As chaves, do zero

Um guia de cinco minutos. Sem criptografia, sem código, sem nomes difíceis.

1 O que é uma chave

Quando crias uma conta na Stripe, eles dão-te uma string enorme. Essa string **é a tua identidade para eles**. Cada pedido que a leve é aceite como sendo teu.

Uma chave é, portanto, **uma password que não inventas: que te dão**. Não é código, não é magia. É uma password comprida e aleatória.

2 Onde é que ela fica

Tens cinco serviços — Gmail, Stripe, Telegram, Sheets, Resend — e portanto cinco dessas strings. Só há três sítios onde as pôr.

No programa	**No agente**	**Num cofre**
Quem vê o código vê as chaves. Ficam no histórico para sempre.	A chave viaja para o fornecedor do modelo, para os registos e para a conversa.	Só o servidor abre. Não aparece em conversas, registos nem cópias.
Não serve	Não serve	É o que usamos

Fig. 1 — os três sítios possíveis. A escolha do cofre é a única decisão de segurança do sistema.

3 A segunda chave: a do cofre

Se o cofre for só uma caixa, quem a abrir leva tudo. Então a caixa está **fechada com uma chave**. É a essa que chamamos **chave do cofre** (ou chave primária).

COFRE — o que está lá dentro

fechada com a chave do cofre

`chave do Gmail` `chave da Stripe` `chave do Telegram` `chave do Sheets` `chave da Resend`

Fig. 2 — uma caixa, cinco chaves dentro, uma fechadura. Só existem estes dois tipos de chave.

Ou seja, em todo o sistema há **apenas duas espécies** de chave:

1	**5**
chave do cofre (a fechadura)	chaves dos serviços (uma por conta)

Repara numa coisa importante

As chaves dos serviços **não são chaves do sistema**. São passwords de contas tuas, dadas por terceiros (Google, Stripe…). A única chave que este sistema cria e guarda é **a do cofre** — e é por isso que só essa precisa de backup e de rotação.

4 Quando o agente chama um método

Aqui está o ponto que confunde. O agente quer enviar um email, e o pedido dele é **só isto**:

O PEDIDO QUE O AGENTE FAZ	O QUE NESTE PEDIDO NÃO EXISTE
método: `email_elizeu.enviar`	nenhuma chave
para: `joao@exemplo.pt`	nenhuma password
assunto: `Relatório`	nada que venha do cofre
corpo: `Segue em anexo.`	—

O agente nunca envia uma chave. Envia o nome do método e os dados. Nem sabe que existe uma chave — se lhe perguntarem, responde que não tem acesso a credenciais.

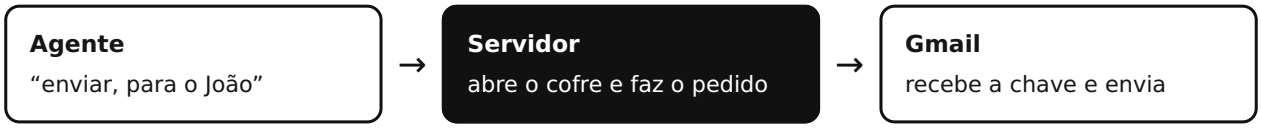

Fig. 3 — o agente fala com o servidor. O servidor fala com o Gmail. São conversas separadas.

O que acontece dentro do servidor, em seis passos

1. Recebe “enviar, para o João”.
2. Abre o cofre — com a chave do cofre, a única que ele guarda.
3. Tira a chave do Gmail.
4. Põe essa chave no pedido ao Gmail, com o destinatário e o texto.
5. O Gmail responde “enviado”.
6. Fecha o cofre, esquece a chave, devolve “enviado” ao agente.

> O agente participa no passo 1 e no passo 6. Os passos 2 a 5 acontecem à porta fechada.

5 Porque é que às vezes as chaves mudam

A **chave do cofre** pode ser trocada de tempos a tempos. Chama-se a isso **rotação**. É como mudar a fechadura da caixa: as cinco chaves lá dentro **não mudam**.

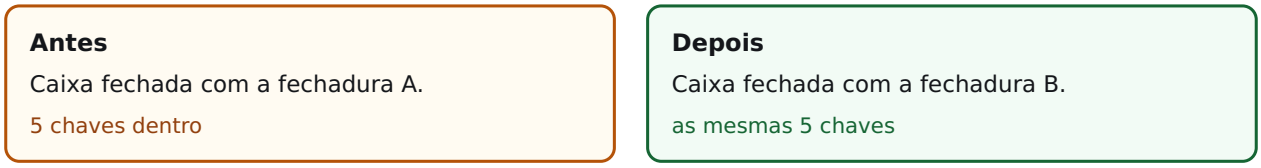

Fig. 4 — rotação troca a fechadura, não o conteúdo. Ninguém volta a colar chaves.

Serve para uma coisa concreta: se alguém copiou a fechadura A há meio ano, essa cópia deixa de abrir a caixa. É limitação de dano, não prevenção de assaltos.

As chaves dos serviços **não mudam** com a rotação. A do Gmail continua a mesma até tu decidires trocá-la no site do Google.

6 Um exemplo com números

Duas contas ligadas: Gmail do Eliseu e Stripe.

2	1	3
chaves dos serviços Gmail + Stripe	chave do cofre a fechadura	chaves no total do sistema inteiro

O agente chama `email_elizeu.enviar`: o servidor abre o cofre com a chave do cofre, tira a chave do Gmail, envia, fecha. O agente nunca viu nenhuma das três.

As três perguntas que costumam ficar

A chave vai no pedido ao agente?
Não. O agente envia o método e os dados. Nada mais.

Quem tem a chave do cofre?
Só o servidor, num ficheiro fora da base de dados. Nem tu precisas dela.

Se mudar a chave do cofre, tenho de colar tudo outra vez?
Não. As chaves dos serviços ficam. Só a fechadura da caixa muda.

Glossário em cinco linhas

cofre	onde ficam guardadas as chaves dos serviços, fechadas.
credencial	a chave de uma conta concreta (a do Gmail do Eliseu).
chave do cofre	a fechadura da caixa. Uma só, no servidor, fora da base de dados.
rotação	trocar a fechadura. As chaves lá dentro ficam as mesmas.
revogação	tirar uma chave da caixa. O agente perde essa conta de imediato.

Resumo em uma frase: **o agente pede o trabalho, o servidor usa a chave, e a chave nunca sai da caixa.**