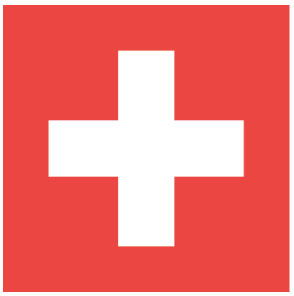

SWISS SUBNET
SUBNET SUISSE
SCHWEIZER SUBNET
SUBNET SVIZZERA

# Swiss Subnet White Paper

January 30, 2025

Powered by INTERNET COMPUTER

# Abstract

The Swiss Subnet represents a novel implementation of the Internet Computer Protocol (ICP), designed to address the specific needs of institutional clients requiring high levels of data sovereignty, regulatory compliance, and privacy. This white paper outlines the technical architecture, unique advancements, and innovative use cases enabled by the Swiss Subnet, which leverages the subnet capabilities of ICP to create a geographically constrained, permissioned blockchain network within Switzerland and Liechtenstein.

Our focus is on the technical innovations that differentiate the Swiss Subnet from other blockchain implementations, particularly in the areas related to canister-in-canister architecture, geographic exclusivity, and regulatory compliance. By building on ICP's subnet model, we have developed a platform that combines the transparency and decentralization of public blockchains with the control and privacy required for enterprise-grade applications.

The architecture provides developers with the necessary tools to achieve the highest levels of data protection and Swiss military-grade encryption. By leveraging these capabilities at the application design layer, developers can implement robust encryption mechanisms, secure data handling, and compliance measures to maximize security and regulatory adherence.

# Contents

1. Introduction..... 4
2. Technical Architecture..... 5
    2.1 Why the Internet Computer Protocol?..... 5
    2.2 Canister-in-Canister Architecture..... 6
        2.2.1 Key Features..... 7
        2.2.2 Use Case Example..... 7
    2.3 Geographic Exclusivity..... 7
        2.3.1 Node Distribution..... 7
        2.3.2 Data Residency..... 7
    2.4 Regulatory Compliance..... 8
        2.4.1 Built-In Compliance Mechanisms..... 8
        2.4.2 Auditability..... 8
3. Use Cases..... 8
    3.1 Secure Document Management (SDM)..... 9
    3.2 Network Custody: Next-Generation Digital Asset Management..... 9
    3.3 Swiss Product Certification System..... 9
    3.4 Advanced Digital Legacy Planning..... 10
    3.5 Identity as a Service (IDaaS) – Zero-Knowledge Proof System..... 10
4. Conclusion..... 10

# 1. Introduction

The Swiss Subnet is a Layer-1 blockchain built on the Internet Computer Protocol (ICP), designed to meet the stringent requirements of institutional clients in Switzerland and Liechtenstein. While ICP provides a robust foundation for decentralized applications, the Swiss Subnet extends this foundation with several key innovations:

- **Canister-in-Canister Architecture**: A novel approach to nested smart contract execution, enabling complex, multi-layered applications with enhanced privacy and security.
- **Geographic Exclusivity**: A subnet architecture that ensures all nodes are physically located within Switzerland and Liechtenstein, providing guaranteed data residency and compliance with local regulations.
- **Regulatory Compliance**: Built-in mechanisms for adhering to Swiss and Liechtenstein financial regulations, including data protection laws and tokenization frameworks.

This white paper will explore these advancements in detail, providing a technical overview of the Swiss Subnet's architecture, its unique features and use cases.

# 2. Technical Architecture

## 2.1 Why the Internet Computer Protocol?

The Internet Computer Protocol represents a fundamental reimagining of blockchain architecture. Its unique architecture addresses the core challenges that have historically prevented institutional adoption of blockchain technology. ICP has multiple features without which the Swiss Subnet advancements wouldn’t be possible:

**Subnet Architecture** — While conventional blockchains maintain a single global state, ICP orchestrates a network of independent state machines called subnets. Each subnet operates as an autonomous blockchain yet remains integrated with the rest of the network. Some subnets are permissioned to only critical network dApps, some subnets are use-case specific, while others can be tied to a specific geography. The Swiss Subnet uses this unique capability.

**Chain Key Cryptography & MPC** — The protocol's Chain Key Cryptography (chain-key) stands as one of ICP’s most significant innovations. This technology enables secure communication between subnets through sophisticated threshold signatures, while providing cryptographic verification of subnet states. Through threshold ECDSA, it facilitates seamless integration with external networks, ensuring each subnet maintains independence while benefiting from protocol-level security. Each subnet holds one master key that helps derive keys for each application. Multi-Party Computation (MPC) allows for Decentralized Key Generation, where the key

is generated in a decentralized manner and never reconstructed. For each message to be signed, it needs ⅓ of the nodes on the network to sign it. This puts the availability at ⅔. While there are at least ⅓ of healthy nodes, signing can happen.

**Web Assembly** — Each node runs multiple replicated state machines, which are called canisters. Every canister is a web assembly program run in a sandbox in a lock-step fashion across the subnet. The protocol's canister smart contracts operate in a WebAssembly-based execution environment, incorporating orthogonal persistence that eliminates complex state management. These canisters can handle native HTTP requests and guarantee deterministic execution, making them ideal for enterprise applications that require reliable, consistent performance. And security-sensitive operations such as encryption or advanced data protection can be implemented at the App Layer by developers to meet military-grade security standards.

**Storage & Orthogonal persistence** — Each canister offers developers 500Gb of storage available with orthogonal persistence, eliminating the need to manage separate replicated databases.

**Web Speed** — ICP manages to reach 75 blocks/s & 5M TPS. While having an easy-to-use storage primitive, ICP remains nonetheless performant. The Swiss Subnet inherits this performance level directly from ICP, as it operates within the same fundamental architecture. The consensus layer implements a novel probabilistic slot consensus protocol that achieves finality in seconds. This speed, combined with the ability to process millions of transactions per second within each subnet, creates a foundation for enterprise-scale applications.

**Reverse gas** — ICP's reverse gas model fundamentally reimagines blockchain economics. Unlike traditional networks where users pay gas fees, ICP implements a “cycles” system where smart contracts (canisters) pay for their own computation. This approach eliminates end-user gas fees, enabling mainstream adoption while providing predictable operational costs for enterprise deployments.

**On-chain randomness** — The protocol implements deterministic randomness generation, which is critical for privacy-specific protocols and applications requiring verifiable unpredictability. This system ensures fair and tamper-proof random number generation directly on-chain.

**Time Management** — Time plays a key role in cryptography and application functionality. ICP provides periodic tasks for scheduled execution, timers for precise control, and system time/timestamps for consistent temporal references across the network.

**Internet Identity** — II is a system canister that provides secure authentication. It leverages WebAuthn for device-based authentication, eliminating traditional username/password combinations while maintaining high security standards.

**HTTP Outcalls & Gateway** — ICP smart contracts can both make external HTTP requests and be accessed through regular web APIs. This allows regular developers to interact with smart contracts without specialized blockchain knowledge, treating them like traditional web services.

**Custom domain names** — The IC allows developers to put custom domain names in front of canister addresses. When combined with the HTTP Gateway, this creates a seamless web2-like experience for users while maintaining the benefits of decentralized applications.

**VetKeys** — In the future, one of the core security features of ICP. Compared to cloud providers, the network is completely transparent while ensuring that no one, but the authorized keyholder, can access the protected information. VetKeys provide verifiable and secure access control essential for enterprise applications and Swiss Subnet use-cases.

## 2.2 Canister-in-Canister Architecture

One of the most significant technical features of the Swiss Subnet is the canister-in-canister architecture, where one smart contract (canister) can host and invoke other canisters within a secure environment. This innovation allows canisters to interact with each other. One canister can call the functions of another canister, which is essential for building complex applications. This interaction facilitates modularity and code reuse.

### 2.2.1 Key Features:

- **Nested Execution**: Canisters can invoke other canisters within a secure, isolated environment, enabling complex workflows without exposing internal logic to the broader network.
- **Privacy Preservation**: By encapsulating sensitive operations within nested canisters, the Swiss Subnet ensures that only authorized parties can access specific data or functionality.
- **Resource Optimization**: Nested canisters share resources more efficiently, reducing the computational overhead associated with traditional smart contract interactions.

### 2.2.2 Use Case Example:

In a financial application, a parent canister could manage high-level transaction logic, while nested canisters handle specific tasks such as identity verification, compliance checks, and asset transfers. This structure ensures that sensitive operations remain isolated and secure, while still benefiting from the transparency and immutability of the blockchain.

## 2.3 Geographic Exclusivity

The Swiss Subnet is designed to operate exclusively within the borders of Switzerland and Liechtenstein, ensuring that all data processing and storage comply with local regulations. This geographic exclusivity is achieved through a carefully curated network of nodes, all of which are physically located within the two countries.

### 2.3.1 Node Distribution:

- **Data Centers**: The Swiss Subnet will operate with 10 nodes in Switzerland, distributed across 10 different cantons, and 3 nodes in Liechtenstein. This distribution ensures geographic redundancy and fault tolerance while maintaining strict compliance with local data residency requirements. The node topology includes:
- **Nakamoto Coefficient**: The network implements a distributed architecture with 13 independent nodes, a key factor in achieving a high Nakamoto Coefficient. This configuration ensures the network's resilience against potential centralized attacks.

### 2.3.2 Data Residency:

- **Guaranteed Compliance**: By ensuring that all nodes are located within Switzerland and Liechtenstein, the Swiss Subnet provides institutional clients with verifiable data residency, a critical requirement for compliance with Swiss data protection laws.
- **Physical Security**: Several data centers are located in decommissioned Swiss Army bunkers, offering enhanced physical security features such as electromagnetic pulse (EMP) protection.

## 2.4 Regulatory Compliance

The Swiss Subnet is designed to seamlessly integrate with the regulatory frameworks of Switzerland and Liechtenstein, providing institutional clients with a blockchain solution that meets the highest standards of legal and financial compliance.

### 2.4.1 Built-In Compliance Mechanisms:

- **Tokenization Framework**: Tokenization refers to converting real-world assets, like securities or real estate, into digital tokens on a blockchain. The subnet supports the tokenization of assets in compliance with the Swiss DLT Act and Liechtenstein's Blockchain Act (TVTG), enabling the creation of tokenized securities and other digital assets.
- **Data Protection**: The subnet's architecture ensures compliance with both the Swiss Federal Act on Data Protection (FADP) and the EU's General Data Protection Regulation (GDPR), providing clients with a secure and legally

compliant platform for data storage and processing (however, ultimate compliance relies on the application layer's proper implementation of encryption, secure access control, and key management techniques).

#### 2.4.2 Auditability:

- **Immutable Audit Trails:** All transactions and operations on the Swiss Subnet are recorded on the blockchain, providing an immutable audit trail that can be easily accessed for regulatory reporting and compliance checks.
- **Real-Time Monitoring**: The subnet includes built-in tools for real-time monitoring of transactions, enabling institutions to quickly identify and address any compliance issues.

# 3. Use Cases

The Swiss Subnet's unique architecture enables a range of innovative use cases, particularly in the areas of secure document management, digital asset custody, product certification, digital legacy planning, and identity management.

## 3.1 Secure Document Management (SDM)

The SDM system leverages the Swiss Subnet's canister-in-canister architecture to provide a secure, blockchain-based solution for document management. Key features include:

- **Military-Grade Encryption**: Developers implement application-level encryption, so documents are protected using advanced cryptographic techniques. Key management leverages a nested canister architecture, enhancing security and ensuring compliance with the highest standards.
- **Immutable Audit Trails**: All document access and modifications are recorded on the blockchain, providing a verifiable history of changes.
- **Granular Access Controls**: Institutions can define precise access permissions for different users, ensuring that only authorized parties can view or modify sensitive documents.

## 3.2 Network Custody: Next-Generation Digital Asset Management

The Swiss Subnet's network custody solution redefines digital asset management by combining on-chain governance with sophisticated key management. Key features include:

- **Multi-Signature Wallets**: Assets are managed using multi-signature wallets, with keys distributed across multiple nested canisters to enhance security.

- **Automated Compliance**: All transactions are automatically checked for compliance with Swiss and Liechtenstein regulations, reducing the risk of legal or financial penalties.
- **Inheritance Planning**: The system includes tools for digital legacy planning, enabling institutions to automate the transfer of assets in accordance with predefined conditions.

## 3.3 Swiss Product Certification System

The Swiss Product Certification System uses the Swiss Subnet to create an immutable, verifiable record of product authenticity and origin. Key features include:

- **Blockchain-Based Certification**: Products are issued with blockchain-based certificates that can be easily verified by consumers and regulators.
- **Supply Chain Integration**: The system integrates with existing supply chain networks, providing end-to-end tracking of products from manufacture to sale.
- **Quality Assurance**: The system includes built-in tools for verifying compliance with Swiss quality standards, ensuring that only products meeting these standards receive certification.

## 3.4 Advanced Digital Legacy Planning

The Swiss Subnet enables sophisticated digital legacy planning through smart contracts that automate the transfer of digital assets upon predefined conditions. Key features include:

- **Triggering Mechanism**: A mechanism that triggers specific actions (like transferring assets) when predefined conditions are met, such as the absence of user activity for a certain period of time. In the context of digital legacy planning, it ensures that assets are securely and automatically passed to designated beneficiaries. This secure automated system can be used for transferring assets to beneficiaries upon verified trigger conditions, such as the death of the asset holder.
- **Tokenized Inheritance Rights**: Inheritance rights are tokenized on the blockchain, ensuring transparency and immutability in the execution of wills and estate plans.
- **Regulatory Compliance**: The system integrates with Swiss inheritance laws, providing a legally compliant framework for digital asset succession.

## 3.5 Identity as a Service (IDaaS) – Zero-Knowledge Proof System

The Swiss Subnet's Identity as a Service (IDaaS) platform leverages zero-knowledge proofs to enable secure identity verification without exposing sensitive personal information. Key features include:

- **Attribute-Based Proofs**: Users can prove specific attributes about their identity (e.g., age, nationality) without revealing unnecessary personal data.
- **Privacy-Preserving Verification**: The system ensures that identity verification can be performed without compromising user privacy.
- **Decentralized Identity Anchoring**: Identity credentials are anchored on the blockchain, providing a secure and tamper-proof record of user attributes.

# 4. Conclusion

The Swiss Subnet represents a significant advancement in blockchain technology, combining the transparency and decentralization of public networks with the privacy and control required for institutional applications. By leveraging ICP's subnet architecture and introducing innovations such as canister-in-canister execution, geographic exclusivity, and built-in regulatory compliance, the Swiss Subnet provides a powerful platform for the future of digital asset management.

As blockchain technology continues to evolve, the Swiss Subnet will remain at the forefront of innovation, enabling institutions to navigate the complexities of the digital economy with confidence and security.