 13/10/2026; arts. 2º–6º, 8º e 10: https://www.in.gov.br/web/dou/-/medida-provisoria-n-1.396-de-9-de-outubro-de-2026-737772550
- Resolução Anatel nº 777/2025: https://informacoes.anatel.gov.br/legislacao/resolucoes/2025/2022-resolucao-777
- Anatel — Medidas cautelares sobre chamadas abusivas: https://www.gov.br/anatel/pt-br/consumidor/chamadas-abusivas/medidas-cautelares
- Anatel — regras para antispam próprio das prestadoras: https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-estabelece-regras-para-ampliacao-dos-mecanismos-de-bloqueio-automatico-de-chamadas-abusivas-pelas-prestadoras

Documento técnico-comercial. A topologia, os códigos de integração, o alcance regulatório e as regras de bloqueio devem ser homologados para o ambiente, contrato e atos aplicáveis ao cliente.