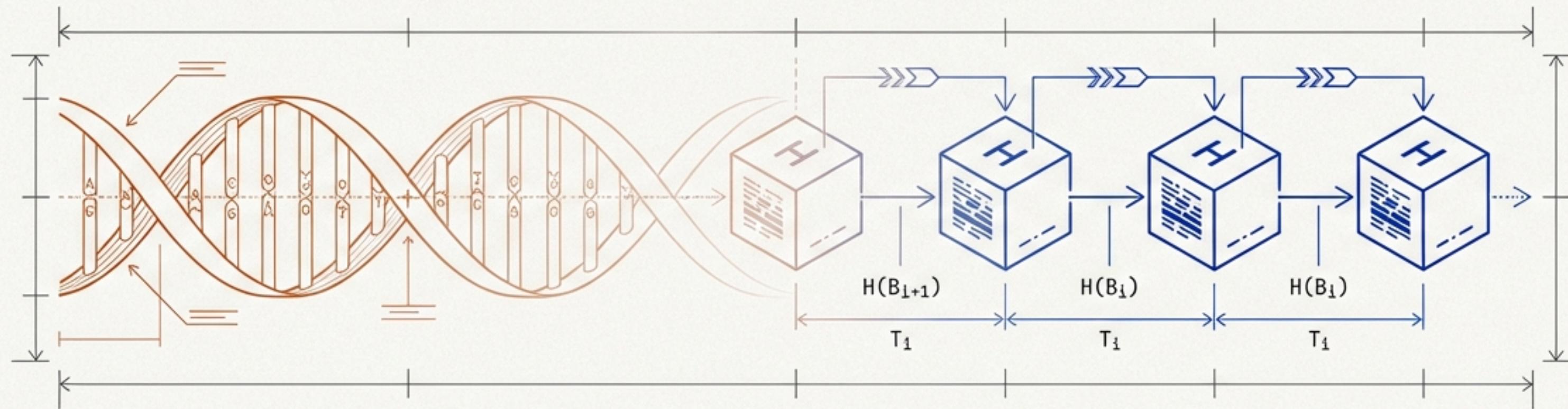


Q-TOTP

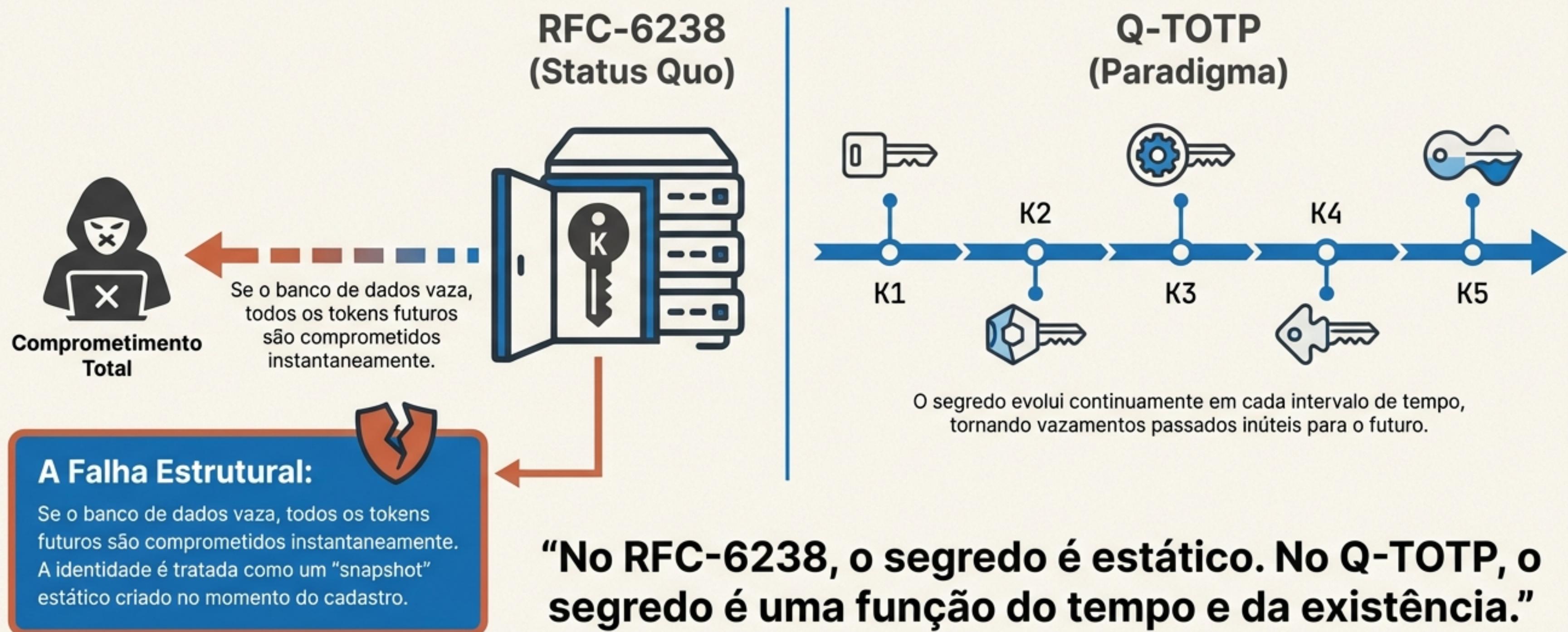
Quantum-Linked Time-based One-Time Password



Autenticando a continuidade biológica, não apenas o acesso. Uma evolução do padrão RFC-6238 que substitui segredos estáticos por sementes dinâmicas, vinculando criptografia temporal à biometria comportamental.

O Paradigma do Segredo Estático (RFC-6238)

No TOTP tradicional, a segurança depende inteiramente de um segredo compartilhado (K) que nunca muda.



A Filosofia Q-TOTP: Identidade como Continuidade

O Q-TOTP não pergunta apenas "você tem a chave?". Ele pergunta "você é a continuação válida da pessoa que criou esta conta?".



Identidade Externa (IdP)

A âncora de confiança
(Google, Gov.br, Open Finance).



Biometria Comportamental

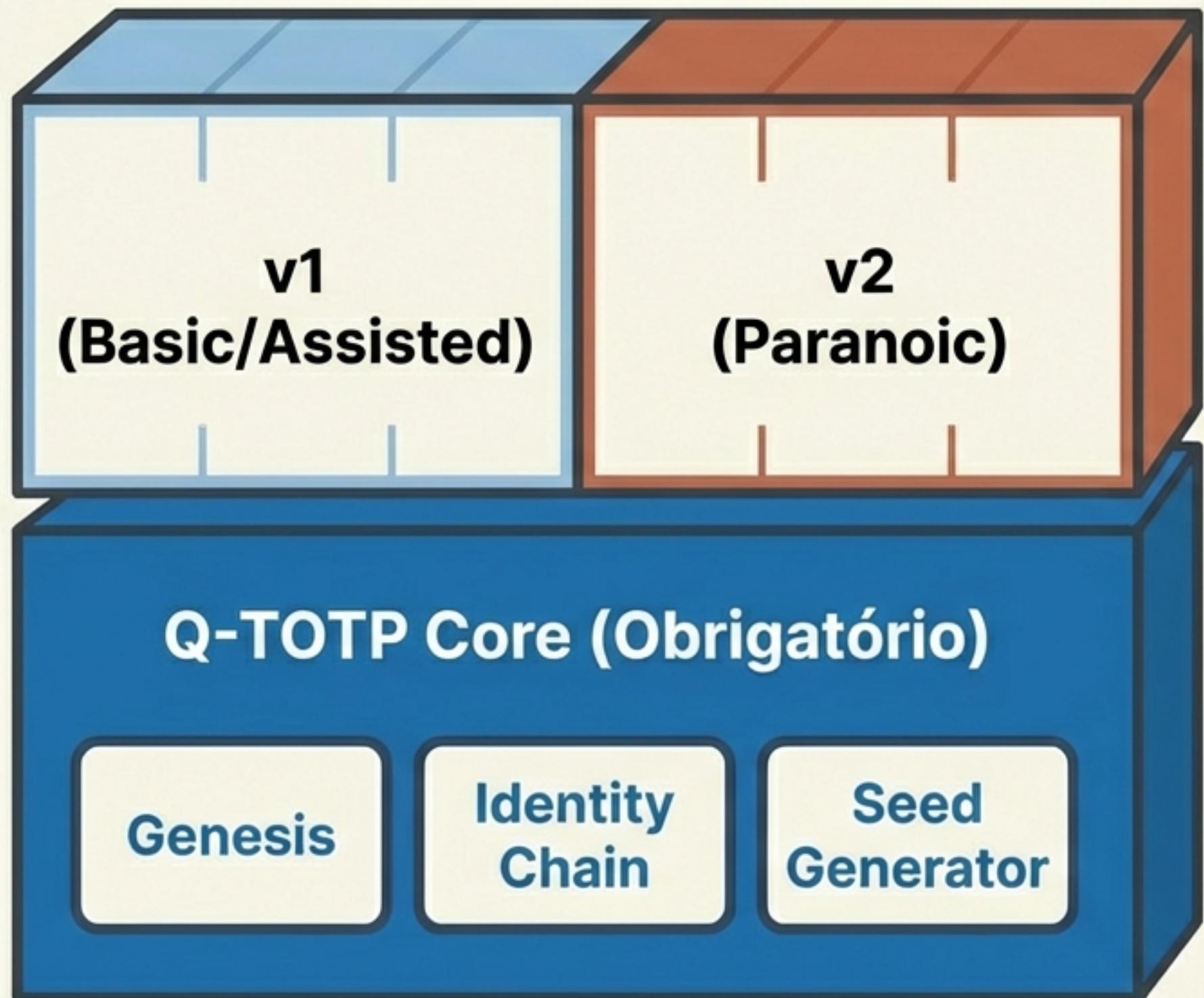
O ritmo de digitação,
tempo de voo e latência.



Dados Biológicos

Constantes imutáveis
(Aniversário, Tipo Sanguíneo).

Arquitetura Conceitual e Domínios

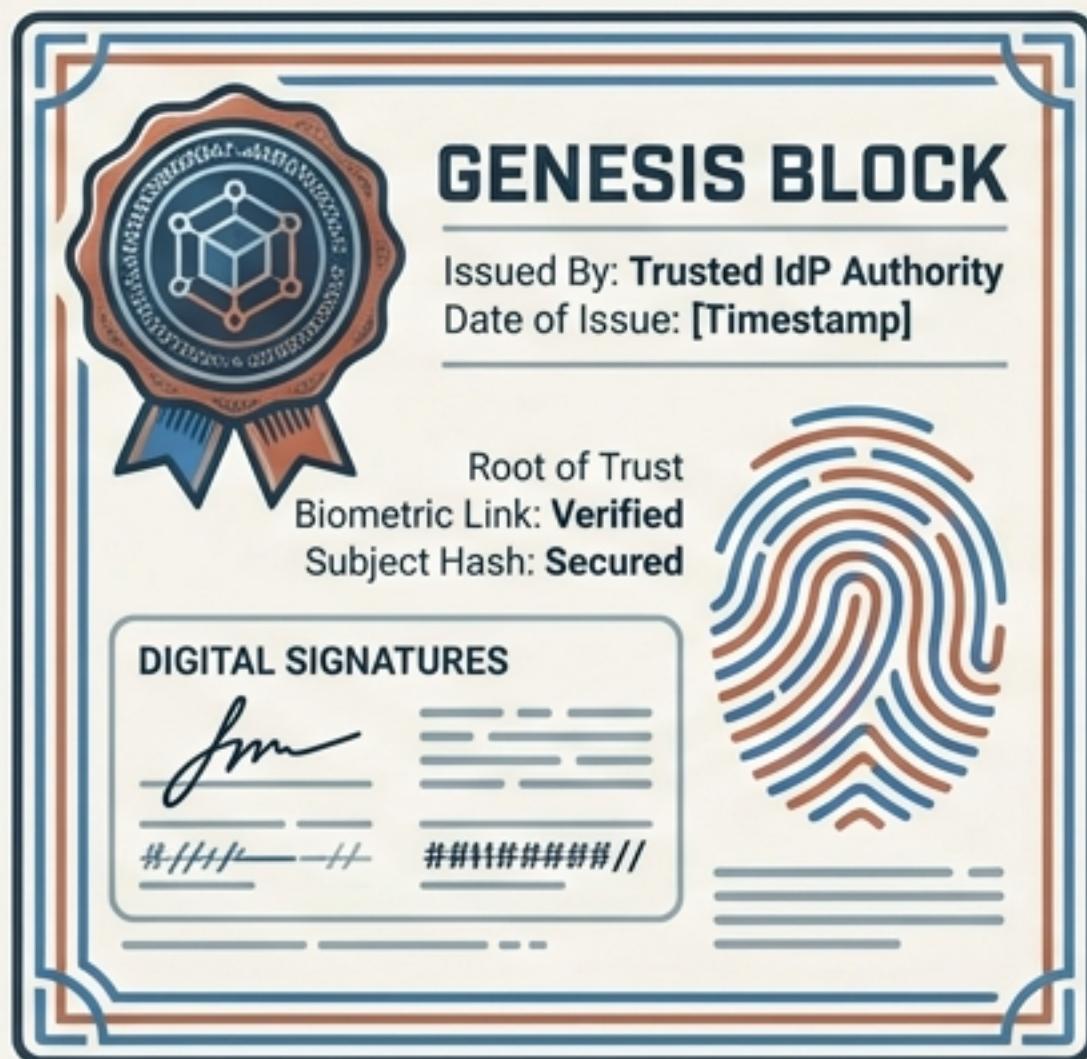


Helvetica Now Display Bold	Inter Regular
Identidade	Quem o humano é (Biologia + IdP)
Segredo	O que assina os códigos (S_user)
Persistência	Onde os dados vivem (Local vs. Vault)

Sem o Core, não existe Q-TOTP. Os modos v1 e v2 apenas alteram como o segredo é protegido.

Genesis: O Nascimento Digital

Nenhum usuário existe no sistema sem um bloco Genesis válido. É a raiz de confiança da cadeia.

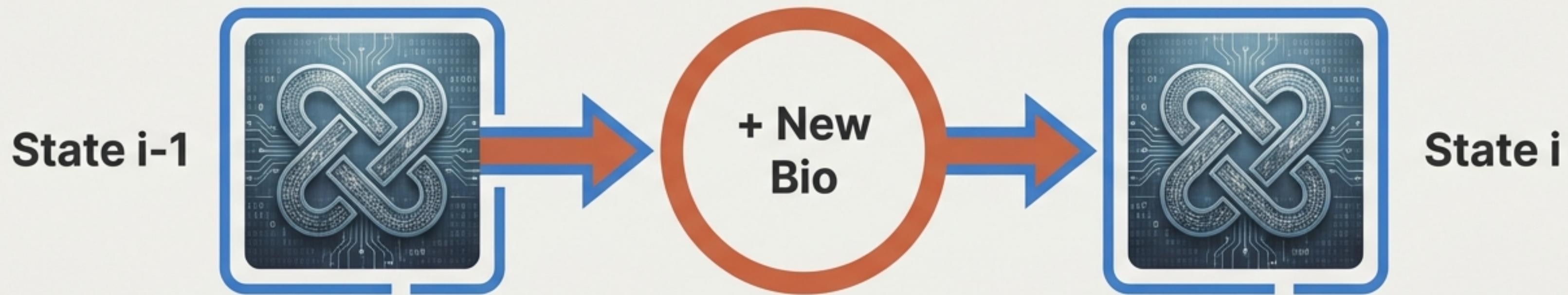


- Assinatura de um Identity Provider (IdP) confiável.
- Vinculação a um Perfil Biométrico Inicial.
- Persistência do hash do sujeito (IDP SUBJECT HASH), nunca dados em texto claro.

```
"genesis": {  
  "idp": "google_oauth",  
  "idp_subject_hash": "sha256(sub)",  
  "verified": true,  
  "verified_at": 1739474000  
}
```

The Identity Chain: Evolução Criptográfica

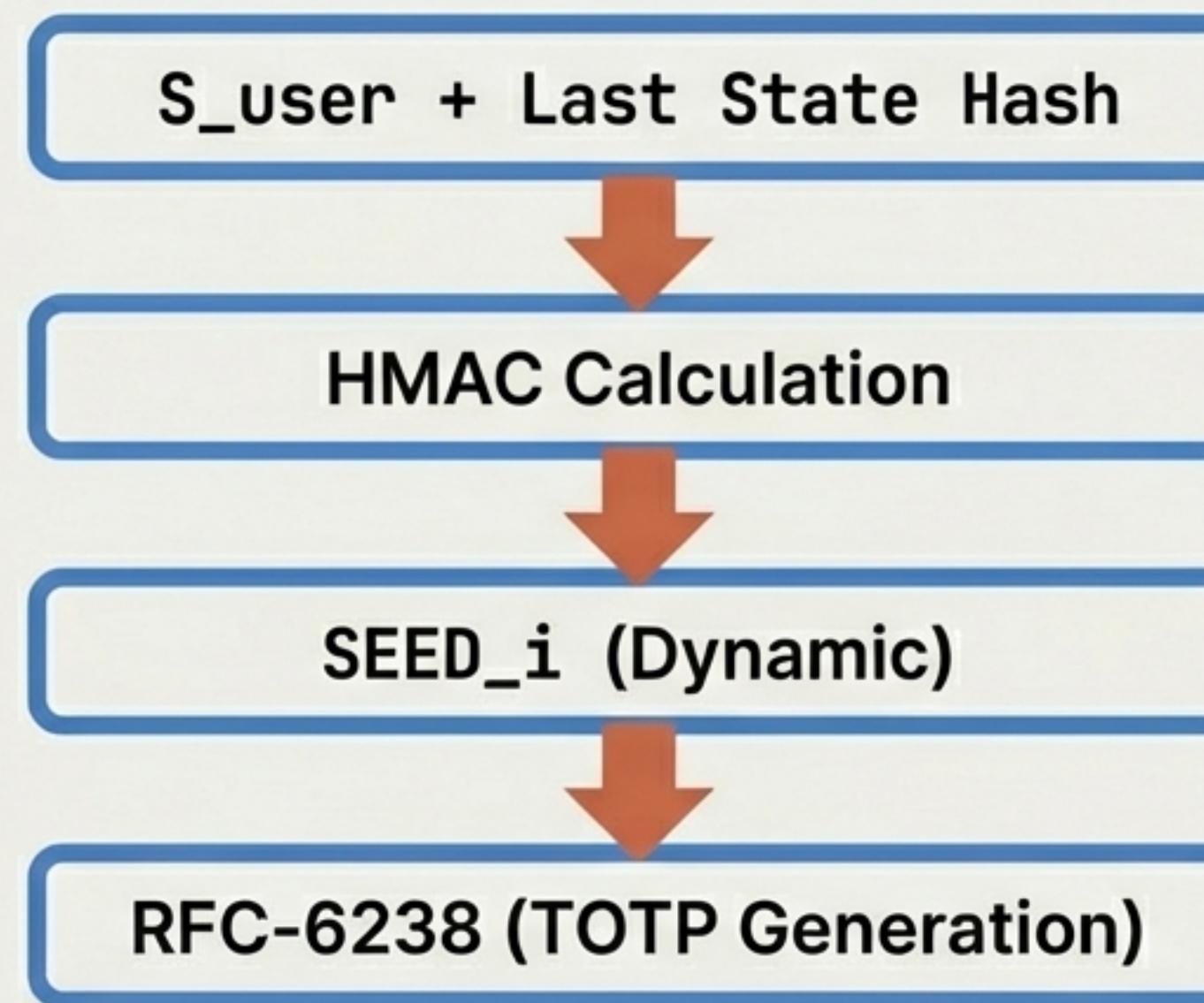
`state_hash_i = SHA256(new_bio + state_hash_(i-1))`



- Cada login bem-sucedido gera um novo bloco na cadeia.
- O estado atual depende matematicamente de todo o histórico anterior.
- Um atacante não pode forjar o estado atual sem ter vivido toda a cadeia de eventos biométricos do usuário.

O Seed Dinâmico (Dynamic Seed)

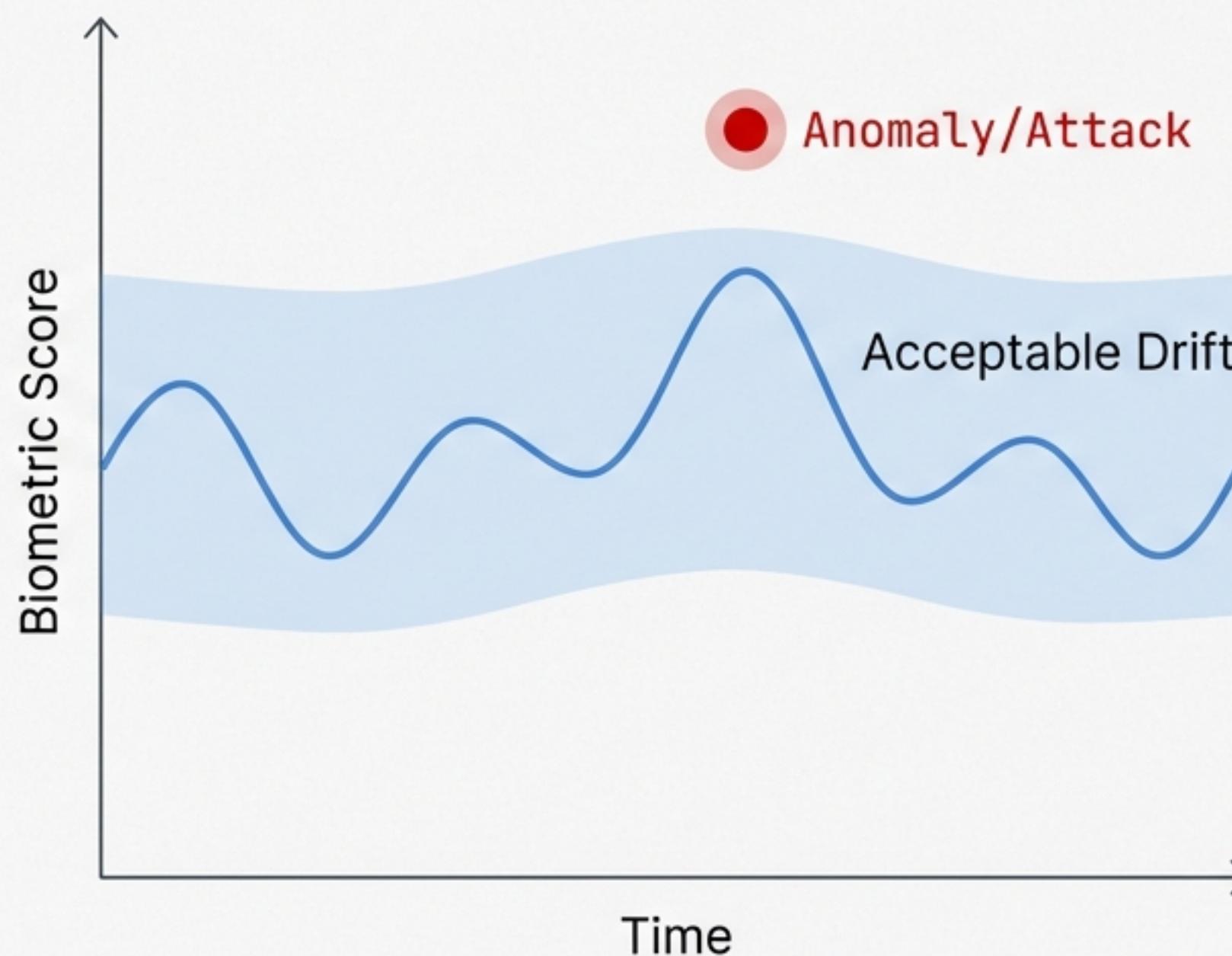
O segredo utilizado para gerar o código muda a cada iteração.
Um seed roubado hoje é inútil amanhã.



`SEEDi = HMAC(S_user , last_state_hash)`

`TOTP = RFC6238(SEEDi , current_time)`

O Fator Humano: Drift e Thresholds Adaptativos



Atualização Suave (Alpha Decay)

$\text{new_template} = (1 - \text{alpha}) * \text{old} + \text{alpha} * \text{new_capture}$

O parâmetro alpha (0.05–0.15) permite evolução gradual sem permitir mudanças abruptas.

Threshold Dinâmico

O sistema ajusta a exigência de pontuação (min_score) baseando-se na variância histórica do usuário, evitando bloqueios indevidos (lockouts).

Modos de Operação: Escalabilidade de Segurança

Q-TOTP v1



- **Foco:** Facilidade de implementação.
- **Armazenamento:** S_user local protegido pelo OS.
- **Ideal para:** Ambientes controlados e recuperação assistida.

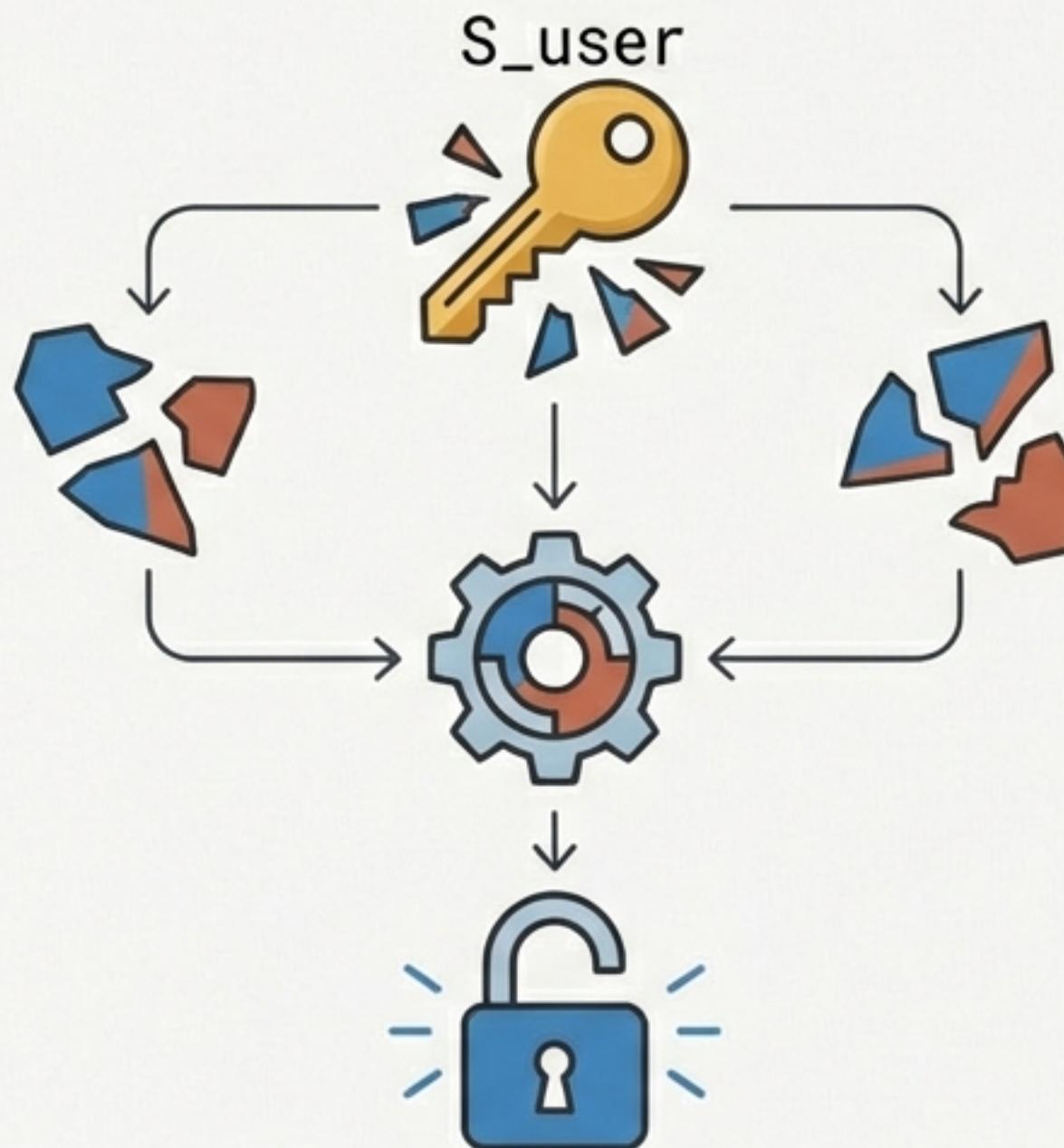
Q-TOTP v2 (Paranoic)



- **Foco:** Segurança extrema e Zero-Trust.
- **Features:** Fragmentação de segredo, Vault Cego, Zero-Knowledge Biometrics.
- **Ideal para:** Proteção de ativos críticos e finanças.

Deep Dive v2: Proteção Paranoica

Feature 1: Fragmentação (Shamir Secret Sharing)



O Segredo Mestre (S_{user}) é dividido em N partes.
Requer K partes para reconstruir.

Ex: 1 parte no celular, 1 no notebook, 1 em token
físico.

Feature 2: Vault Cego



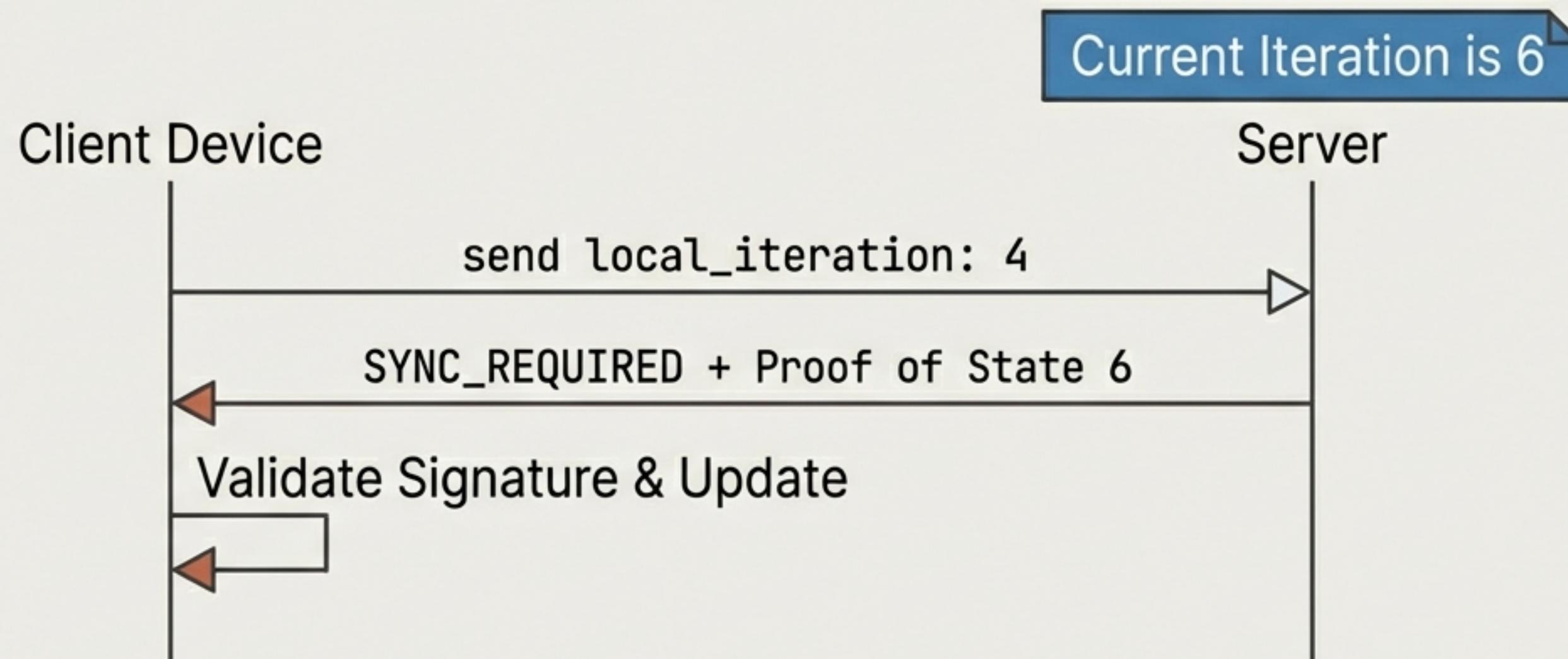
O servidor armazena apenas um cofre criptografado:

$$\text{Vault} = \text{Encrypt}(S_{user}, P)$$

O servidor não possui a chave P . Sem a senha do usuário e o segredo do dispositivo, o banco de dados é inútil para o atacante.

Sincronização Multi-Dispositivo (ICSH)

O servidor atua como a 'Fonte da Verdade' para o estado da cadeia.
A sincronização impede 'Forks' de identidade (bifurcações maliciosas).



Threat Model: Por que é Seguro?

Vazamento de DB

Atacante obtém hashes, mas não tem biometria nem PIN.



BLOCKED

Roubo de Dispositivo

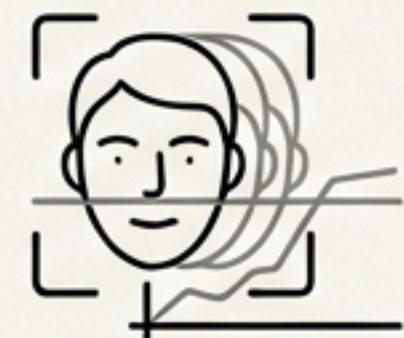
Atacante tem seed atual, mas falha na biometria comportamental.



CHAIN HALTED

Ataque de Interpolação

Tentativa de treinar biometria lentamente.

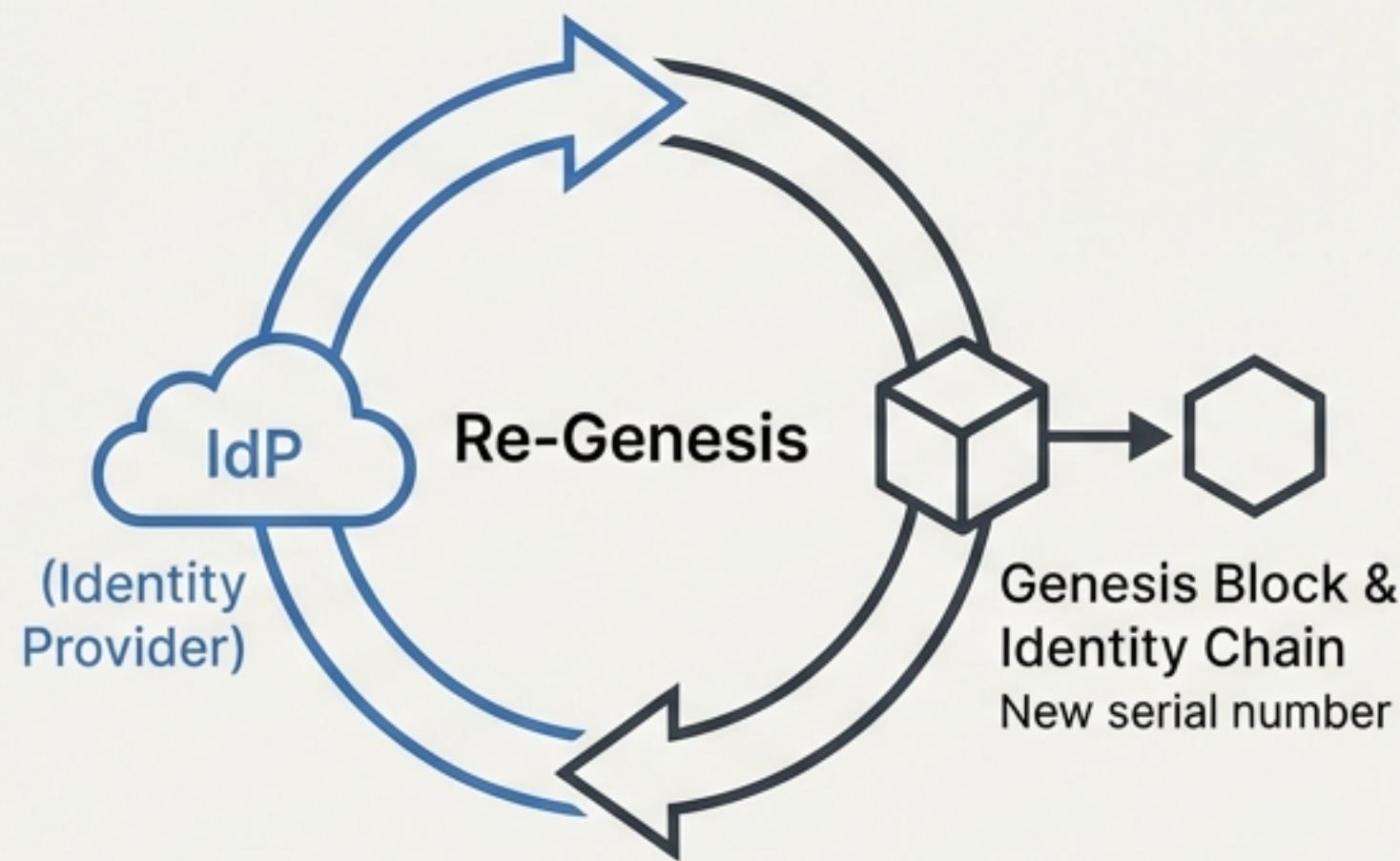


→ MAX_DELTA LIMIT

Para clonar, o atacante precisa de todos os fatores simultaneamente:
IdP + PIN + Biometria Viva + Histórico completo.

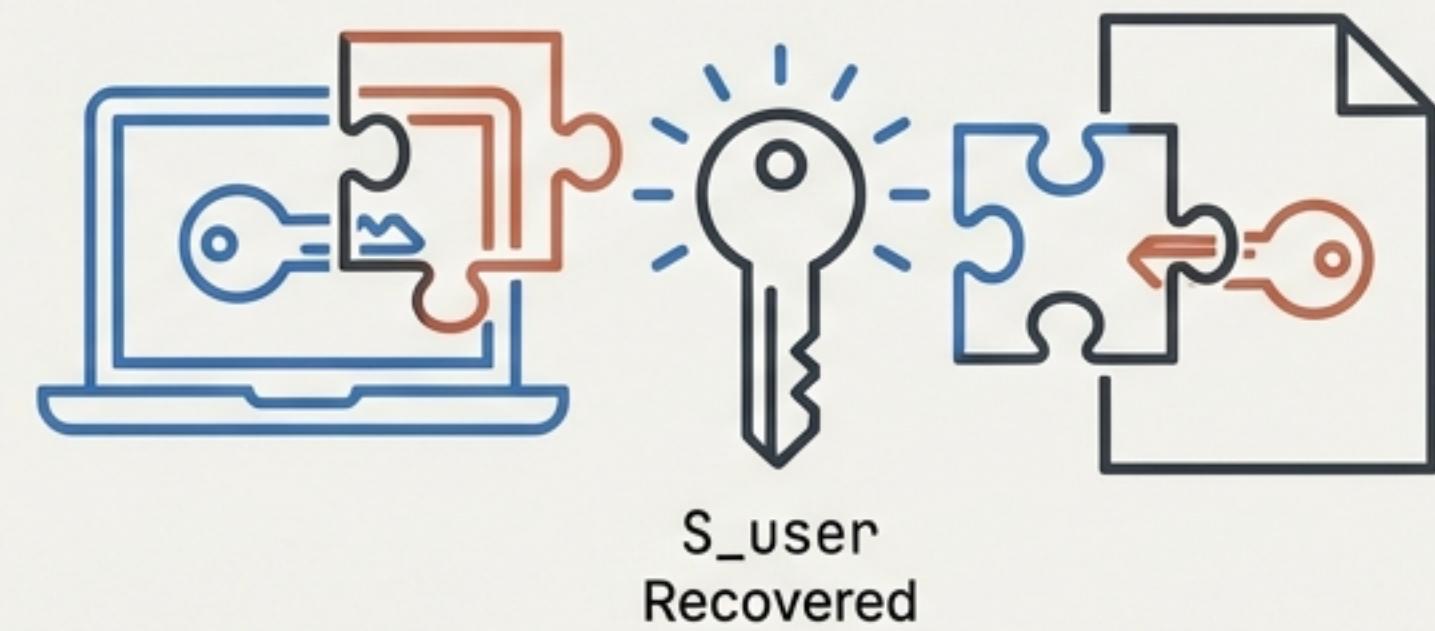
Estratégias de Recuperação e Resiliência

v1-Assisted (Re-Genesis)



Perda do dispositivo = Reinício da cadeia.
O usuário realiza nova validação no IdP
(Genesis) e cria uma nova Identity Chain
vinculada ao mesmo user_id lógico.

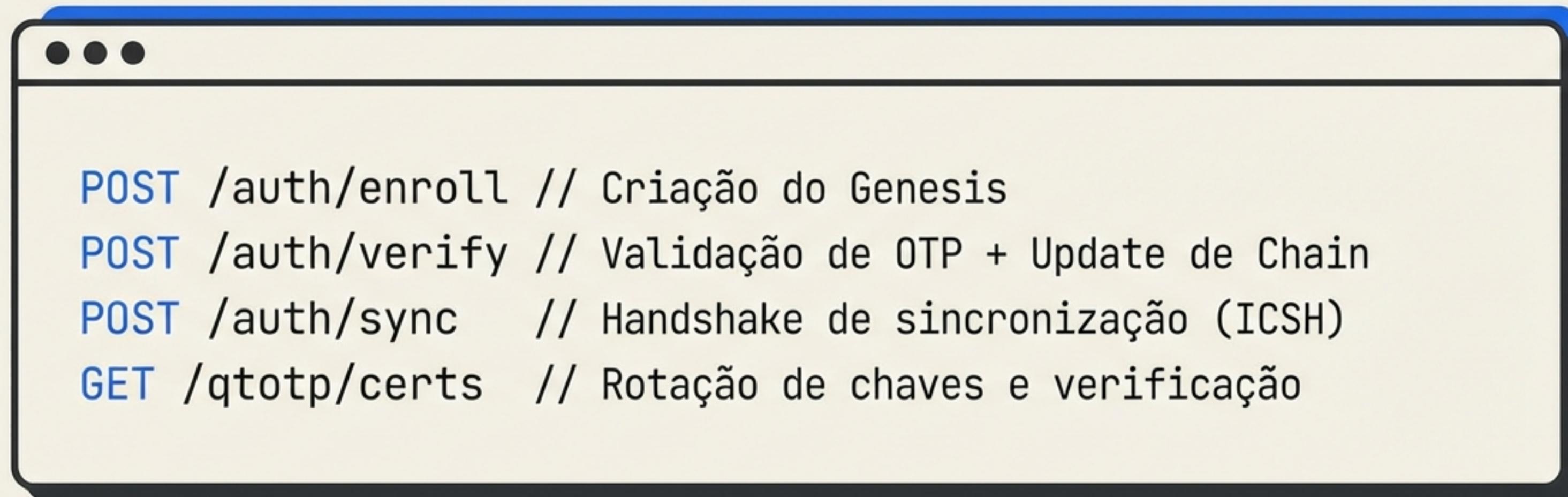
v2-Reconstitution



O usuário recupera o acesso combinando
fragmentos restantes (ex: Notebook + Backup
em Papel). Permite restaurar o S_user sem
reiniciar a cadeia do zero.

Especificações e APIs (Ready to Build)

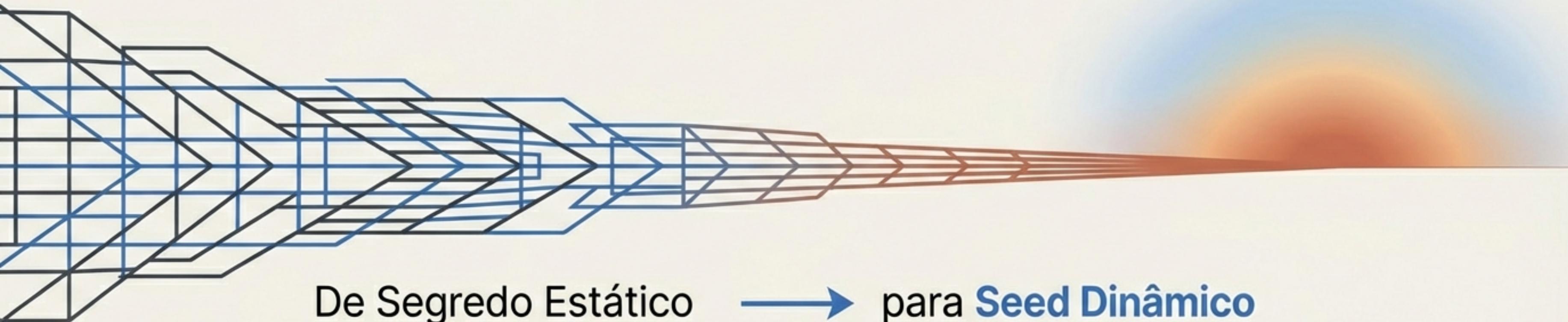
Draft de Protocolo Aberto



Security Recommendations: SHA-256, HMAC-SHA-256, Ed25519 Signatures.

O Futuro da Autenticação Temporal

O Q-TOTP é a primeira versão definitiva de um protocolo que une biologia e criptografia temporal.



Implemente o Core. Escolha seu Modo (v1/v2). Contribua.