

# Mellon — Keep Your Secrets

Innovative, Open-Source Password Manager for the Post-Quantum Era Aligned with GDPR, OWASP, WCAG and Portugal's National Strategy for Cyberspace Security



# What is Mellon?



## Password management

A next-generation, open-source tool that combines technical innovations like zero-knowledge local-first architecture, end-to-end encryption, and adaptive security with user-first design

## Core Value

Built to counter today's cyber threats, tomorrow's quantum challenges and empower users with control over their digital security and sensitive data

## Goal

To establish a market-leading solution that scales from individual users to enterprises leveraging free and paid tiers as well as dual-licensing model

# Market Opportunity

Mellon is uniquely positioned to capture both individual and SME segments

**28%**

## Market growth

On European password management market in 2019–2024 according to the [Mordor Intelligence report](#)

**27.5%**

## CAGR

Global market forecasted at most, reaching \$8B by 2030 according to the same report

**7.75%**

## Market growth

Projected in Portugal, reaching \$239M by 2029 according to the [Statista forecast](#)

**25%**

## Password management usage

Comparing to indirect competitors like digital and paper notes, memorisation and build in browser storage



## Key Technical Innovations

### **Open-source codebase**

Full codebase transparency and community-driven development to establish trust

### **AI-driven security**

Adaptive behaviour based on user's common patterns and current context to detect threats and response in real-time

### **Local-first architecture**

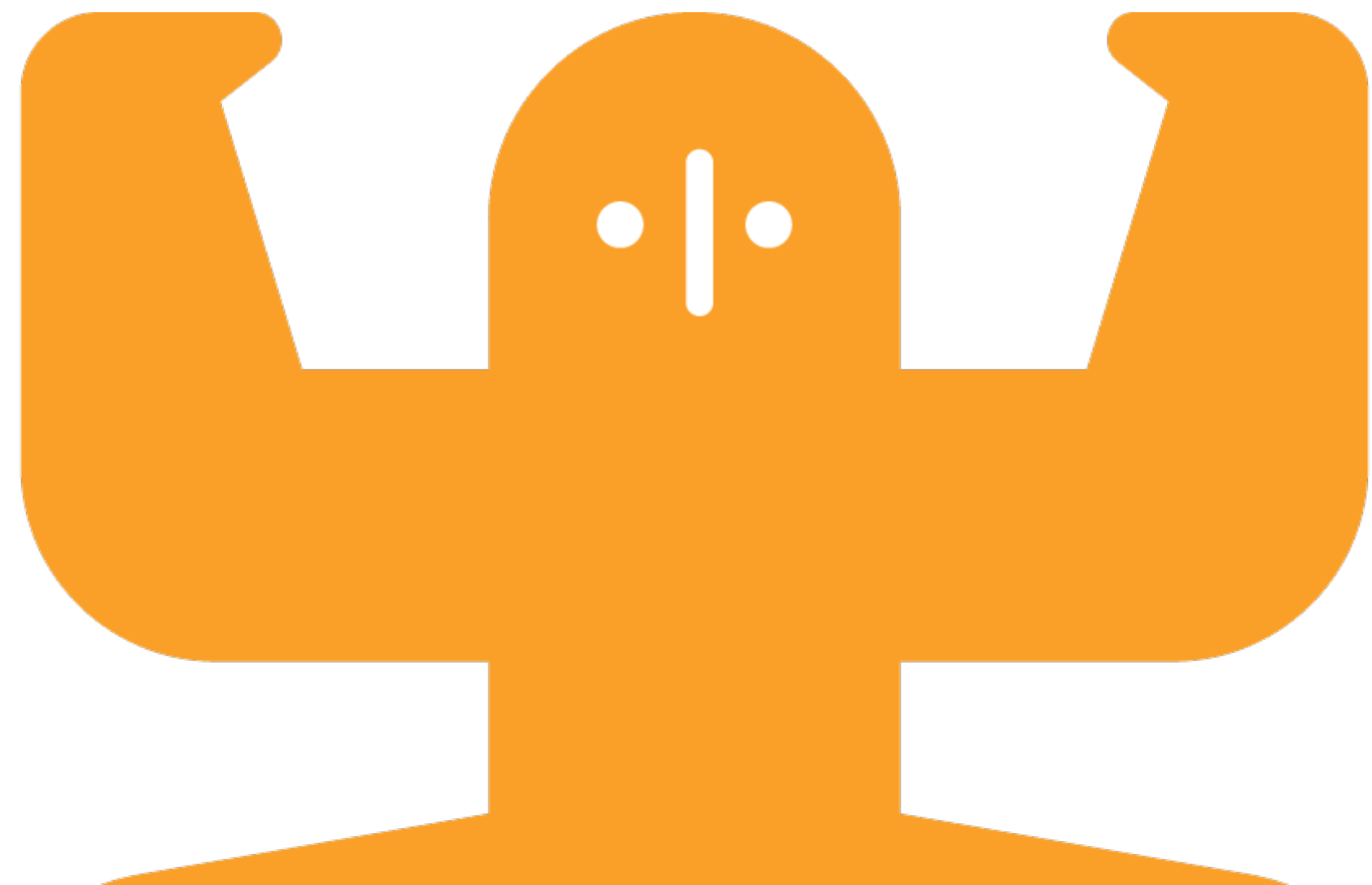
With offline capability, end-to-end encryption and seamless cross-device synchronization with CRDT mechanism

### **Advanced security**

Incorporating passwordless authentication, zero-knowledge design, biometric authentication, emergency access and many other features

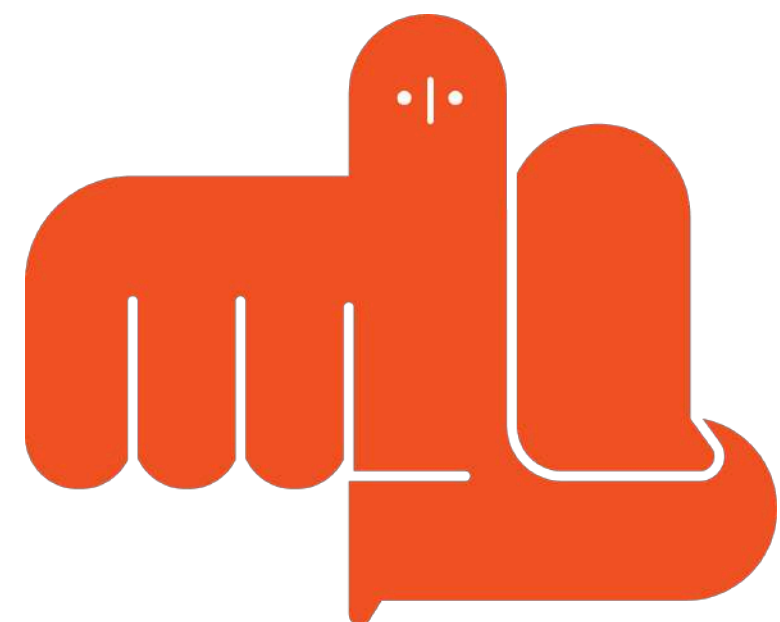
# Competitive Edge

Missing in all the currently presented solutions



Post-quantum cryptography algorithms standardized by US National Institute of Standards and Technology. Kyber, Dilithium and SPHINCS+ prepared for quantum computing threats to current encryption methods

# Competitive Differentiation



## Market Gaps Addressed

Overcomes usability, transparency and functionality issues in current solutions: Bitwarden, LastPass, 1Password, etc

## Unique Selling Points

Transparent, sustainable, simple and decentralised secret management where users controls all the data

## Various Pricing

Several paid tiers and unique dual-licensing model allowing free self-hosting and community development with premium enterprise features

## Corporate Features

Seamless cross-platform synchronization and real-time sharing and collaboration

# Subscription Tiers

Tailored to stand away from the competitors yet to thrive financially targeting both B2C and B2B markets

**VISA**



**PayPal**



**€4/month**

Individual Cloud  
Subscription

**€100/month**

Corporate Contracts  
and Subscription Flat  
Rate

**€10/month**

Family Bundle

**Individual**

Dedicated self-hosted  
options for enhanced  
privacy and isolation



## Revenue Streams

Based on our financial model  
by year 5

**€148,000**

Individual and Family  
Subscriptions

**€126,000**

Corporate Contracts

**€78,000**

Corporate  
Subscriptions

**39,000**

Active users out of  
256,000 total userbase



# Financial Outlook

**€352,000**

Year 5 turnover

**€365,000**

Year 5 asset valuation

**10 positions**

Opened to hire high-qualified specialists in first two operational years

**10-20%**

Of turnover allocated to marketing budget

**>1.0**

A break-even point of a return on investment ratio after year 5

**4,000**

Monthly acquired new users from various marketing channels

# Backed by Researches

Made by Mordor Intelligence, Security.org, Statista, Nucamp, Grand View, Fortune Business Insights and us.

Product	Open Source	Passkey Synchronisation	Token Generation	Local-first	Global Security Standards	Post-quantum cryptography	Accessibility Features	End-to-End Encryption
Bitwarden	Yes	Supports cross-platform synchronization of passwords and passkeys through cloud storage; users can also opt for self-hosting to manage synchronization. <a href="#">Wikipedia</a>	Offers TOTP generation for 2FA; integrates with authenticator apps like Authy and Google Authenticator. <a href="#">Tom's Guide</a>	Primarily cloud-based; requires internet connection for synchronization, but local access to stored passwords is available offline. <a href="#">Wikipedia</a>	Compliant with HIPAA, GDPR, CCPA, SOC 2, SOC 3, and the EU-US and Swiss-US Privacy Shield frameworks. <a href="#">Wikipedia</a>	No information available, probably — not	Yes	Yes
LastPass	No	Provides cloud-based synchronization of passwords across devices; does not specifically mention passkey synchronization. <a href="#">Tom's Guide</a>	Supports TOTP for 2FA; integrates with various authenticator apps, including its own LastPass Authenticator. <a href="#">Tom's Guide</a>	Primarily cloud-based; offers offline access to stored passwords, but certain features may require internet connectivity. <a href="#">Tom's Guide</a>	Compliant with GDPR and CCPA; adheres to industry-standard security practices. <a href="#">Tom's Guide</a>	No information available, probably — not	Yes	Yes
Proton Pass	Only clients	Offers synchronization of passwords and passkeys across devices through end-to-end encrypted cloud storage. <a href="#">It's FOSS</a>	Supports TOTP for 2FA; integrates with authenticator apps for generating time-based one-time passwords. <a href="#">It's FOSS</a>	Designed to function offline with local access to stored passwords; synchronization features require internet connectivity. <a href="#">It's FOSS</a>	Compliant with GDPR; employs end-to-end encryption to ensure data privacy. <a href="#">It's FOSS</a>	No information available, probably — not	Yes	Yes
Keeper Password Manager	No	Supports synchronization of passwords and passkeys across devices through encrypted cloud storage. <a href="#">Wikipedia</a>	Offers TOTP generation for 2FA; integrates with various authenticator apps and supports hardware-based security keys. <a href="#">Wikipedia</a>	Primarily cloud-based; provides offline access to stored passwords, with synchronization occurring when internet connectivity is available. <a href="#">Wikipedia</a>	Compliant with SOC 2, GDPR, and CCPA; utilizes AES-256 encryption combined with PBKDF2 encryption for data security. <a href="#">Wikipedia</a>	No information available, probably — not	Yes	Yes
Dashlane	No	Provides cloud-based synchronization of passwords across devices; does not specifically mention passkey synchronization. <a href="#">TechRepublic</a>	Supports TOTP for 2FA; integrates with various authenticator apps to enhance account security. <a href="#">TechRepublic</a>	Primarily cloud-based; offers offline access to stored passwords, with certain features requiring internet connectivity. <a href="#">TechRepublic</a>	Compliant with GDPR and CCPA; employs industry-standard security measures to protect user data. <a href="#">TechRepublic</a>	No information available, probably — not	Yes	Yes
Okta	No	Focuses on identity and access management; does not provide traditional password management or passkey synchronization features. <a href="#">GingerSec</a>	Offers robust 2FA and multi-factor authentication solutions, including support for TOTP, push notifications, and hardware tokens. <a href="#">GingerSec</a>	Cloud-based service; requires internet connectivity for authentication and access management functions. <a href="#">GingerSec</a>	Compliant with various global security standards, including SOC 2, ISO 27001, and GDPR; provides enterprise-grade security solutions. <a href="#">GingerSec</a>	No information available, probably — not	Yes	Yes
Google Authenticator	No	Does not support passkey synchronization; designed solely for generating 2FA codes on a single device.	Generates TOTP-based 2FA codes for various accounts; does not offer additional 2FA methods.	Functions entirely offline; does not require internet connectivity to generate 2FA codes.	Not detailed.	No information available, probably — not	Yes	No
Password Safe and Manager	No	Provides encrypted cloud-based synchronization for passwords across devices	Does not natively support 2FA token generation	Supports offline access to locally stored passwords; sync requires internet	AES-256 encryption; no explicit compliance info	No information available, probably — not	No	Yes
Twilio Authy Authenticator	No	Synchronizes 2FA tokens via encrypted cloud services	Generates TOTP codes and supports push notifications	TOTP works offline; sync requires internet	SOC 2, GDPR compliant	No information available, probably — not	No	Yes
1Password	No	Synchronizes passwords and passkeys through encrypted cloud storage	Generates TOTP codes	Allows offline access to stored passwords; sync requires internet	SOC 2, GDPR, and CCPA compliant	No information available, probably — not	Yes	Yes

## Competitors and Market Analysis

Shows how we stand from other solutions in features, pricing, principles and market strategy

Month	Product milestones	Marketing milestones	B2C Turnover	Subscriptions	Contracts	B2B Subscriptions	Expenses	Taxes	Marketing	Salaries	IT Infrastructure	Saldo	Month retention	Quarter retention	Year retention	Viral
1 (August 2025)	Password generator launch	Contacts form launch	0	0	0	0	45	0	0	0	45	-45	0%	0%	0%	
2	Basic password management 2 features launch	Announcement in founders social networks. Email campaigns setup	0	0	0	0	20	0	0	0	20	-20	5%	0%	0%	
3	2FA TOTP generator launch	SEO blog launch. Universities partnerships preparations: internships, courses, practices and collaborative qualification works	0	0	0	0	220	0	200	0	20	-220	6%	0%	0%	
4	Initial security audit and open-sourcing the codebase	Products social networks launch. Initial advertisement test to verify conversion rates	0	0	0	0	1220	0	1200	0	20	-1220	10%	4%	0%	
5	GitHub Actions and other 5 automations set up	Dual-licensing model for commercial usage activation and template contract publishing. Announcements on sites like Product Hunt or AppSumo	0	0	0	0	1240	0	1200	0	40	-1240	10%	5%	0%	
6 (January 2026)	Local-first web client and secrets synchronization launch	Partnerships with first open-source communities like open source alternative lists or self-host enthusiasts	200	0	200	0	286	46	200	0	40	-66	12%	6%	0%	
7	End-to-end encryption launch	Partnerships with local-first development communities	300	0	300	0	309	69	200	0	40	-9	14%	7%	0%	
8	Debit and credit card payments integration. Paid monthly subscription launch	Partnerships with security open source communities like OpenPrivacy or PrivacyTools.io	400	0	400	0	332	92	200	0	40	68	16%	7%	0%	
9	MEWay, PayPal and Multibanco integration. Yearly plan launch	Test marketing campaigns on individuals with open source, transparency, and community audits value propositions	616	116	500	0	1382	142	1200	0	40	-766	18%	8%	0%	
10	Subscription pause and resume, promo codes launch	Test marketing campaigns on individuals with local-first and EZE encryption value propositions	736	136	600	0	1409	169	1200	0	40	-673	16%	9%	0%	
11	Backup encryption and Shamir's Secret Sharing for account recovery launch	Press-kit publishing, initial media publications in outlets like Público or Codrops. First summer sales	1124	324	800	0	498	258	200	0	40	625	18%	9%	0%	
12	zk-SNARK incorporation for server auth and validations	Community building on forums like Reddit and Zwame	1213	313	900	0	519	279	200	0	40	694	20%	9%	0%	
Sum for a year			4588	888	3700	0	7480	1055	6000	0	425	-2892				

## Financial Model

Aligned with product, marketing and hiring strategies to achieve estimated turnover, assets values and future sustainable growth



# Founding Team Highlights



Vladimir Lazarev

Tech leader scaled teams up to 50 engineers  
and building products for 20kk MAU  
7 years of engineering and management  
experience



Sofia Azzheurova

UX/UI visionary with a track record of  
boosting conversion rates with creatives  
5 years of digital design experience



Evgenii Antonenkov

Performance marketing expert driving  
effective digital strategies with \$1M-\$2.2M  
annual budgets  
6 years of digital marketing experience

## Combined Strengths

Deep technical expertise, strategic vision,  
and proven market execution

Prior international experience and a commitment  
to building a robust, secure product

# Incubation Fit

## Why Portugal?

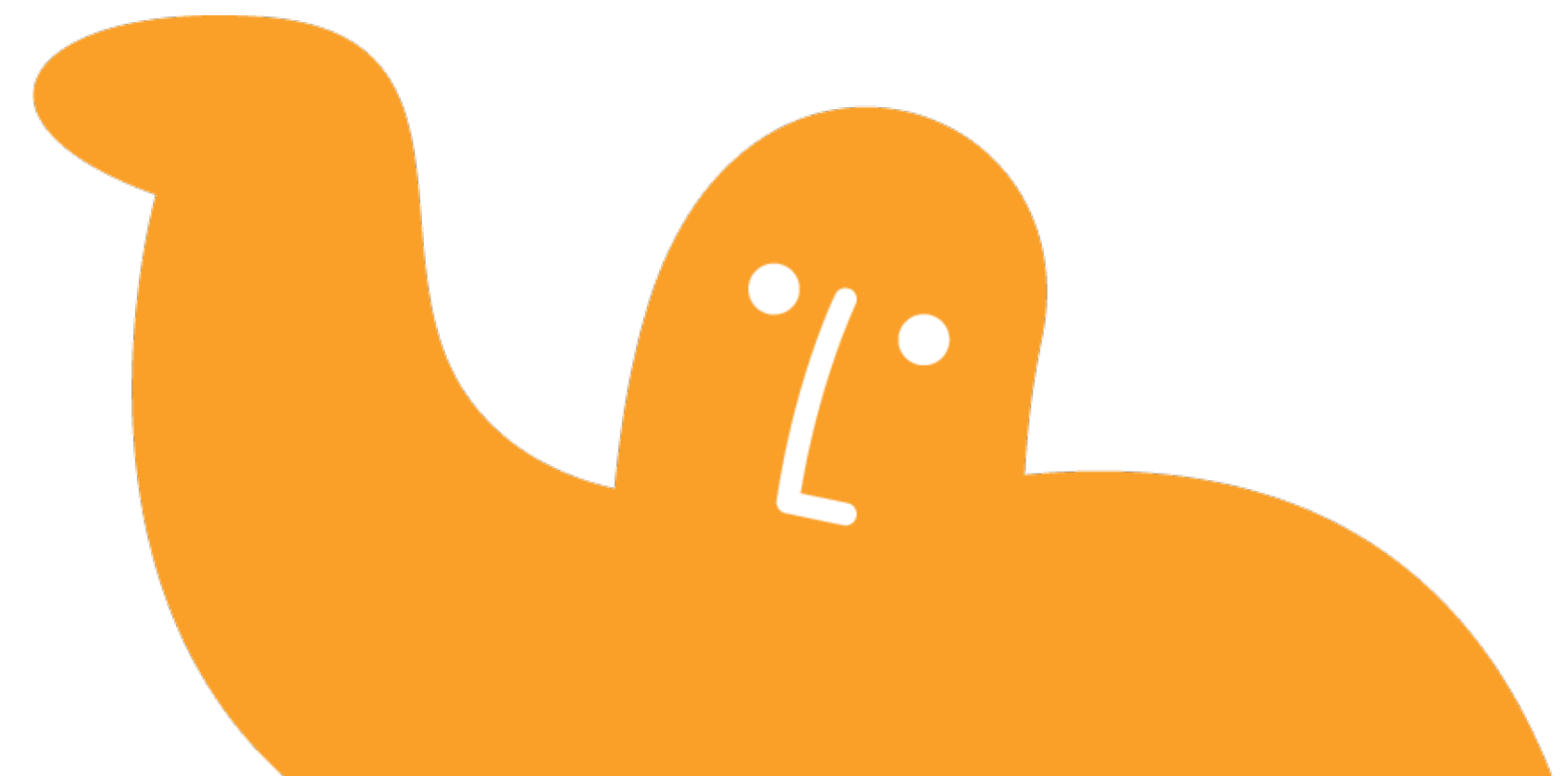
- Thriving startup ecosystem with strategic government and legal support like "Law no. 21/2023"
- Incubators providing a fertile environment for innovation

## Incubator Partnership

- Leveraging legal advisory, office space, and professional events
- Gates into local networks for partnerships, collaboration with universities and talent acquisition

## Our Commitment

- Self-funding initial development, validated prototypes, and clear milestones to achieve post-incubation acceleration



# Nearest Milestones

## Incubation Q1

Basic feature development, blog launch, early user testing

## Incubation Q3/Q4

Final product refinement, company registration and launch



## Pre-Incubation

Prototype and hypothesis validation, initial documentation

## Incubation Q2

Scaling product features, initiating B2B discussions, Security audit and open-source release

## Break-Even & Growth

Focus on sustainable growth with clear B2C/B2B acquisition strategies

Detailed technical roadmap and clear user acquisition KPIs are represented in the financial model.

# Let's build the future of digital security together

Please, support and incubate Mellon for one year to scale our secure, innovative solution.

Contact Vladimir for further discussion:  
[laidrivm@gmail.com](mailto:laidrivm@gmail.com)



[Find out more about Mellon](#)