The Sovereign Communication & Digital Fiat Ecosystem

A MiCA-Compliant Whitepaper and Strategic Proposal

Version 19.0

April 2026

Table of Contents

Important Notice & MiCA Disclaimer

This whitepaper is provided for informational purposes only. Prospective purchasers of the Securcoin (SMS) token must read this notice carefully before making any decision.

Regulatory Status

In accordance with Article 5(5) of Regulation (EU) 2023/1114 (MiCA), please be advised that: **This crypto-asset white paper has not been approved by any competent authority in any Member State of the European Union.** The issuer, Securmeet, is solely responsible for the content of this crypto-asset white paper.

Risk of Loss and No Guarantee of Value

The purchase of crypto-assets involves a high degree of risk. The market price of the SMS token may decline and could become worthless. This crypto-asset is not covered by the investor compensation schemes under Directive 97/9/EC nor by the deposit guarantee schemes under Directive 2014/49/EU.

Right of Withdrawal for Consumers

In accordance with Article 13 of MiCA, if you are acquiring SMS tokens as a consumer, you have a 14-calendar-day period during which you may withdraw from the agreement to purchase without incurring any fees or costs and without being required to provide a reason.

The withdrawal period begins on the day you give your consent to be bound by the purchase agreement. To exercise this right, you must notify Securmeet of your decision to withdraw before the period expires. The procedure for exercising this right is available on our official website.

Executive Summary

The Vision

We are creating the world's first unified platform for **sovereign communication.** In a world of escalating data regulation and digital security threats, the market urgently needs a single solution that combines unbreakable, self-hosted communication with a sustainable, utility-driven economic model.

The Opportunity

This platform solves critical, billion-dollar problems for regulated industries like finance, government, and critical infrastructure. New EU regulations (NIS2, DORA) now make executives personally liable for cybersecurity and operational resilience failures, creating an urgent, board-level need for our solution. Our unique, sovereign architecture provides a powerful moat, making us the only viable choice for high-value clients who cannot compromise on security and data control.

The Ask

This document serves as the MiCA-compliant whitepaper for the Securcoin (SMS) utility token and outlines our strategic proposal. We are raising a **$5 million strategic round** to fund ecosystem growth and accelerate our market entry to capture a clear first-mover advantage.

Part I: The Strategic Problem

A Market in Crisis

1.1 The End of Trust in Centralized Architectures

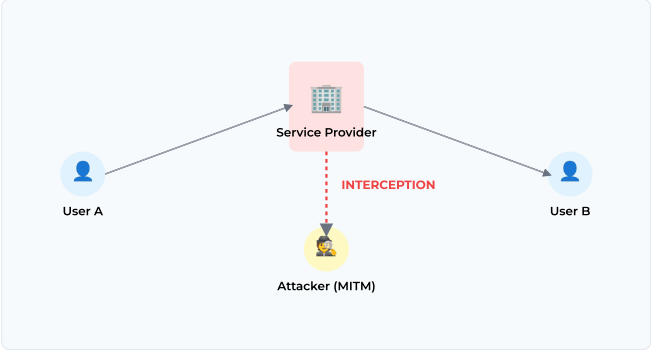
The foundational model of modern cloud software—where user data is processed and stored on servers controlled by a third-party provider—is fundamentally broken for high-security use cases. This centralized model creates a single, high-value target for state-sponsored attackers and a single point of legal pressure for government agencies. As evidenced by a continuous stream of data breaches, any architecture that requires trust in the provider is an architecture that will eventually fail.

1.2 Geopolitical Realities and the Mandate for Digital Sovereignty

The geopolitical landscape has made data locality and control a matter of national and economic security. Digital sovereignty is not merely about where data is stored; it is the absolute control over the entire digital infrastructure—hardware, software, and data—without dependence on foreign entities whose legal frameworks may conflict with an organization's interests. Legislation such as the U.S. CLOUD Act creates an untenable threat to this sovereignty. For European governments and critical industries, relying on such providers is no longer a viable option.

1.3 The Problem Visualized: The Man-in-the-Middle

Even with encryption, centralized services act as a mandatory intermediary. All communication flows through their servers, creating an unavoidable vulnerability. A compromised provider, whether through technical breach or legal compulsion, becomes a "Man-in-the-Middle" (MITM), capable of intercepting and logging communications. This structural flaw is unacceptable for any organization handling sensitive information.



1.4 The Deepfake Dilemma: A Crisis of Digital Trust

The proliferation of sophisticated, AI-generated "deepfakes" presents an existential threat to digital communication. Malicious actors can now create highly convincing fake audio and video, making it trivial to impersonate executives and government officials. This creates a crisis of trust where the need for a communication platform with unforgeable, cryptographically-verifiable identity is no longer a luxury; it is a necessity.

Part II: The Unified Solution

A New Paradigm: The Utility Flywheel

Our solution is a simple, powerful economic loop that connects real-world utility to a sustainable token economy. This "Utility Flywheel" is our core strategic advantage.

Step 1: The Sovereign Platform

First, we solve the foundational problem of trust by providing clients with the Securmeet communication platform. This is a secure, on-premise "digital vault" where high-value collaborations happen with absolute privacy. This is the bedrock upon which all future value is built.

Step 2: Fiat Revenue & Optional SMS Utility

Clients pay for services in traditional fiat currency (e.g., USD, EUR), creating a stable revenue stream. To create tangible utility for the SMS token, clients are offered the option to pay their service fees directly in SMS tokens at a discount, providing a direct economic benefit for acquiring and using the token.

Step 3: Buy-Back & Burn

A significant portion of the fiat revenue is used to systematically buy SMS tokens from the open market. These tokens are then permanently burned, reducing the total supply. This creates a powerful deflationary mechanism that links platform revenue to token scarcity, completing the virtuous loop: **Platform Utility → Fiat Revenue → Token Burn.**

Part III: Deep Dive: The Sovereign Architecture

3.1 Core Principle: A Peer-to-Peer, Zero-Trust Foundation

Unlike platforms that route all data through centralized servers, Securmeet is built on a true peer-to-peer (P2P) architecture. This is our most fundamental differentiator. Using standard protocols like WebRTC, communication streams are established directly between participant endpoints. This minimizes the attack surface and provides structural privacy.

3.2 Cryptographic Implementation: E2EE and The Double Ratchet

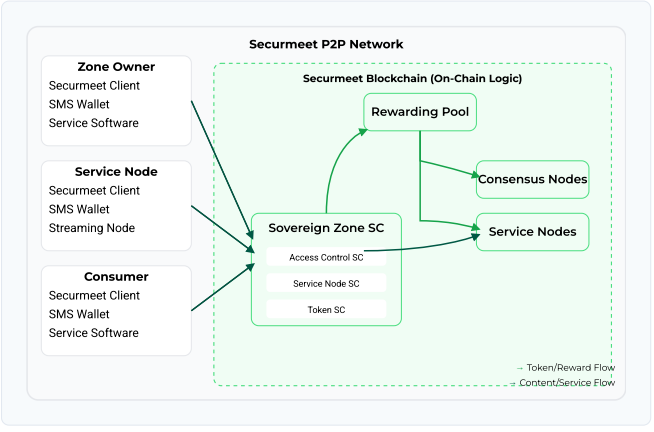
Mandatory, non-negotiable end-to-end encryption is applied to every stream on the platform. Our cryptographic stack is built on open, publicly vetted, and robust standards, including the Double Ratchet Algorithm, pioneered by Signal, to provide perfect forward secrecy and post-compromise security.

3.3 The Securmeet Identity Layer: An Ethereum Layer 2 for Verifiable Trust

The decentralized identity services of the Securmeet platform are powered by a dedicated Ethereum Layer 2 (L2) network. To provide maximum security, scalability, and access to deep liquidity, the SMS token will be an **ERC-20 compliant token launched on the Arbitrum network.** This approach provides the best of both worlds: the security of Ethereum with the speed and low cost of a leading L2.

3.4 Ecosystem Architecture Diagram

The diagram below illustrates the high-level architecture of the Securmeet ecosystem. It shows how different user roles interact with the on-chain components and the underlying P2P network.

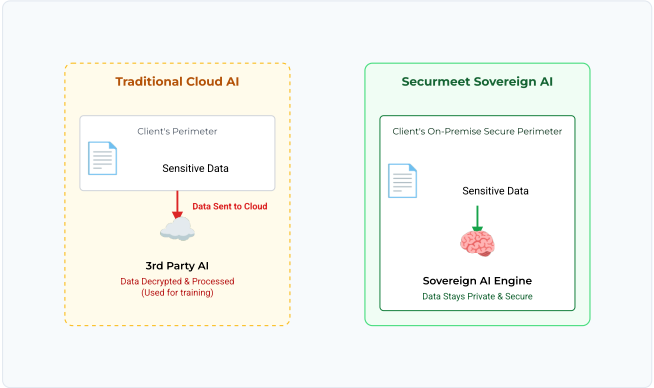


The Rewarding Pool is critical for ensuring the long-term health and decentralization of the network. To ensure its sustainability, the pool is funded through two primary mechanisms: **a 15% allocation from all Sovereign Zone transaction fees**, and a dedicated portion of the company's fiat revenues used to purchase SMS tokens from the open market. This dual-funding model creates a sustainable incentive for Service Node operators, aligning their success with the overall growth of the platform.

3.5 Sovereign AI: Intelligence Without Compromise

The use of Artificial Intelligence in enterprise settings creates a fundamental conflict with data privacy. Most AI services require data to be sent to their servers for processing, breaking any E2EE promise and exposing sensitive intellectual property.

Securmeet resolves this conflict with its **Sovereign AI model**. We provide clients with a powerful AI engine that is deployed as part of their on-premise installation. All AI processing happens entirely within the client's secure perimeter. Data is never sent to Securmeet or any other third party. This is the only architecture that allows organizations to leverage AI without violating the core principles of E2EE, data sovereignty, and the NIS2 directive.



Part IV: Deep Dive: Solving the NIS2 Compliance Challenge

The NIS2 Directive is not merely a set of recommendations; it is a legally binding framework that EU Member States must transpose into national law by October 17, 2024. This directive empowers national competent authorities to conduct audits, demand information, and impose severe penalties for non-compliance. This creates an urgent, board-level imperative for organizations to re-evaluate their entire digital infrastructure.

A central tenet of NIS2 is the security of the supply chain. For any "Essential" or "Important" entity, using a non-EU or centralized cloud provider for critical communications now represents a significant and documented supply chain risk. Securmeet's peer-to-peer, on-premise architecture is the definitive solution to this compliance challenge. By design, it removes the third-party provider from the communication supply chain entirely, giving management a clear, defensible, and technically superior answer to regulators.

Mapping Securmeet's Architecture to Key NIS2 Articles

NIS2 Directive Article	How Securmeet Provides the Solution
Article 20: Governance *Management bodies must approve and oversee cybersecurity measures and can be held liable for infringements.*	By implementing Securmeet, management can demonstrate they have taken decisive action. Deploying an on-premise, E2EE platform for critical communications is a clear, defensible measure that directly addresses the core of their responsibility, providing auditable proof of oversight.
Article 21(2)(d): Supply Chain Security *Entities must manage risks posed by their direct suppliers and service providers.*	This is Securmeet's most powerful differentiator. By removing the third-party cloud provider from the critical communication supply chain, Securmeet eliminates a massive and uncontrollable risk vector. The client's on-premise server is the only one involved, giving them full control.
Article 21(2)(h): Cryptography and Encryption *Entities must have policies and procedures on the use of cryptography and, where appropriate, encryption.*	Securmeet makes this straightforward. Encryption is not optional; it is mandatory and end-to-end for all communications. Our use of the modern, publicly-vetted Double Ratchet algorithm provides a state-of-the-art implementation that meets and exceeds the standard of "appropriate" measures.

Part V: Deep Dive: The Competitive Landscape

5.1 Centralized Cloud Providers (Microsoft, Zoom)

These platforms represent the incumbent model. Their centralized, non-sovereign architecture makes them fundamentally unsuitable for organizations requiring high security and NIS2 compliance.

5.2 Privacy-Focused Competitors (Wire, Threema)

These European companies represent our most direct competitors. While strong on privacy, their architecture is often federated, still relying on intermediary servers, which presents a larger attack surface than Securmeet's true P2P model. They also lack an integrated blockchain for verifiable identity or a comparable economic model to drive token utility.

5.3 The Web3 Contender (Telegram & The TON Blockchain)

Telegram, while popular, is not a true E2EE platform by default. It lacks the on-premise deployment, sovereign design, and enterprise-grade compliance features required by our target market.

5.4 The Securmeet Advantage: A Unified Sovereign Stack

The following table provides a clear comparison of Securmeet against incumbent and niche competitors across the features most critical for our target market of regulated and security-conscious enterprises.

Feature	Securmeet	Microsoft Teams / Zoom	Wire / Threema	Telegram
Core Architecture	**P2P & On-Premise**	**Centralized Cloud**	Federated / Centralized	**Centralized Cloud**
Data Sovereignty	**Absolute Client Control**	**Provider Controlled**	Partial (Federated)	**Provider Controlled**
Verifiable Identity	**Decentralized (On-Chain)**	**Centralized (Email)**	Centralized	**Phone Number Based**
Sovereign AI Model	**Yes (On-Premise)**	**No (Cloud-Based)**	N/A	N/A
Token-Driven Ecosystem	**Yes (SMS Utility Token)**	**N/A**	**N/A**	Consumer Crypto (TON)
Revenue-Based Burn	**Yes (Deflationary)**	**N/A**	**N/A**	**N/A**

Part VI: The SMS Utility Token

A MICA-Compliant Framework

6.1 Introduction: The Economic Engine of the Securmeet Ecosystem

The Securcoin (SMS) token is the native utility token that fuels the Securmeet ecosystem. The issuer of the SMS token is **SECURCOM INC, UNIPESSOAL LDA**, a limited liability company registered in Portugal (NIPC: 513930442).

6.2 Alignment with MiCA's Definition of a Utility Token

The SMS token is intentionally designed to fall within the definition of a "utility token" under Regulation (EU) 2023/1114 (MiCA). Specifically, it is a crypto-asset which is intended to provide digital access to a good or service, available on DLT, and is only accepted by the issuer of that token. Its primary purpose is **consumptive**—it is acquired to be used for accessing platform services, activating features, or receiving economic benefits such as discounts. It is not designed or promoted as a financial instrument for speculative investment.

6.3 The SMS Utility Framework: Driving Demand

The SMS token's core utility is to function as the exclusive mechanism for accessing services and receiving benefits on the Securmeet platform. To create true utility and drive demand, clients are offered a discount for paying for services directly in SMS tokens. While fiat payments are accepted for convenience, the economic incentive is designed to encourage the acquisition and use of SMS, creating a direct, quantifiable link between platform usage and token demand.

6.4 Token Holder Value & Protection

The Buy-Back and Burn Flywheel

The primary mechanism for managing the token's economic model is our **Buy-Back and Burn** program. This model creates a virtuous economic cycle that is directly fueled by real-world business activity:

Fiat Revenue: Securmeet generates stable revenue from enterprise clients paying for platform services in fiat currency.

Market Buy-Back: The Company commits to allocating **a minimum of 30% of its Gross Platform Revenue** to buying SMS tokens from the open market.

Permanent Burn: All tokens purchased through the buy-back program are permanently removed from circulation by sending them to an unrecoverable "burner" address.

This model creates deflationary pressure on the token supply, meaning that as platform adoption and revenue grow, the token supply decreases. This links the success of the Securmeet business to the scarcity of the SMS token. This is a feature of the ecosystem's design and not a promise of future profit or price appreciation.

6.5 Controlled Supply & Vesting

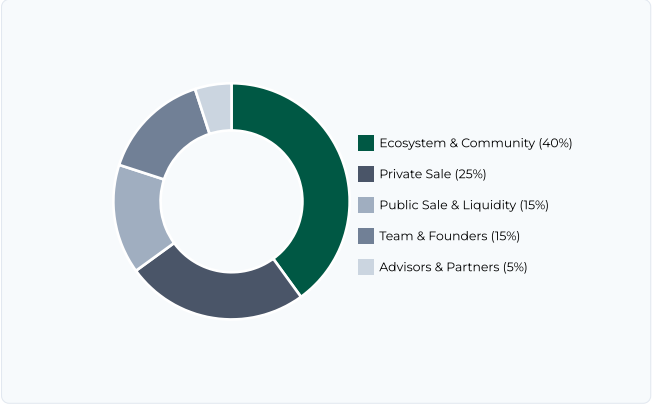
The vesting schedules for the team, founders, and advisors are specifically designed to prevent a post-launch "dump." The schedule features an initial **12-month lock-up period**, after which tokens are released linearly on a daily basis for the subsequent 24 months. This ensures a controlled and predictable release of the token supply without a "cliff" event that could create supply shocks.

6.6 Token Economics (Tokenomics)

The economic model for the Securcoin (SMS) token is designed for long-term sustainability. The smart contract will mint a fixed, non-inflationary total supply of **1,000,000,000 SMS**. This supply is final and cannot be increased.

Allocation & Distribution

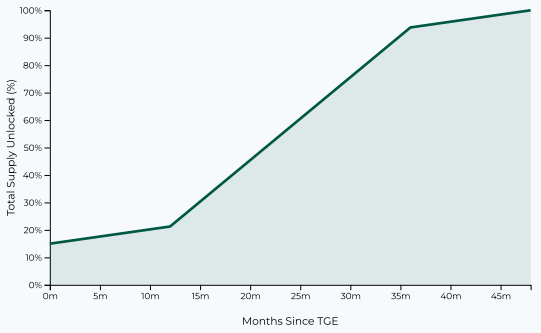
The total supply will be allocated to key areas to ensure the healthy growth and decentralization of the ecosystem. The current $5M strategic round represents a portion of the total 25% Private Sale allocation. The Fully Diluted Value (FDV) at this private sale price ($0.04) is $40M.



Allocation Category	Percentage	Purpose & Rationale
Ecosystem & Community Fund	40%	To catalyze a self-sustaining ecosystem. Funds are used for developer grants, community growth programs, liquidity incentives, and funding the sustainable rewards pool for network operators.
Private Sale (Seed & Strategic)	25%	Allocated to early strategic partners who provide critical initial capital. The vesting schedule ensures market stability post-launch.
Public Sale & Liquidity	15%	To provide initial liquidity on decentralized and centralized exchanges, ensuring a healthy and accessible market for the SMS token from day one.
Team & Founders	15%	To reward and retain the core team. The long vesting schedule (12-month lock, 24-month linear daily release) ensures long-term alignment with the project's success.
Advisors & Early Partners	5%	To compensate strategic advisors. The vesting schedule ensures they remain aligned with the project's medium-term goals.

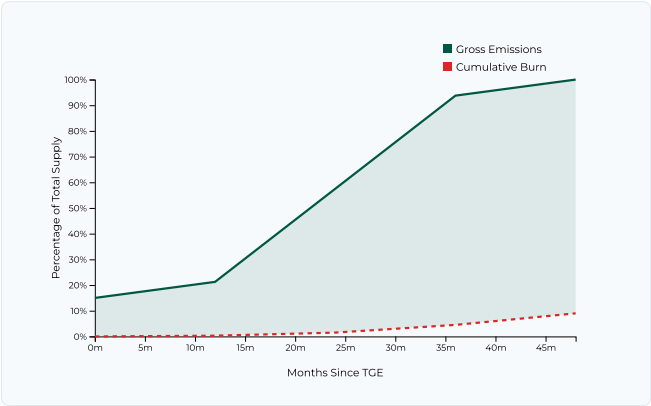
Vesting & Emission Schedule

A transparent and structured vesting schedule is crucial for market stability. The chart below illustrates the gross supply of tokens being unlocked over time (emissions), starting with the initial liquidity unlocked at the Token Generation Event (TGE).



Projected Net Circulating Supply (Emissions vs. Burn)

To fully understand the token's economics, the gross emission schedule must be viewed in conjunction with the **Buy-Back & Burn** model. The conceptual chart below shows the emission line offset by a projected deflationary line representing the tokens being permanently burned. As platform revenue grows, the rate of burn is projected to increase, creating a powerful net-deflationary pressure on the total circulating supply over the long term.



Part VII: Technical Implementation

The Smart Contract & Wallet Strategy

7.1 The SMS Token Smart Contract

The SMS token is a standard **ERC-20 compliant token** deployed on the **Arbitrum One** network. The contract is developed using industry-best-practice OpenZeppelin templates to ensure maximum security, transparency, and compatibility. Its source code will be publicly verified on Arbiscan, allowing anyone to review and audit the code.

7.2 Wallet Integration Strategy

Our strategy is to ensure seamless interaction for crypto-native users while completely abstracting away complexity for our enterprise clients.

For Individual Users: The Securmeet website will feature standard "Connect Wallet" functionality, ensuring compatibility with trusted wallets like **MetaMask, Trust Wallet, and hardware wallets.**

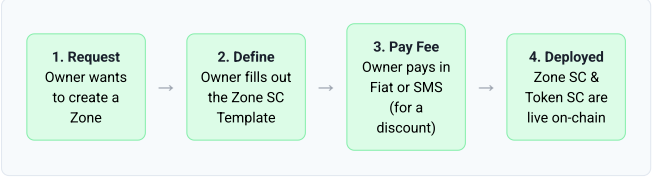
For Enterprise Clients: Enterprises will interact with Securmeet through a standard SaaS model, paying in fiat currency (e.g., EUR, USD). They will **not** be required to hold or manage crypto assets. The Buy-Back and Burn mechanism is an internal process funded by our fiat revenues, creating a seamless experience for our core customers.

Part VIII: Use Cases & Workflows

The following use cases illustrate how Securmeet becomes indispensable operational infrastructure and how each action translates into demand for the SMS token.

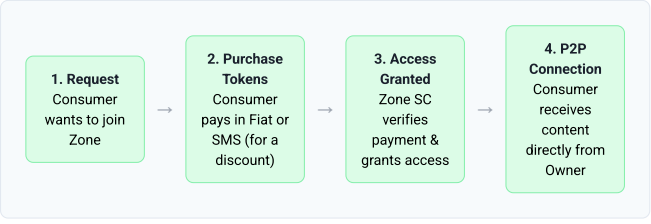
8.1 Workflow: Creating a Sovereign Zone

A "Sovereign Zone" is a private, on-chain space for communication. An Owner (e.g., a corporation) can create a Zone to share proprietary content with paying customers.



8.2 Workflow: Using a Sovereign Zone

A Consumer who wishes to access the content within a Sovereign Zone must purchase access tokens. This creates a direct economic link between the content's value and the platform's utility.



Tokenomics: When the consumer pays, the Zone's Smart Contract automatically distributes the SMS tokens: 85% goes to the Zone Owner, and 15% goes to the Securmeet Rewarding Pool. This entire transaction, whether initiated with fiat or crypto, drives demand for SMS tokens on the open market and is fundamental to the ecosystem's economy. Funding the Rewarding Pool is a direct investment in the network's health, which underpins the value and utility of every SMS token.

8.3 Workflow: Streaming Content via Service Nodes

For high-bandwidth content, Zone Owners can enable streaming via a decentralized network of Service Nodes. This allows for scalable, resilient content delivery while maintaining sovereign control.

Tokenomics & Node Incentives

The primary revenue driver for the Rewarding Pool will be fees generated from high-volume platform usage. Our financial models indicate that as the platform scales, the volume of fees flowing to the reward pool should ensure that operating a Service Node remains a profitable and attractive endeavor.

Modeling & Risks

These projections are based on internal scenario testing and financial modeling. However, they are subject to risks. The primary risk is slower-than-projected user adoption and transaction volume, which could impact the profitability for node operators in the early stages of the network. The sustainability of the rewards pool, funded from both transaction percentages and a portion of fiat-based enterprise revenue, is designed to mitigate this risk and ensure the network remains robust even during periods of slower growth.

Part IX: The Path Forward

9.1 Go-to-Market Strategy

Our go-to-market strategy is a highly targeted, multi-channel approach focused on acquiring high-value enterprise clients within our key verticals.

Target Customer Profiles:

Europe: Financial institutions, critical infrastructure operators, and government agencies directly impacted by NIS2.

USA: Large enterprises with complex supply chains and B2B payment needs.

Sales & Marketing Channels:

Direct Sales Team: An experienced enterprise sales team with deep relationships in the finance and cybersecurity sectors.

Strategic Partnerships: Partnering with leading cybersecurity consulting firms and systems integrators who advise our target clients on compliance and digital transformation.

Content Marketing & Thought Leadership: Publishing in-depth analysis and hosting webinars on digital sovereignty, MiCA compliance, and secure finance.

9.2 Product & Technology Roadmap

Phase 1: Foundation & Early Adopters (Q1-Q4 2026)

- Launch Securmeet core communication platform (On-Premise) for initial NIS2-focused enterprise clients in Europe.
- Internal Testnet deployment of the Securmeet Identity Layer (L2).
- Complete Seed & Strategic funding rounds for the SMS token.

Phase 2: Ecosystem & Market Expansion (Q1-Q4 2027)

- Mainnet launch of the Securmeet Identity Layer on Arbitrum.
- Initial DEX Listing (IDL) for the SMS token on Uniswap v3.
- Initiate global expansion of sales operations.

Phase 3: Advanced Features & Decentralization (2027+)

- Pursue listings on major centralized exchanges to enhance liquidity and accessibility, subject to meeting the exchanges' volume, compliance, and community size requirements.
- Launch Sovereign AI module for on-premise deployment.
- Begin R&D and integration of Zero-Knowledge Proofs (ZKPs) for private verification.
- Launch the Securmeet Ecosystem Council for decentralized governance.

Part X: The Leadership Team

The success of Securmeet is driven by a team of seasoned executives with deep expertise across enterprise technology, decentralized systems, product design, and client services.

Pavol Cvengroš

Chief Technology Officer (CTO)

Co-founder of SecurCom Inc. with over 25 years of experience in programming and computers. Creator of the core SecurCom technology. Infrastructure Architect for government and enterprise sectors for 15 years.

Sebastian Whitlock

Chief Design Officer (CDO)

Sebastian leads product design and user experience for the Securmeet ecosystem. He brings a wealth of experience in designing intuitive interfaces for complex financial and security products, ensuring powerful technology is accessible to all users.

Joanna Kirpsza

Chief Customer Service Officer (CCSO)

Joanna is a key member of the original SecurCom team. She has many years of IT experience, including as Manager of Microsoft/Skype Europe's CEE support team. She leads all customer success and support operations.

Part XI: Tying It All Together

A Corporate Headquarters Analogy

To ensure our model is fully understood, we can summarize the entire business with a powerful analogy. In simple terms, Securmeet is building the secure operational infrastructure for a modern global enterprise:

1. The Secure Corporate Headquarters

First, we provide the **secure corporate headquarters and its confidential boardroom** (our communication platform) where strategic decisions are made, completely shielded from corporate espionage.

2. The Operational Fuel

The SMS token acts as the essential **fuel or utility credit** required to power all operations within this secure headquarters—from initiating communications to receiving service discounts.

3. The Deflationary Engine

As the company (the platform) generates revenue, it uses a portion of those earnings to **buy back and burn the 'fuel' (SMS tokens)**, making the remaining supply more scarce over time.

Part XII: The Opportunity & The Ask

We are offering a ground-floor opportunity to participate in the initial distribution of the foundational utility token for this ecosystem. This offering is structured to fund the next stage of development and go-to-market activities.

Current Strategic Round: $5M Offering

We are currently raising a $5 million tranche as part of our broader Strategic Round. The terms for this specific offering are as follows:

Round Size: $5,000,000 USD

Tokens Offered: 125,000,000 SMS

Price per Token: $0.04 USD

Accepted Currencies: USDC, USDT, and Fiat (EUR/USD) via bank transfer.

Vesting: Tokens are subject to a structured vesting schedule: a 12-month lock-up, followed by a 24-month linear release, with tokens vesting on a daily basis.

Use of Proceeds

The funds raised in this strategic round are allocated to ensure the robust growth and decentralization of the Securmeet ecosystem. Proceeds will not be used for the development of the core product, which is already substantially complete. The allocation is as follows:

Ecosystem Growth & Market Expansion (50%): Funding for sales and marketing operations, strategic partnerships, and community-building initiatives to drive platform adoption.

Liquidity Provisioning (30%): To ensure a healthy and stable market for the SMS token upon its public launch on decentralized exchanges.

Legal & Compliance Overhead (20%): To navigate the evolving global regulatory landscape, secure necessary licenses, and ensure ongoing compliance with MiCA and other relevant frameworks.

Part XIII: Risk Factors & Disclosures

The purchase of SMS tokens involves a high degree of risk. Before purchasing SMS tokens, prospective purchasers should carefully consider the following risks and uncertainties.

No Expectation of Profit: The SMS token is a utility token intended to be used to access and pay for services within the Securmeet ecosystem. It is not a security, share, or any form of investment product. Purchasers should not have any expectation of profit from the purchase of SMS tokens.

Risk of Loss of Value: The market price of SMS tokens could decline significantly and may become worthless. The market for digital assets is highly volatile. The Company does not guarantee the market price of SMS tokens on any secondary markets.

Regulatory Uncertainty: The legal and regulatory framework governing digital assets is uncertain and rapidly evolving. While the SMS token is structured to be a utility token under MiCA, there is no guarantee that a regulator in any jurisdiction will not take a contrary view. Future legislative changes could adversely affect the use, transfer, and value of SMS tokens.

Technical and Security Risks: The Securmeet platform and the underlying blockchain technology are subject to technical risks, including but not limited to smart contract vulnerabilities, bugs, and malicious attacks.

No Governance or Equity Rights: Holding SMS tokens does not confer any ownership, equity, or voting rights in the Company.

Information Subject to Change: This whitepaper is a living document. The information contained herein is subject to change or update at any time without notice. All plans and projections are subject to change.

Comprehensive Legal Disclaimer

This Securmeet whitepaper is for informational purposes only and does not constitute an offer to sell, a solicitation of an offer to buy, or a recommendation for any security or investment product. Securmeet does not guarantee the accuracy of or the conclusions reached in this whitepaper, and this document is provided "as is." Securmeet does not make and expressly disclaims all representations and warranties, express, implied, statutory or otherwise, whatsoever. Securmeet and its affiliates shall have no liability for damages of any kind arising out of the use, reference to, or reliance on this whitepaper or any of the content contained herein. The information in this document is subject to change without notice, and all forward-looking statements involve inherent risks and uncertainties. The Securcoin (SMS) token is a utility token intended to be used within the Securmeet ecosystem; it is not a security and has not been registered under any securities laws. Prospective purchasers must conduct their own due diligence and consult their own legal, financial, and regulatory advisors before making any decisions.

Appendix A: 3-Year Token Protection & Projection Model

This appendix outlines the core economic mechanisms designed to support the SMS token economy and provides illustrative projections for the first three years post-launch. This model is built on a foundation of controlled supply, utility-driven demand, and a deflationary mechanism linked to platform revenue.

Three Pillars of a Sustainable Token Economy

1. Controlled Supply

Long-term vesting schedules for all team, advisor, and private sale tokens (12-month lock, 24-month linear daily release) prevent market shocks and align all parties with the long-term success of the project.

2. Utility-Driven Demand

Demand is not speculative. It is driven by fundamental platform utility, as SMS tokens are the core mechanism for accessing services and receiving discounts, creating a direct link between usage and demand.

3. Deflationary Buy-Back & Burn

The Company will allocate **a minimum of 30% of Gross Platform Revenue** to systematically buy back SMS tokens from the open market and permanently burn them. This creates a powerful, ongoing deflationary pressure, linking platform success to token scarcity.

Illustrative 3-Year Projection (Buy-Back & Burn Model)

The following projections are illustrative and based on our business plan for client acquisition and platform usage. They are intended to demonstrate the potential impact of our deflationary economic model.

Metric	Year 1	Year 2	Year 3
Gross Platform Revenue	$1.5M	$6.0M	$15.0M
Revenue for Buy-Back & Burn (30%)	$450,000	$1,800,000	$4,500,000
Projected SMS Tokens Burned**	3.0M	12.0M	30.0M
Cumulative Supply Reduction	**0.3%**	**1.5%**	**4.5%**

*Gross Platform Revenue includes all subscription and service fees.

**Projections are for illustrative purposes only. Assumes an average token price of $0.15 for buy-back calculations.

> **Disclaimer:** The projections and information contained in this appendix are forward-looking statements based on the Company's current assumptions and expectations. They are not guarantees of future performance. Actual results may differ materially due to various risks and uncertainties. This document does not constitute financial advice.