**Gnosis Ecosystem Application – Finoa GmbH**

**Project name**

Development of a warm-storage Hardware-Security-Module (HSM) custody solution for the Gnosis protocol and its GNOs

**Team members**

* Henrik Gebbing (Co-Founder & Managing Director)
* Christopher May (Co-Founder & Managing Director)
* Dr. Martin Rieke (Chief Technology Officer)
* Fabio Nelson Macchi (Head of Operations)
* Jan-Peter Kind (Chief Banking Officer)
* Wilhelm Eduard Nöffke (Senior Compliance Manager)
* Pietro Danzi (Software Engineer)
* Amarildo Grembi (Junior Software Engineer)
* Victor Kausch (Business Development Analyst)
* Lucero Pinilla (Operations Analyst)

**What project are you building**

Integration of Gnosis into Finoa’s warm-storage HSM custody solution enabling Finoa’s customers, which range from Digital Asset Managers, Venture Capital Firms and Tokenization Platforms to Corporates, to securely safeguard, manage and later on stake their GNO based Digital Assets.

**Why did you decide to build it**

We decided to integrate the Gnosis protocol into our infrastructure, to attract new investors and market participants. Once integrated, Finoa will also be able to offer its existing customers the opportunity to custody and safely manage their own GNO tokens. Consequently, promoting the Gnosis community by providing Digital Asset Investors with the means to store and manage their GNO/OWL tokens in a secure and compliant infrastructure, including custody, trading and staking services.

**How long will it take**

Integrating and developing the Gnosis specifics into our infrastructure will take between 9-10 weeks. We expect to be able to leverage a significant part from our existing and advanced custody and node infrastructure. With the grant, we will be able to cover the setup of the additional hardware infrastructure as well as the development of the Gnosis specifics including its integration. Excessive costs, in case they’ll arise, will be sourced from our funding.

**How much funding are you requesting**

As indicated in the previous paragraph, we expect the project to require a total of 46 days (approx. 9-10 weeks) to be completed including a go-live of GNO in our system. Through the mix of internal as well as external capacity (from our sister company The Cluster Company GmbH), we are calculating with an average cost per FTE per day of EUR 650. In addition to that, a cost of EUR 15,000 for the purchasing of additional hardware (Servers, HDDs, Redundant Setup) should be calculated. Summing this up, we are expecting a total cost for the execution of the described project of EUR 45k, consisting of 46 (# of FTE days) x EUR 650 (average costs per FTE day) plus Hardware costs of EUR 15k.

**How did you hear about the GECO**

Multiple customers of ours have shown interest in securely storing their GNOs with us and additional desktop research on the Gnosis protocol and community itself has ultimately guided us towards, as advertised on the Gnosis homepage, GECO as a means of funding.

**Your Proposal**

**Project description**

Finoa, based in Germany, is Europe’s first fully digital (warm-storage) custody and asset-servicing solution for Institutional Players in the Digital Asset space.  
Our solution is built on crypto-native banking infrastructure and combines maximum user-friendliness with the highest military-grade security levels available in the market. Consequently, we are building a fully compliant (PSD2, EBICS, Central Bank Reporting) solution to obtain the newly to be introduced “crypto custody-banking license” issued by the local regulator BaFin in Germany.

Despite our regulatory approach, our vision and mission are to build a platform to enables crypto as well as traditional players out of the various industries (including financial, industrials, telecommunication, energy, manufacturing) to benefit from a decentralized ecosystem. Thus, it is a logical step for us to aim to integrate the Gnosis protocol into our infrastructure to facilitate our current and future client base of institutional players, which range from Digital Asset Managers, Venture Capital Firms and Tokenization Platforms to Corporates, in securely safeguarding and in a later step staking their Digital Assets and providing them with secure access to the Gnosis ecosystem.

**Features**

The target deliverable is a library written in C99 with as few external dependencies as possible so it may be used in embedded systems, such as programmable hardware security modules. It may be assumed that all necessary cryptographic functionality is provided externally and is not part of the library.

The library shall provide functionality for:

1) Generating a new pair of private key and public address for a given currency

2) Checking the consistency and correctness of an address

* Given the public address, the function should check the consistency of the address

3) Creation of signed raw transactions

* Given a private key and details of a transaction (such as destination and amount), generate a raw transaction for the specified details, signed by the private key

**Team description (Project participants) and past relevant projects**

* Christopher May – Co-Founder & Managing Director
* Dr. Martin Rieke – Chief Technology Officer
* Pietro Danzi – Senior Software Engineer
* Amarildo Grembi – Junior Software Engineer

Previously integrated the Tezos and Polkadot Protocol into Finoa’s warm-storage HSM custody solution enabling our customers, which range from Digital Asset Managers, Venture Capital Firms and Tokenization Platforms to Corporates, to securely safeguard and later on stake the above mentioned protocols’ respective tokens.

**Milestones for integrating Gnosis based currencies into the Finoa custody system**

**Phase I**

**Planning and design of C library for Gnosis**

Planning and design of library interfaces, functionality, and user experience in order to ensure consistency with the existing Gnosis ecosystem of libraries and programs as well as easy testability, modularity, and allowing for easy auditability and potential formal verification.

*Time required: 4 developer days*

*Costs: 2600 €*

**Phase II**

**Development of a C library for Gnosis**  
The target deliverable is a library written in C99 with as few external dependencies as possible so it may be used in embedded systems, such as programmable hardware security modules. It may be assumed that all necessary cryptographic functionality is provided externally and is not part of the library.

1) Generating a new pair of private key and public address for a given currency.

*Time required: 4 developer days*

*Costs: 2600€*

2) Checking the consistency and correctness of an address

* Given the public address the function should check the consistency of the address

*Time required: 5 developer days*

*Costs: 3250 €*

3) Creation of signed raw transactions

* Given a private key and details of a transaction (such as destination and amount), generate a raw transaction for the specified details, signed by the private key

*Time required: 7 developer days*

*Costs: 4550 €*

**Phase III**

**Integration of Gnosis based currencies into the Finoa custody system**

By integrating the developed library into our proprietary HSMs and enabling the required features in our custody system, we will support custody solutions for Gnosis based currencies. Core functionality will include the generation of a new address, the observation of incoming and outgoing transactions, withdrawing assets from the generated address

*Time required: 10 developer days*

*Costs: 6500 €*

**Phase IV**

**Setup and deployment of full Gnosis node for testing and verification**

In order for our system to support Gnosis, we will deploy a full node, which will serve the custody system with access to the Gnosis blockchain in order to provide functionality such as:

* Query account balance  
  \* List incoming and outgoing transactions for a given address  
  \* Send signed transactions into the blockchain

*Time required: 7 developer days*

*Costs: 4550 €*

**Phase V**

**Testing and auditing of library**

To ensure correctness, a full series of automatic and manual integration and unit tests needs to be performed, including generation and verification of addresses, performing transactions and handling incorrect inputs.

*Time required: 9 developer days*

*Costs: 5850 €*

**Detailed time schedule:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Project Steps** | | **Apr**  **1** | **Apr**  **08** | **Apr 15** | **Apr 22** | **Apr 29** | **May 6** | **May 13** | **May**  **20** | **May 27** | **June**  **6** |
| **Planning and design of C library for Gnosis** | * 1. Compiling an overview cryptographic processes and infrastructure details of the Gnosis eco system |  |  |  |  |  |  |  |  |  |  |
| **Development of a C library for Gnosis (with the substeps listed and with days)** | * 1. Generating a new pair of private key and public address for a given currency. |  |  |  |  |  |  |  |  |  |  |
| * 1. Checking the consistency and correctness of an address |  |  |  |  |  |  |  |  |  |  |
| * 1. Creation of signed raw transactions |  |  |  |  |  |  |  |  |  |  |
| **Integration of Gnosis based currencies into the Finoa custody system** | 3.1  integrating the developed library into our proprietary HSMs and enabling the required features in our custody system |  |  |  |  |  |  |  |  |  |  |
| **Deployment of full Gnosis node for servicing of the Finoa custody system** | 4.1 Deployment of a full node, which will serve the custody system with access to the Gnosis blockchain |  |  |  |  |  |  |  |  |  |  |
| **Testing** | 5.1 A full series of automatic and manual integration & unit tests |  |  |  |  |  |  |  |  |  |  |

