

PAULO JOSÉ ELIAS MANZANO

**INTEGRAÇÃO DE MECANISMOS MODERNOS DE AUTENTICAÇÃO
(PASSKEYS/WEBAUTHN + MPC) AO ECOSISTEMA STELLAR**

PAULO JOSÉ ELIAS MANZANO

**INTEGRAÇÃO DE MECANISMOS MODERNOS DE AUTENTICAÇÃO
(PASSKEYS/WEBAUTHN + MPC) AO ECOSISTEMA STELLAR**

Proposta de projeto apresentada ao departamento responsável da **Stellar Development Foundation** para solicitação de **grant de inovação**, com o objetivo de desenvolver, padronizar e implementar um novo método de autenticação baseado em Passkeys (WebAuthn/FIDO2) e Multi-Party Computation (MPC) no ecossistema Stellar.

Esta proposta apresenta o desenvolvimento de um novo padrão de autenticação para o ecossistema Stellar, integrando Passkeys (WebAuthn/FIDO2) e MPC (Multi-Party Computation). O objetivo é substituir processos inseguros baseados em seed phrases por métodos modernos amplamente adotados por navegadores e dispositivos móveis. O projeto inclui desenvolvimento do SEP-XX, implementação de referência em Java e JavaScript, integração ao SDK oficial e auditoria de segurança. O prazo total estimado é de 7 meses, com orçamento entre **USD 180.000 e USD 240.000**. Este projeto fortalece segurança, usabilidade e competitividade da rede Stellar, promovendo adoção institucional e melhoria significativa da experiência do usuário.

1. Resumo

Esta proposta apresenta um projeto de inovação voltado à implementação de um novo método de autenticação no ecossistema Stellar, baseado em Passkeys (WebAuthn/FIDO2) e MPC (Multi-Party Computation). A iniciativa propõe a modernização da autenticação utilizada por aplicações Stellar, reduzindo dependência de seed phrases, aumentando a segurança criptográfica e oferecendo uma experiência de usuário simplificada, suportada nativamente por navegadores e dispositivos móveis.

O projeto prevê:

- a) criação de um novo padrão técnico (SEP-XX),
- b) desenvolvimento de implementações de referência em Java e JavaScript,
- c) integração do método diretamente no Stellar SDK,
- d) testes, documentação e auditoria de segurança.

O objetivo é entregar um padrão seguro, auditável, escalável e pronto para adoção oficial no ecossistema Stellar.

2. Justificativa

A autenticação atual utilizada pelo ecossistema Stellar é baseada principalmente no SEP-10, que depende de assinaturas Ed25519 diretas — modelo adequado à época de sua criação, mas limitado para os padrões modernos de segurança digital.

Os principais desafios atualmente observados incluem:

- dependência de seed phrases, que representam alto risco de perda ou comprometimento;
- ausência de autenticação biométrica nativa;
- falta de integração com padrões modernos de segurança amplamente aceitos (FIDO2/WebAuthn);
- aumento global de ataques envolvendo phishing, fraudes e comprometimento de chaves privadas;
- necessidade de aprimorar a experiência de novos usuários, especialmente em dispositivos móveis.

A integração de Passkeys e MPC representa uma evolução natural para o ecossistema Stellar, permitindo:

- autenticação sem necessidade de memorizar senhas ou seed phrases;
- uso de biometria nativa de dispositivos (Face ID, Touch ID, Windows Hello, Android Biometrics);
- maior segurança graças à descentralização da chave privada com MPC;
- compatibilidade direta com todos os navegadores modernos (Google, Microsoft, Apple).

Este projeto atende à necessidade atual da comunidade Stellar por soluções de autenticação mais seguras, acessíveis e padronizadas.

3. Objetivos

3.1 Objetivo Geral

Criar, implementar e propor para adoção oficial um novo padrão de autenticação no ecossistema Stellar, baseado em Passkeys/WebAuthn e MPC, incluindo documentação técnica, implementação de referência e atualização do Stellar SDK.

3.2 Objetivos Específicos

- Desenvolver a especificação técnica “SEP-XX: Stellar Passkey & MPC Authentication”.
- Criar fluxos formais de autenticação compatíveis com SEP-10, mantendo retrocompatibilidade.
- Desenvolver implementações de referência em:
 - Java (backend / autenticação servidor)
 - JavaScript (apps web, carteiras, dApps)
- Propor integrações diretas no Stellar SDK oficial.
- Realizar testes de integração, validação e segurança.
- Produzir documentação, tutoriais e guias técnicos para adoção.
- Obter feedback da comunidade e preparar submissão oficial ao Stellar Protocol.

4. Metodologia

O projeto será executado em quatro fases principais:

Fase 1 — Pesquisa e Definição

- Análise do SEP-10 existente
- Estudo comparativo de padrões FIDO2/WebAuthn
- Estudo de MPC compatível com Ed25519
- Definição de fluxos e arquitetura

Fase 2 — Especificação SEP-XX

- Redação completa da especificação técnica
- Regras formais para challenge/response
- Definição dos formatos de mensagem
- Estratégias de mapeamento entre credencial WebAuthn e Conta Stellar
- Revisão e discussão com comunidade

Fase 3 — Implementação Técnica

- Desenvolvimento de SDK em JavaScript e Java
- Criação de exemplo funcional (dApp demo + backend demo)
- Integração com WebAuthn em navegadores
- Integração com provedores MPC (quando aplicável)

Fase 4 — Testes, Auditoria e Documentação

- Testes unitários e de integração
- Auditoria externa de segurança
- Redação de documentação oficial, tutoriais e guias
- Preparação para submissão ao Stellar Development Foundation

5. Cronograma

Fase	Atividades	Duração
Fase 1	Pesquisa e definição técnica	1 mês
Fase 2	Especificação SEP-XX	1 mês
Fase 3	Implementação SDK + demos	3 meses
Fase 4	Testes, auditoria e documentação	2 meses
Total	—	7 meses

6. Recursos Necessários

6.1. Recursos Humanos

- 1 Arquiteto de Software
- 2 Desenvolvedores (Java e JavaScript)
- 1 Especialista em Segurança Criptográfica
- 1 Redator técnico

6.2. Infraestrutura

- Ambientes de teste e CI/CD
- Servidores cloud para prototipagem
- Hardware para testes de autenticação (YubiKey, Smartphones, etc.)

6.3. Serviços e Auditorias

- Auditoria externa de segurança (recomendada para adoção oficial)

6.4. Valor Total Solicitado

Categoria	Total Estimado (USD)
Recursos Humanos	127.000 – 189.000
Infraestrutura	5.500 – 10.000
Auditoria	20.000 – 60.000
Documentação Final	4.000 – 8.000
Total Geral Estimado	156.500 – 267.000

7. Resultados Esperados

- Um novo método de autenticação moderno, seguro e escalável.
- Inclusão do novo padrão no Stellar Ecosystem Proposals (SEP).
- Exemplos de referência completos para comunidade e empresas.
- Redução do risco associado ao uso de seed phrases.
- Aumento da adoção institucional da rede Stellar.

- Melhoria na experiência de usuário e acessibilidade.
- Inovação na camada de autenticação, tornando Stellar mais competitiva no cenário global.

8. Considerações Finais

A integração de Passkeys/WebAuthn e MPC representa um avanço estratégico para o ecossistema Stellar, oferecendo segurança de nível empresarial, usabilidade moderna e compatibilidade global com fabricantes e sistemas operacionais.

Este projeto está alinhado às diretrizes de inovação, segurança e acessibilidade promovidas pela Stellar Development Foundation e representa um passo importante para evolução da plataforma.

Solicitamos avaliação e apoio financeiro para execução completa do projeto, com compromisso de transparência, colaboração com a comunidade e entrega de resultados de alto impacto para o ecossistema.