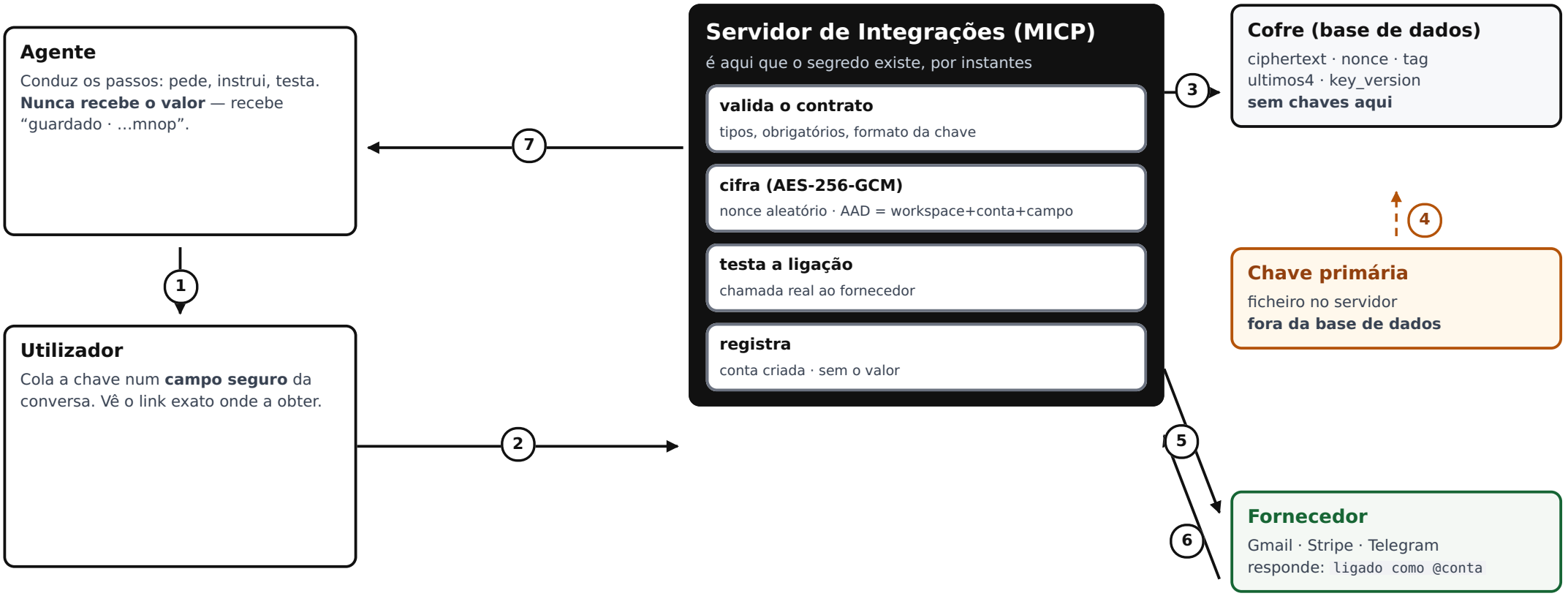
1 · Configurar uma conta

Acontece uma vez. O valor que a pessoa cola nunca passa pelo modelo.

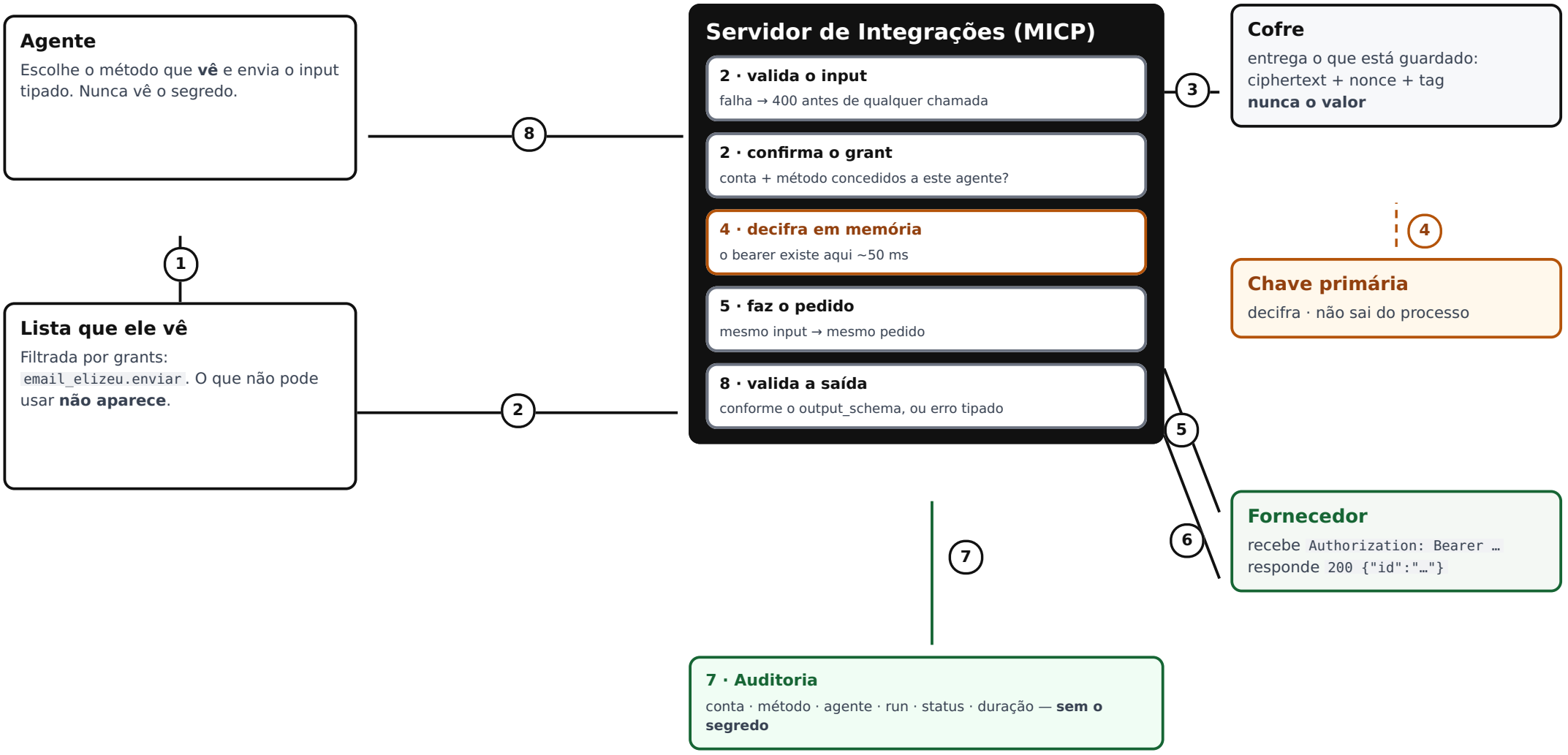


1 O agente pede os campos e o sítio exato onde encontrá-los.
2 A pessoa cola o valor; vai por TLS **direto ao servidor** — o modelo não o vê.
3 O servidor cifra e grava; fica só ciphertext.
4 A chave primária é o único segredo que cifra o cofre.

5 Testa a ligação a sério (falhar aqui evita falhar na primeira execução).
6 O fornecedor confirma: "ligado como @conta".
7 O agente recebe "guardado · …mnop". Nunca o valor.
O valor em claro é descartado no fim do passo 3.

2 · Executar um método

Acontece a cada chamada. O segredo em claro existe ~50 ms, dentro do servidor.



1 Escolhe um método da lista e envia o input.
2 Input validado e grant confirmado — antes de qualquer chamada.
3 O cofre entrega o ciphertext (não o valor).
4 A chave primária decifra, em memória.
5 Pedido determinístico, com o bearer.
6 Resposta do fornecedor.
7 Cada execução fica registada (mesmo as falhadas).
8 Saída validada e devolvida — ou erro tipado.

Se a chave primária faltar: **cofre_indisponivel** · a mesma execução repetida devolve o primeiro resultado (idempotência) ·

3 · Quantas chaves existem, e porquê

Três categorias. Só a primeira é “a tua”. Nenhuma delas chega ao modelo.

1

chave primária · por instalação

Cifra o cofre inteiro. Vive num ficheiro no servidor, **fora da base de dados**, com backup separado.

É a única que tens de guardar, rodar e recuperar. Se fossem N, eram N oportunidades de a perder.

N

credenciais · uma por conta

Uma por **conta ligada**, não por método. A conta é a identidade: `email_elizeu` e `email_suporte` são duas contas; quatro métodos partilham duas credenciais.

Se a conta tiver vários valores (OAuth), é **uma entrada com vários campos**.

M

chaves de acesso

Não cifram nada. Autorizam **quem chama**: token de agente, passe de run (15 min), token de webhook.

Se uma vazar, ninguém lê emails — gastam-se chamadas até revogares.

Exemplo · 3 contas Gmail, 3 agentes

`email_elizeu` → **só enviar**
`email_suporte` → enviar, listar, marcar lido
`email_financeiro` → enviar, listar

1 chave primária + **3** credenciais + **3** tokens de agente = **7 chaves em repouso**, das quais só 1 é “a tua”.
Os métodos **não** acrescentam chaves — mudam apenas o que cada conta expõe.

O que nunca sai do servidor

· a chave primária
· o texto em claro do segredo
· o nonce e a tag (vivem junto do ciphertext)
· um pedido que possa conter o segredo

Quando algo muda

Revogar uma conta
A célula desaparece da lista imediatamente. Nenhum agente a consegue chamar — sem reiniciar nada.

Rodar a chave primária
Escreve em v2, as linhas antigas abrem com v1 e são re-cifradas aos poucos. Ninguém volta a colar chaves.

Restaurar num desastre
Backup da base + backup da chave, em sítios diferentes. Juntos abrem o cofre; separados não servem.

Regra de ouro: **uma chave cifra tudo, cada credencial pertence a uma conta, e o valor em claro só existe durante uma chamada.**