***Spécifications***

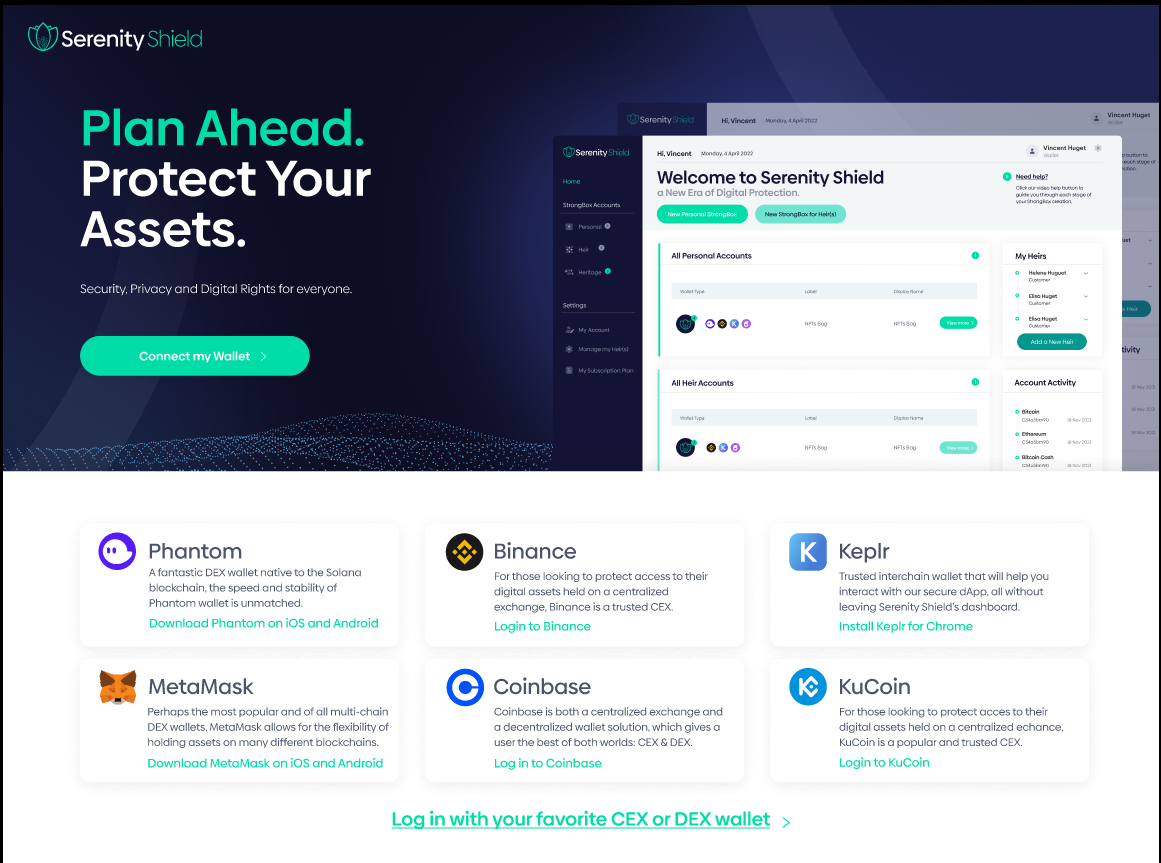
***Version 1.0***

***Work Document***

***07/07/2022***

***Web application MVP Project***

***« Serenity Shield »***



***Table of contents***

[1. Context 2](#_Toc97672237)

[2. System Features & Interface……………………………………………………………………………………………………………………………….4](#_Toc97672238)

[2.1. Navigation 5](#_Toc97672239)

[2.2. Connect your Wallet 5](#_Toc97672240)

[2.3.Home 8](#_Toc97672241)

[2.4. Personal 22](#_Toc97672242)

[2.5. Heir(s) 23](#_Toc97672243)

[2.6. Heritage 24](#_Toc97672244)

[2.7. My Account 25](#_Toc97672244)

[2.8. Manage My Heir(s) 26](#_Toc97672244)

[2.9. My Plan 33](#_Toc97672244)

[3. **Data Dictionary** 34](#_Toc97672246)

[3.1 users 34](#_Toc97672247)

[3.2 Strongboxes 34](#_Toc97672248)

4. **Conceptual data model:**

[4.1 MCD 35](#_Toc97672247)

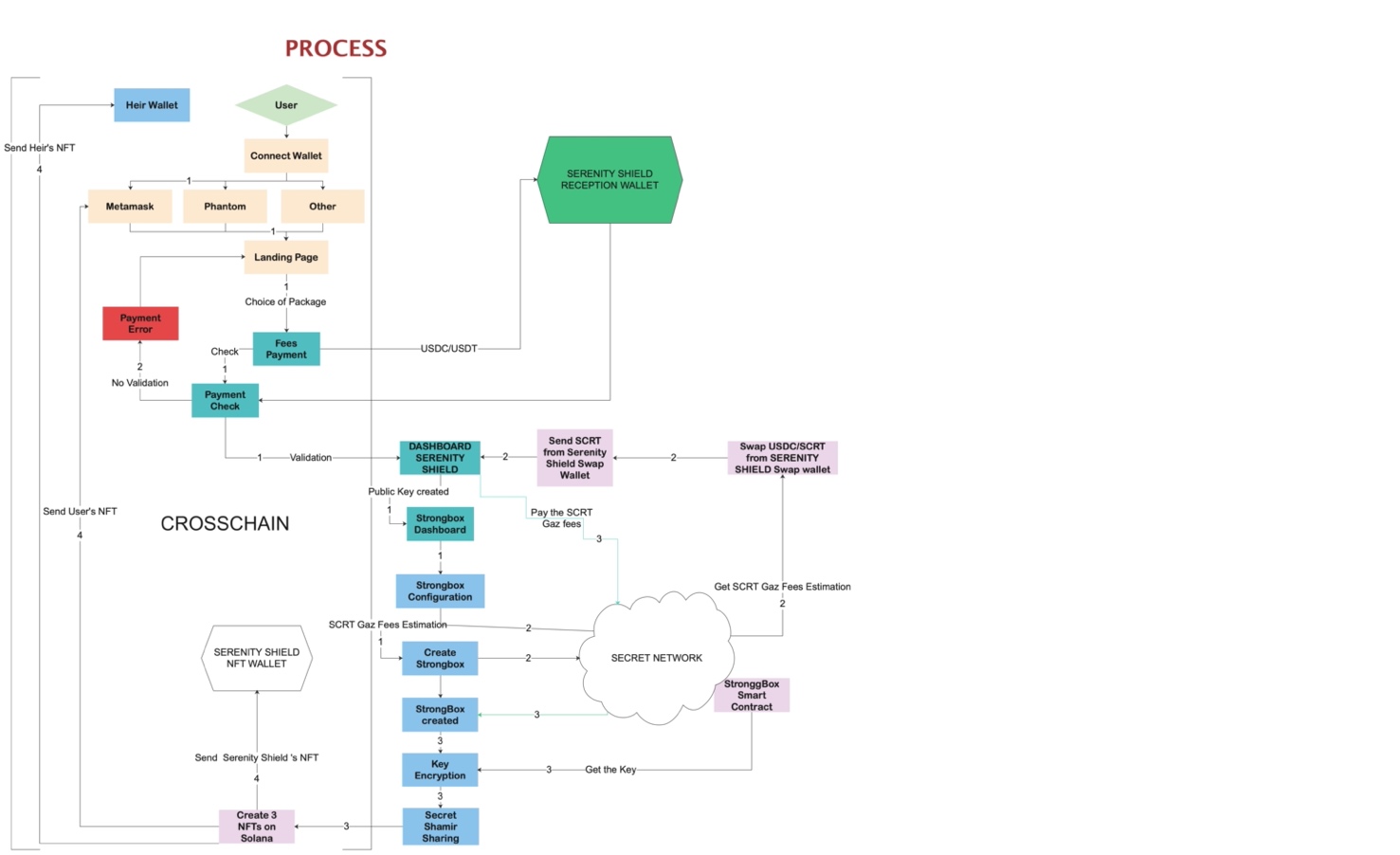
**1. Context**

The purpose of this document is to centralize the needs and solutions retained within the framework of the realization of a web application project based on the Solana blockchain which is aimed at our future customers, in order to secure their digital assets and be able to bequeath it to their heirs. Given the current monetary situation, securing digital assets is increasingly necessary. The creation of a suitable system facilitates the recovery of assets by people designated by our future customers.

The purpose of this “specifications – Serenity Shield” document will be to describe the needs and analyze the solutions.

Objective in building the MVP The objective in building this MVP was simple: to have a product that is technologically very advanced, yet easy to use and intuitive. Challenges in building the MVP The 1er challenge was the integration of Secret Network, an indispensable brick because it guarantees the opacity of the Smart Contract (in fact, normally, everything is transparent and accessible on the blockchain). In particular, the fact that, in order to use Secret Network, each future user of our solution must pay gas fees on this blockchain, and therefore must pay them from a wallet compatible with Secret Network (Torus or Keplr). The creation of such a wallet has been integrated into the customer journey in a simple and intuitive way directly on the Serenity Shield interface so as not to lose the customer. The second challenge was our desire to have a cross-chain solution, allowing the user to connect any wallet to Serenity Shield to purchase our solution (not necessarily a Solana wallet) and use our DApp. The other advantage of cross-chain is the transactions in the next private sales. Unlike in round 1, the investor will be able to pay and invest in our SERSH from any network. This is made possible by the automatic detection of the wallet address used and the orientation of the transactions on this basis. Finally, the 3ème challenge was to think of and pre-empt all possible security flaws, both in our solution and in Secret Network, and to preempt them. By setting up proprietary codes, developing our own libraries, and by setting up a large number of Chinese walls within the Tech team. Consequences and advantages We offer a highly secure solution that guarantees privacy. We simplify and streamline processes, breaking down established codes and business models previously compartmentalised by blockchain. We facilitate access to our solution, allowing the greatest number of people to secure access to their digital assets. All this is perfectly aligned and serves our vision & mission statement, translated into our baseline as : "Security, Privacy and Digital Rights for everyone”.

MVP tech/process pathway

****

Without repeating what is clearly understood in the diagram, here are some points of clarification on the process:

- The framed part on the left is the cross-chain part, the other (right) is the Serenity Shield/Secret Network part.

- The user can connect almost any wallet to our interface (Metamask, Phantom, Binance, etc.); as a reminder our tech is on the Solana blockchain. - The user will be able to choose the package: a priori there will be 3 different packages, including a basic one which is very accessible from a financial point of view (a few dollars).

- Once the payment has been made (in USDC/USDT and received by Serenity Shield on its Reception Wallet), you enter the "Serenity Shield/Secret Network" section on the left.

- The user is told that, in order to create his StrongBox and Smart Contract which will be hosted on the Secret Network blockchain, gas fees will have to be paid. Although deducted from the package paid upstream, these gas fees must be paid via a Secret Network wallet (Torus or Keplr wallet).

- The user is then guided through the creation of this wallet (while not leaving the Serenity Shield interface thanks to a very intuitive user path, with information bubbles, greyed-out areas, etc. ). If the user already has a wallet of this type, then they just need to plug it in at this stage of the process of course.

- The configuration of the StrongBox consists in entering all the information to be kept (passwords etc.) and selecting the desired "Inactivity Policy" (15 days, 6 months, 1 year, etc.). At the chosen frequency, the user will receive a notification from Serenity Shield to confirm his activity, and to confirm that he is "alive". If not, they will be called by our services, then their heirs, etc. A whole procedure is put in place until the heirs can effectively trigger the release of the Serenity Shield NFT, thus allowing access to the contents of the Smart Contract (they are then in possession of 2 out of 3 NFTs, which is the triggering rule).

- In the MVP, the form is well detailed and leaves a wide choice of possibilities.

- If the user wants to use Serenity Shield for transmission, then he has to create as many StrongBoxes as heirs (or pools of heirs), and to configure his StrongBoxes in the same way. Eventually, it will be possible to duplicate the information entered in the reference StrongBox (the 1st), for more practicality.

- Once the StrongBox(es) are created, a total amount of gas fees is calculated based on the number of StrongBoxes and especially the volume of data stored. These are estimated at $1 or $2 per StrongBox.

- This amount is then converted at the USDC/SCRT conversion rate at time T, thanks to a specific Serenity Shield swap wallet (the conversion is done by API, not by Serenity Shield directly, we don't handle financial assets ourselves/exchange tokens on note DApp).

- The newly converted SCRTs are sent by Serenity Shield to the user's Torus/Keplr wallet (of course, Serenity Shield does not "gift" them to the user, it deducts them from the fees paid when the Serenity Shield account was created and the package purchased). The user can then, via their Torus/Keplr wallet, pay their Secret Network fees.

- Its StrongBox(es) and, above all, its Smart Contract are then officially created. To distinguish the two, it is the Smart Contract that actually stores the data, whereas the StrongBox allows the data to be viewed but does not contain it as such (the StrongBox could be seen as a hologram of the Smart Contract's content).

- Serenity Shield then retrieves the Viewing Key from the newly created Smart Contract, encrypts it and splits it into 3 via Secret Shamir Sharing.

- Note that the encryption process takes place twice: encryption of the Viewing Key after creation of the Smart Contract (as seen above), but also encryption of the data to be stored in the Smart Contract, precisely in case Secret Network is hacked.

- The rest is simple: for each of the 3 parts of the Secret Shamir Sharing, an NFT is created. The 1st is sent to the user, the 2nd stored by Serenity Shield, and the 3rd sent to the heir.

- Eventually, the heir will have the possibility to be trained and accompanied (Serenity Shield services).

- Finally, there are 3 special cases that have been anticipated:

o 1. Case where the heir does not have a wallet (if he is a 5 year old child for example): we ask the user to give us a wallet address different from the one he has connected to and on a different network before transmitting him the NFT of the heir on this one. A reminder will also be sent to the user reminding them to create a wallet for their heir so that they can pass on this NFT.

o 2. If the heirs are not informed of the existence of the account: a warning system is set up for this purpose when the user dies. Similarly, the user must have provided an address other than the one with which he or she had connected to the database. In this case too, the heir's NFT is sent to another wallet than NFT #1. Please note: we give the user the possibility to transfer the NFT to another wallet (belonging to Serenity Shield and on another network) by making him accept the conditions of use. To prevent the death of the heir, we will not be able to recover the NFT necessary to open the Smart Contract.

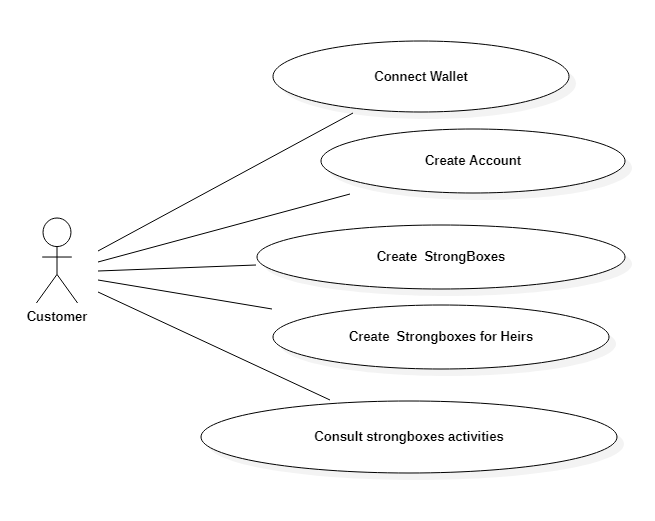
o 3. Case where the user and his heirs all die at the same time (car accident for example) : an option including the donation to a charity or not is proposed at the creation of the StrongBox in all cases.

**2.** **System Features & Interfaces**

The system functionalities represented in the use case diagram (Appendices 1) are as follows::

* Connect Wallet.
* Create Account.
* Create Strongboxes.
* Create Stronboxes for Heirs.

**Annex 1 : Use Case Diagram**



The actors retained are the following: the customers.

**2.1. Navigation**

The first level of navigation in the choice of users is as follows:

* Connect Wallet.

The second level of navigation in the user choices is as follows:

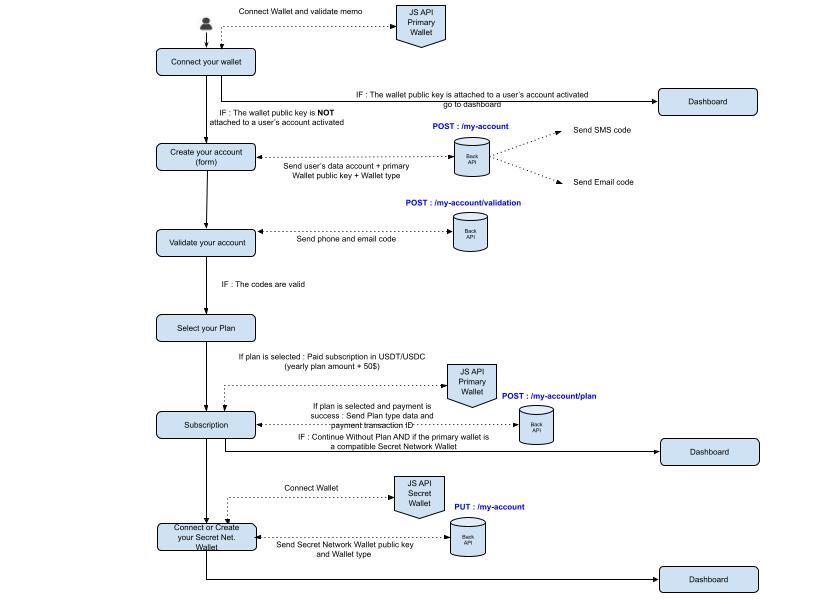
* Navigate through the different sections:Home
  + Strongbox Accounts
    - Personnal
    - Heir
    - Heritage
  + Settings
    - My Account
    - Manage my Heir(s)
    - My Subscription Plan

**2.2. Connect your Wallet**

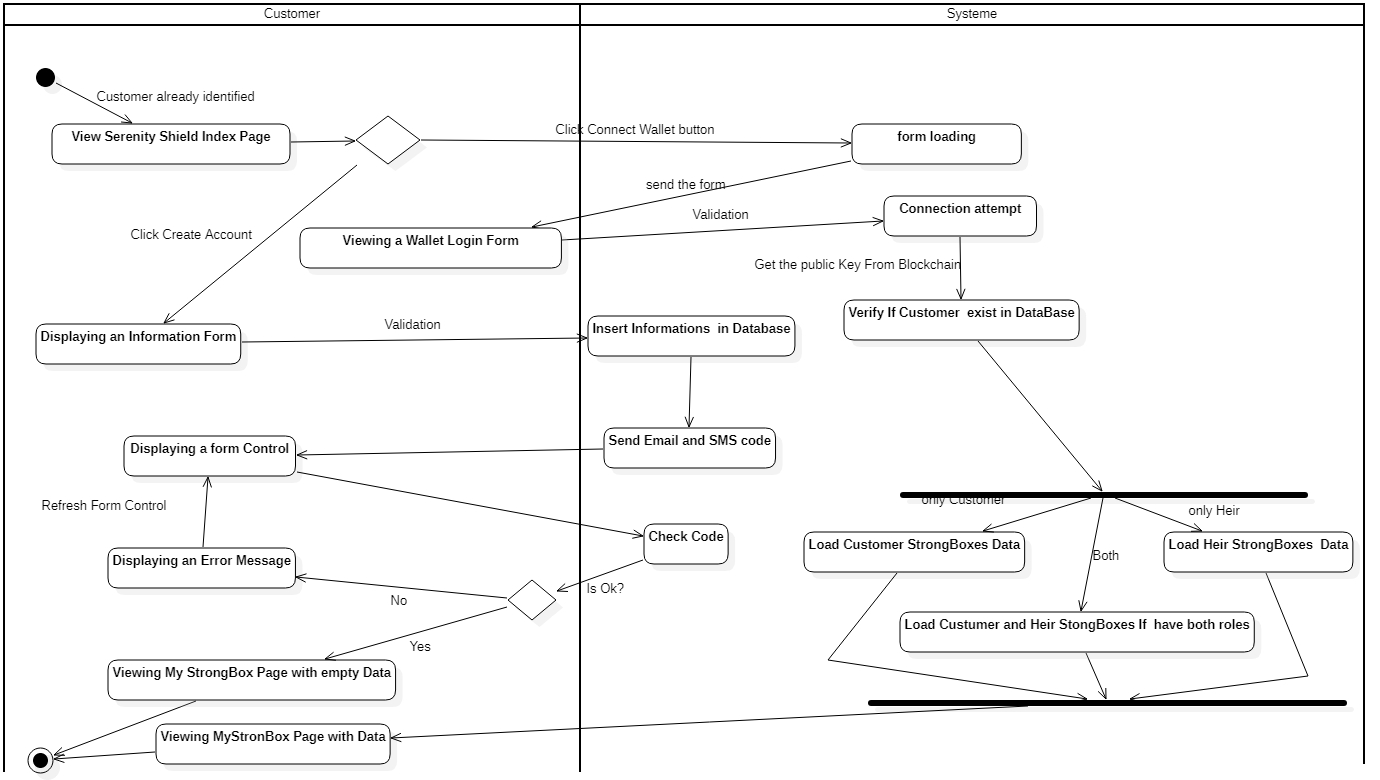
The interface « Connect Wallet» (annex 3 The "Connect Wallet" interface (Appendix 3) is reserved for all customers", i.e. any individual who has been identified will be able to use this interface.

When the user has successfully connected their Wallet, they go to the Home page.

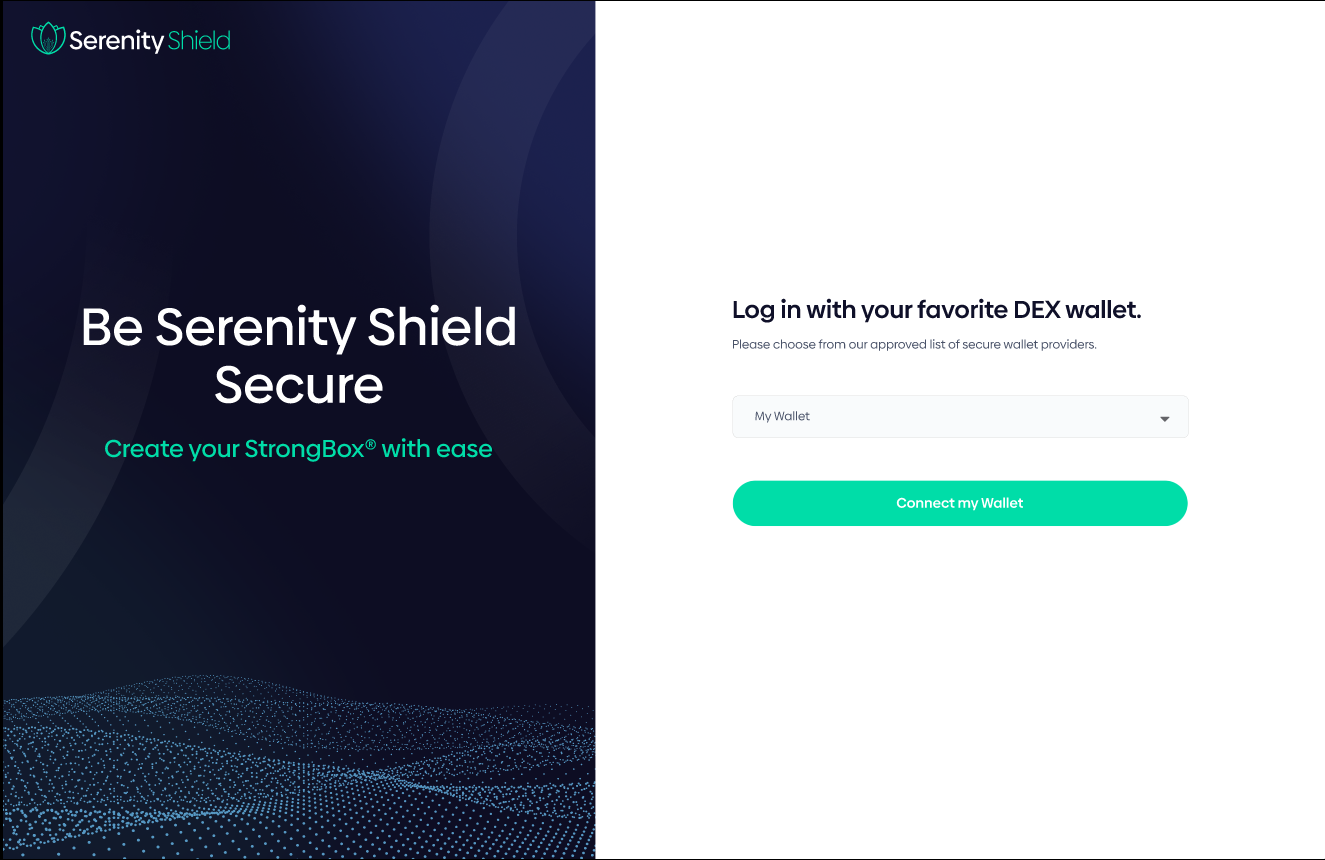
The diagram below shows the connection logic.



**Annex 2: "Connect your Wallet"** activity diagram



**Annex 3 : Interface « Connect Wallet »**



**Connection** Use Case

Here the Customer has the choice to connect his wallet or create an account.

***Standard Scenario 01 – The customer has his right Wallet key***

1. The customer manages to connect his Wallet without any problems and accesses the Home page.

***Standard Scenario 02 -*** ***The customer has his right Wallet key but a connection error***

1. The client enters his key but the system refuses him the connection then an error message is displayed, when closing the message the client returns to the index page and must start again.
2. After three attempts, we must be able to display a message asking him to contact us.

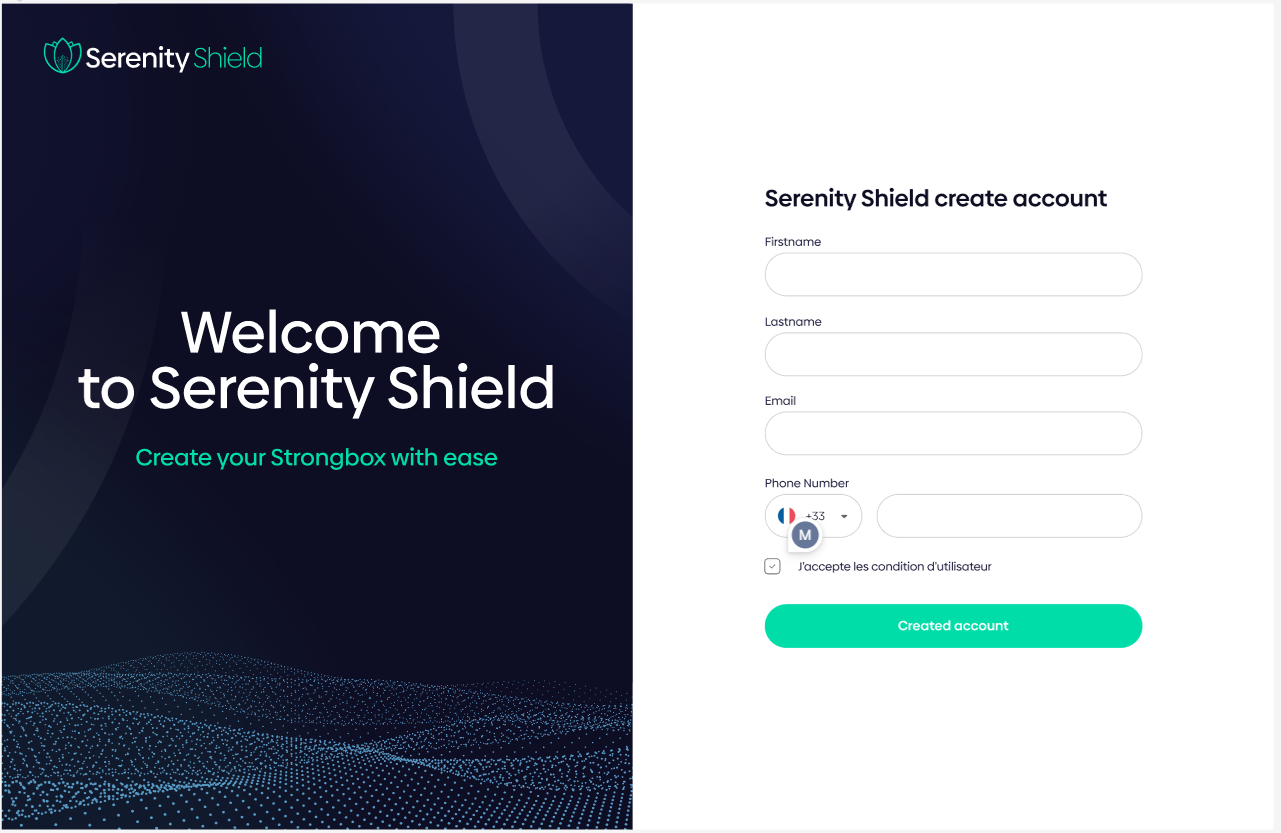
***Standard Scenario 03 - The customer has his right Wallet key but a connection error***

* Same procedure as a scenario 2.

***Standard Scenario 04 - The Customer Create a New Account***

1. The customer must fill in the fields that are proposed to him.
2. Upon receipt of the information the system sends him verification codes by Email and SMS.
3. The codes are correct, the Customer is directed to the Home page.

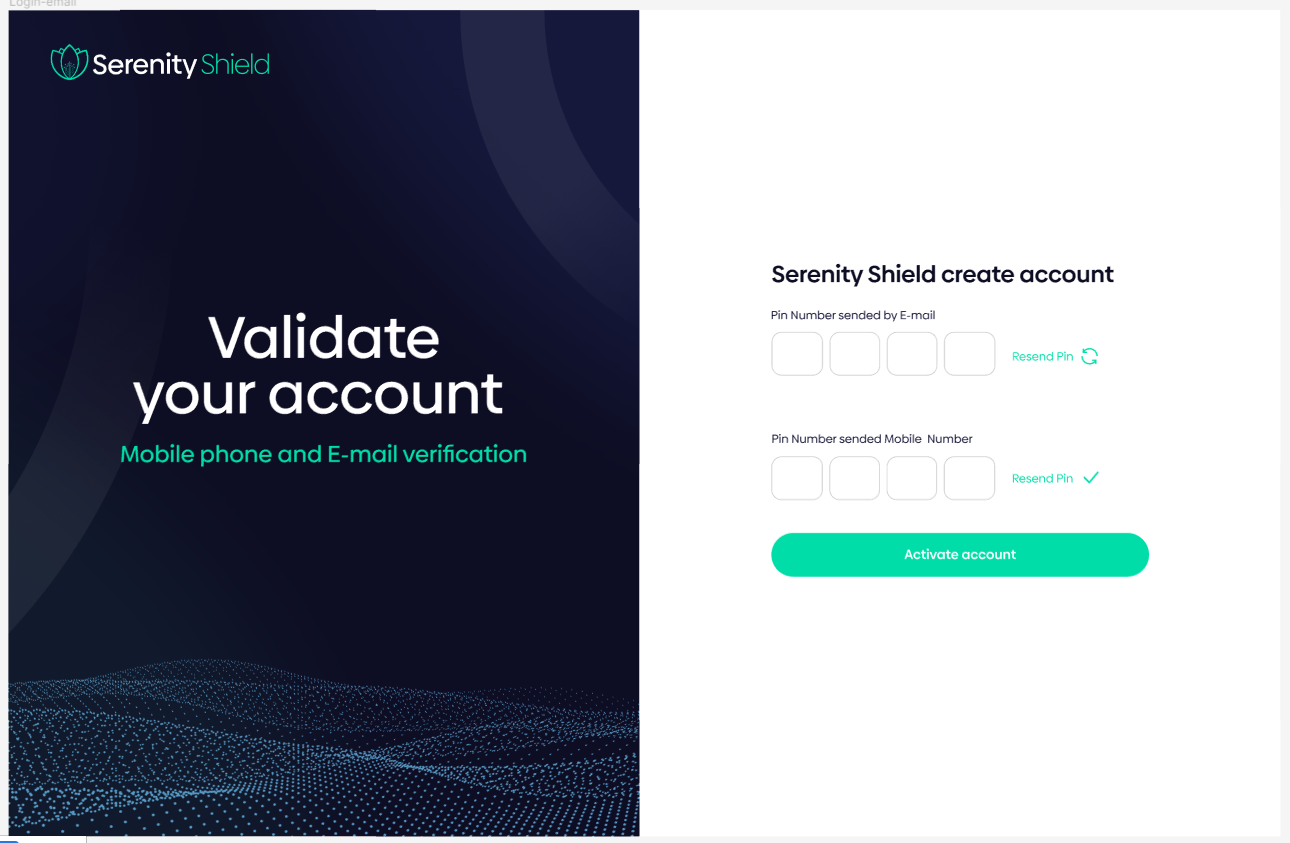
**Annex 4 : Interface « Create Account »**



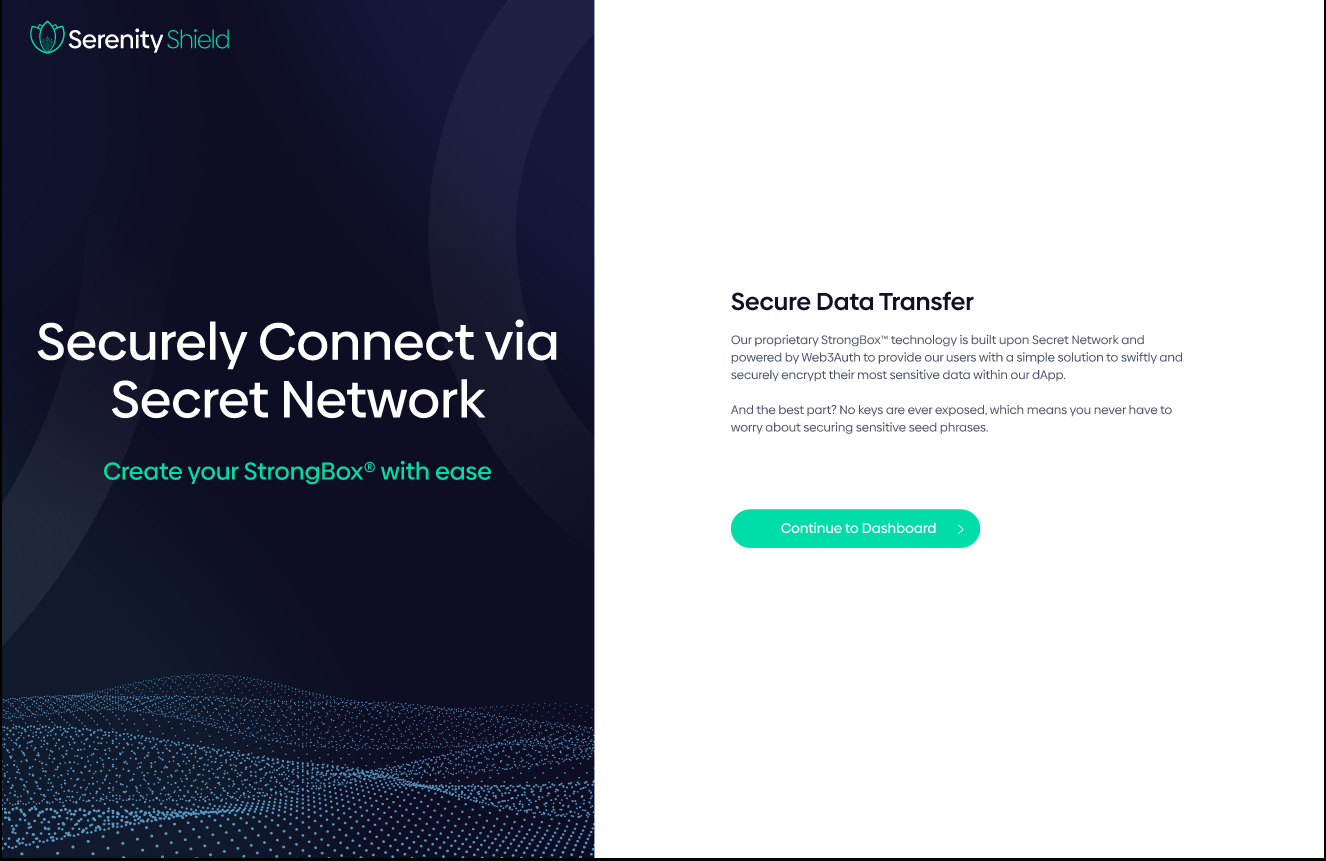
***Standard Scenario 05 - The Customer Create a New Account***

1. The customer must fill in the fields that are proposed to him.
2. Upon receipt of the information the system sends him verification codes by Email and SMS.
3. The verification is not conclusive, an information message offers him to fill in his codes.

**Annex 5 : Interface « Create Account in Progress »**



**Annex 5.1 : Interface « Secure Data Transfert »**



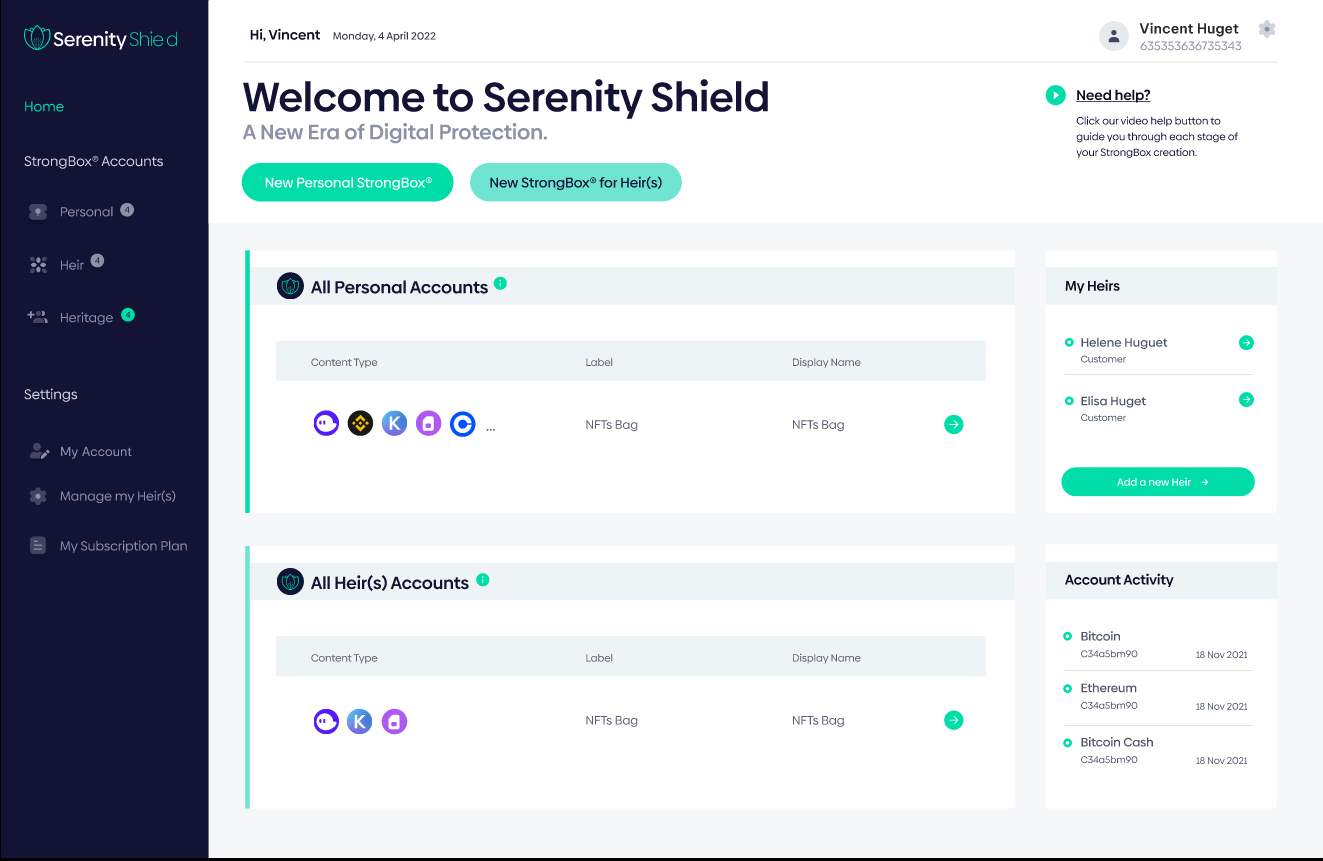
**2.3. Home**

In the Home page we have the view of all the strongboxes that have been created

Every element of this interface is clickable.

At the click we will get a window with the detail of the chosen element.

**Annexe 6 : Custom interface « Home»**



**"Home" Use Case**

***Standard Scenario 06 – Click on a row in All Personnal Accounts list.***

***Standard Scenario 07 – Click on a row in All Heir(s) Account list.***

1. The detail of the Strongbox is displayed in a window.

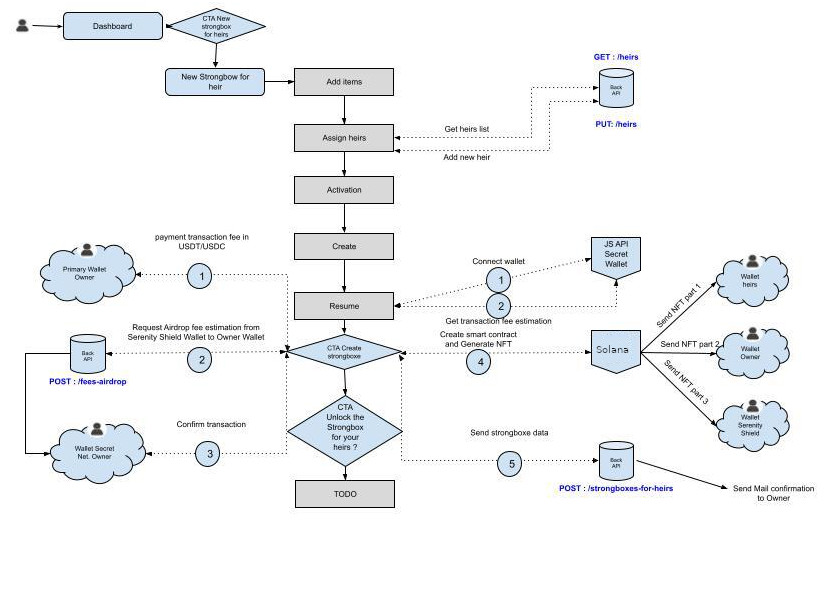
***Standard Scenario 08 - Click on a row in the my Heirs list.***

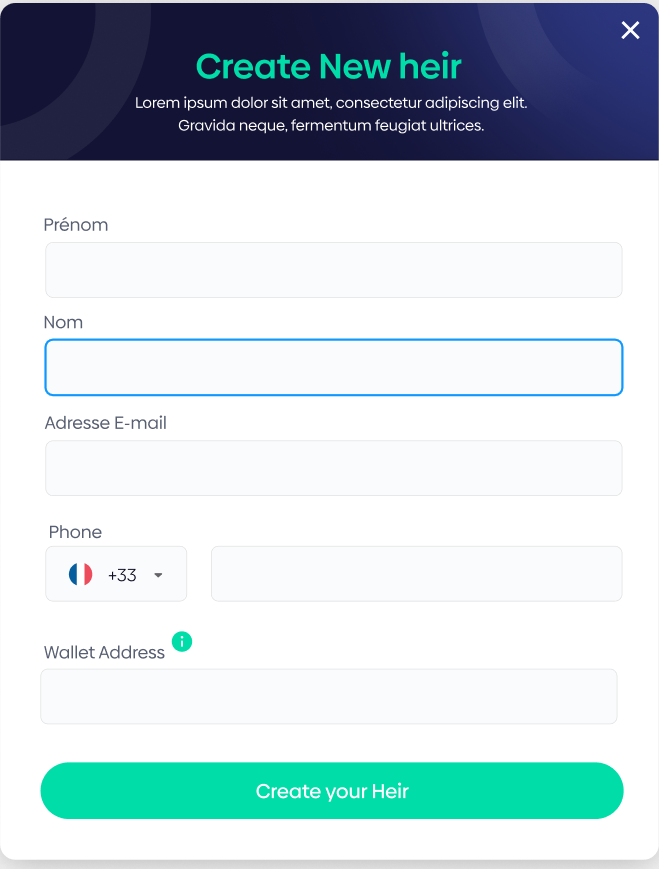
1. The detail of Heir is displayed in a window.

***Standard Scenario 09 - Click on the Add A Heir button.***

1. A window opens with fields to fill in.
2. After Validation of the fields the heir will be apparent in the list of Heirs of the Customer.

**Annex 7 : Interface « Create New Heir »**

****



We have a "New Personnal Strongbox" button and a " New Strongbox for Heir(s)".

These buttons work in the same way, but the objects created are typed differently.

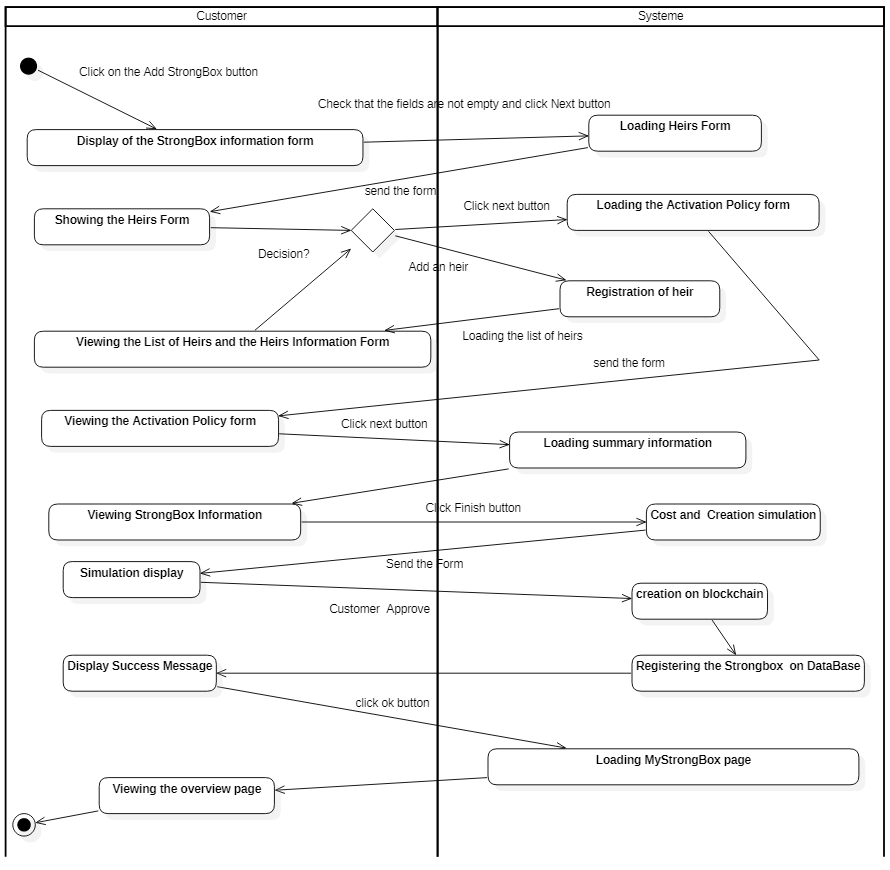
We take the most complex case as an example, the creation of strongbox for Heirs. NEED WALLET ADDRESS !

***Standard Scenario 10 - Click on the New Strongbox button.***

1. The customer will have to fill in all the fields.
2. The Process is carried out by a Wizard.

The diagram below explains the logic of creating the strongbox.

**Annex 8: << Detailed diagram of the construction of the Strongbox >>**



The process is done in 6 steps that we detail through activities.

Activity Step 1 Filling in StrongBox Information

Activity Step 2 Filling in Heirs Information

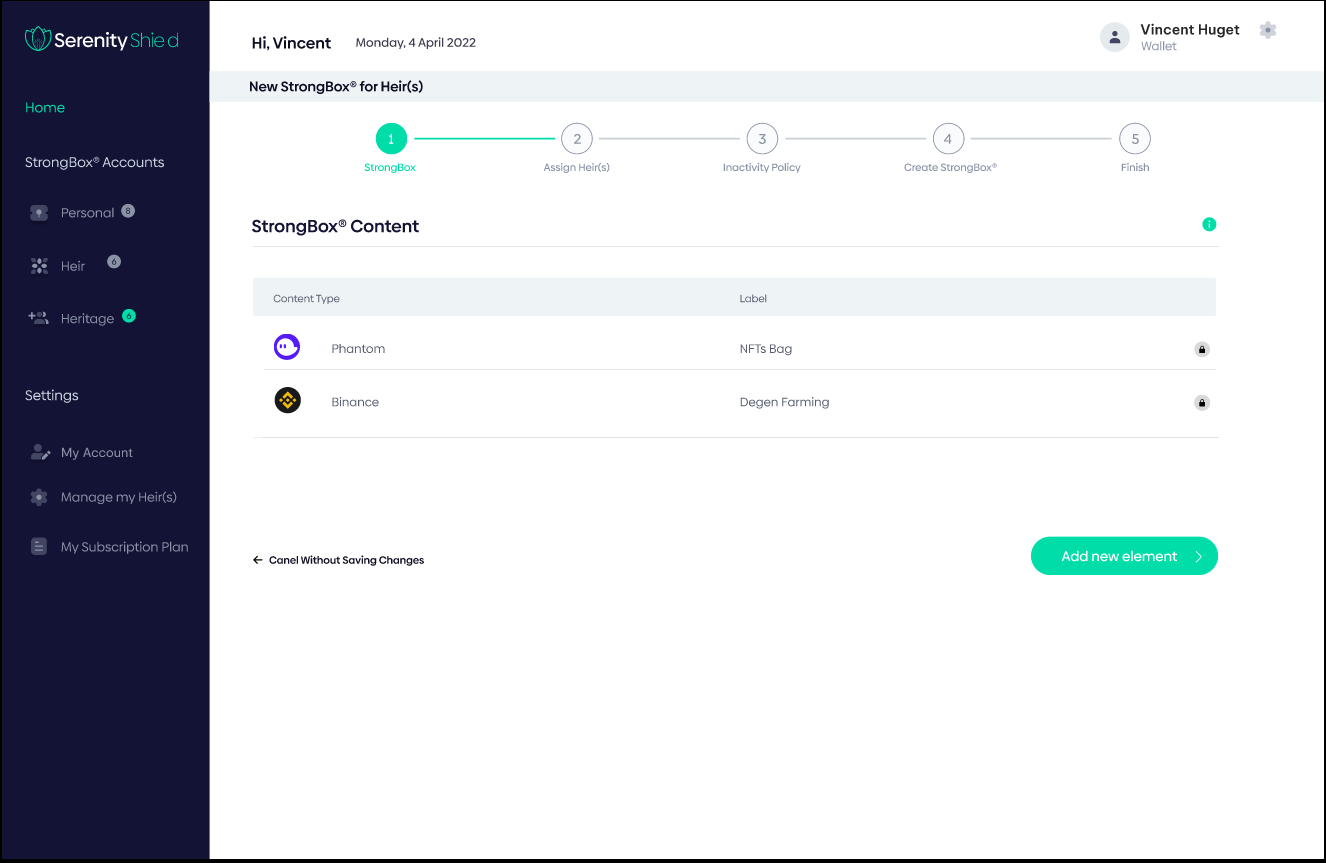
Activity Step 3 Activation Rules

Activity Step 4 Resume

Activity Step 5 Cost Estimate

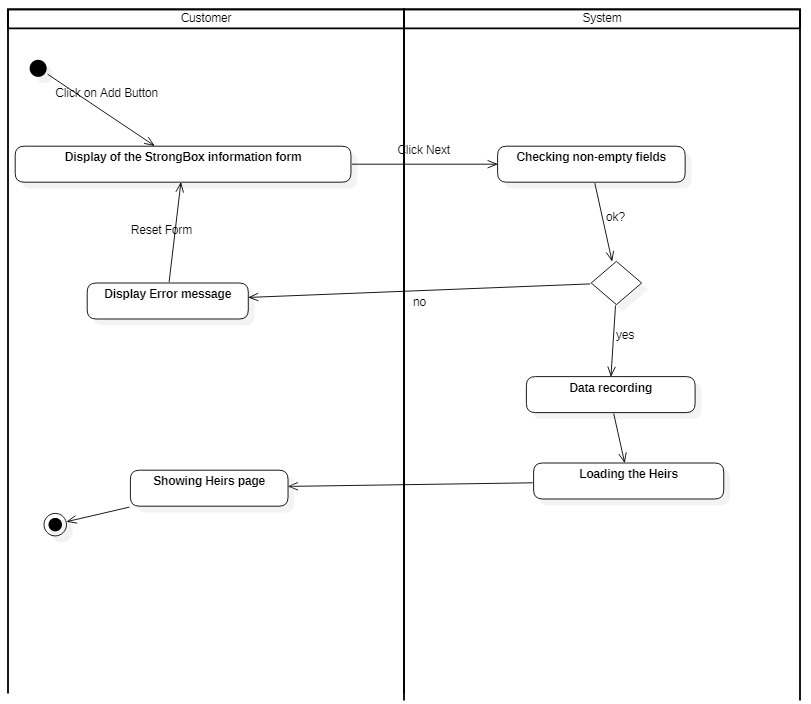
Activity Step 6 Finish

**Annex 8 :** **<< Strongbox ‘s Interface >>**

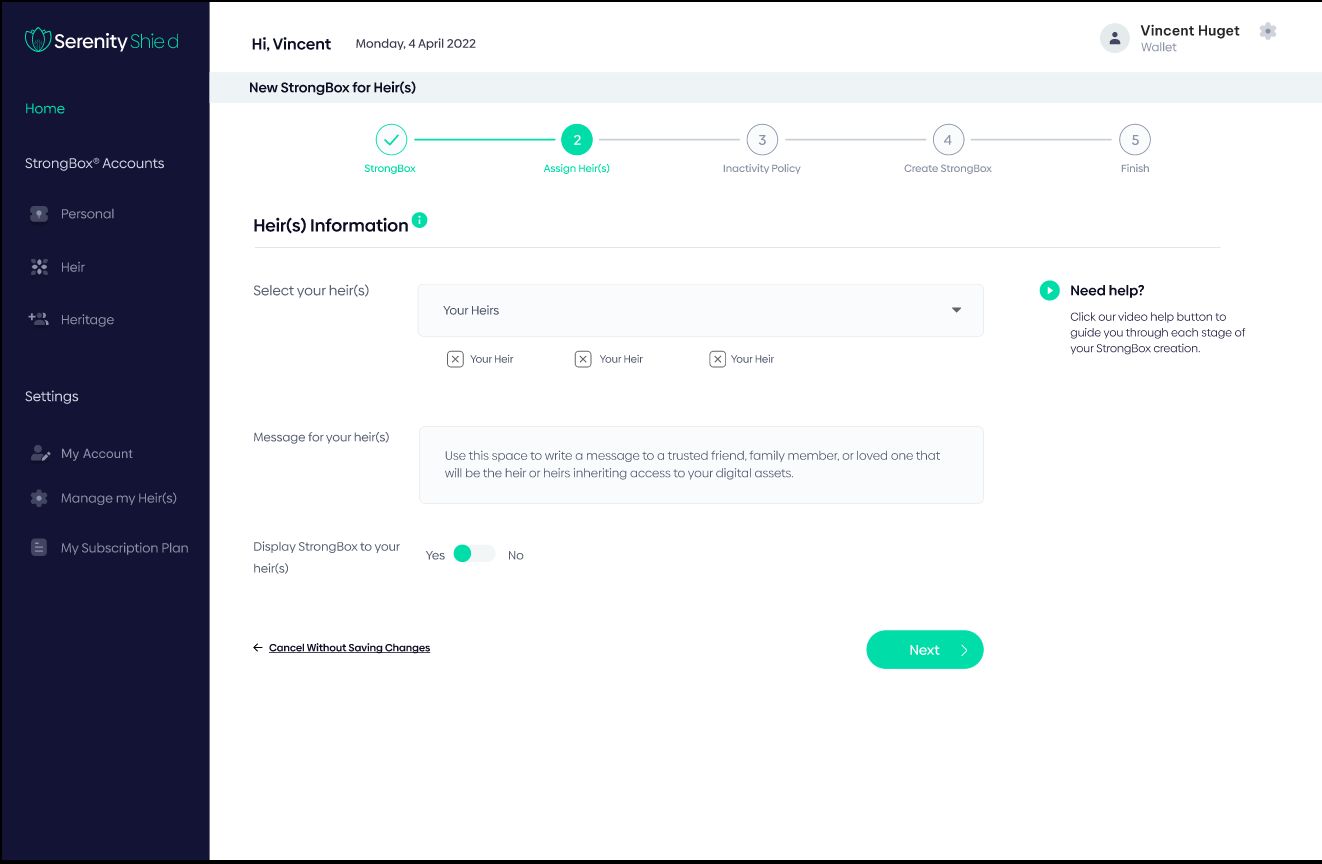


***Standard Scenario 10.1-Strongbox Information***

1. The customer must select a Strongbox Type.
2. The Seed is generated by our system.
3. The Client may write a message for his heirs.
4. The customer must fill in a Label.

 **Annex 9: << Strongbox activity diagram >>**

**Annexe 10 : << Interface Heirs >>**



***Standard Scenario 10.2.1 - All Heirs are listed***

1. The customer must select one or more heirs from the Dropdownlist.
2. The name of each heir is visible in the allocated text box.

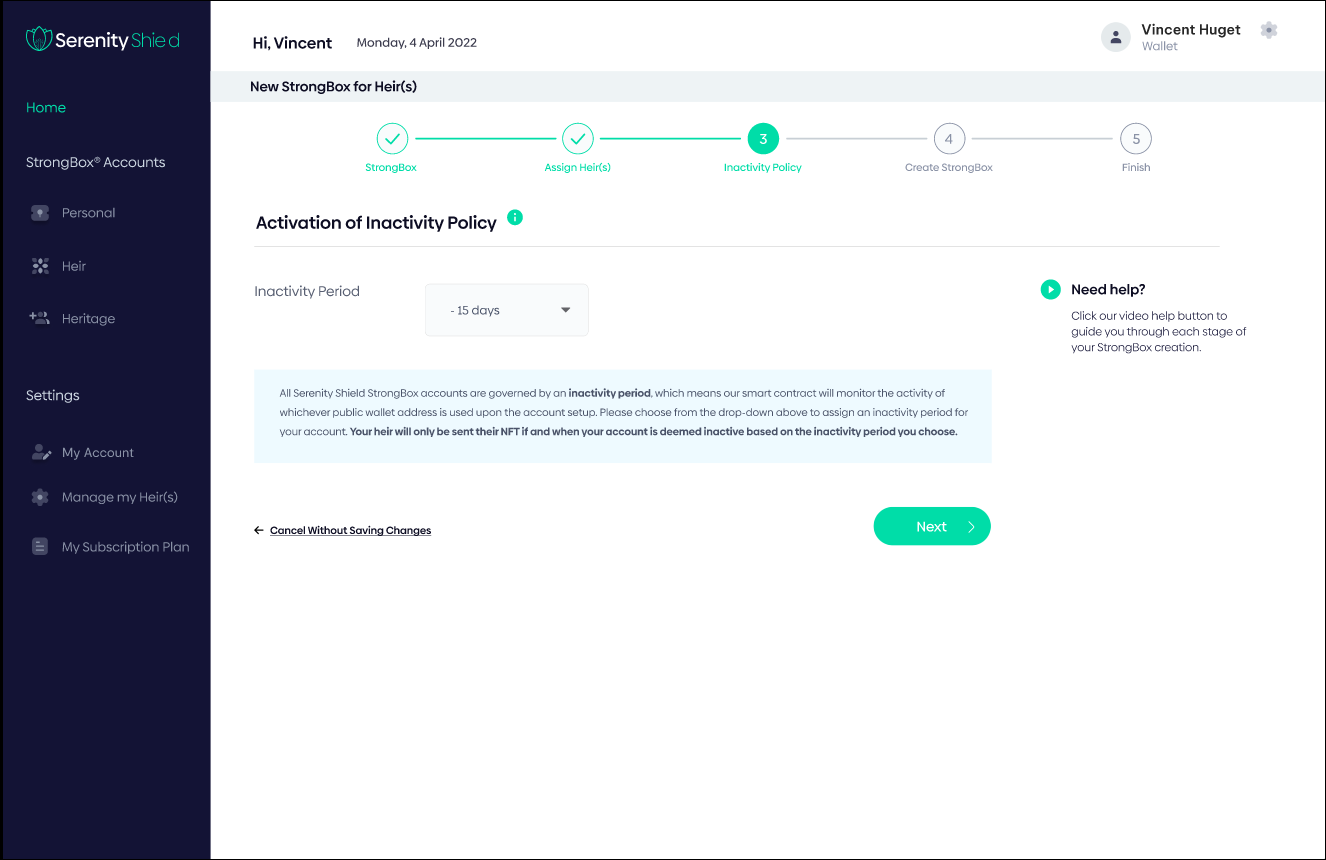
***Standard Scenario 10.2.2 - Not all Heirs are listed.***

1. The customer must select one or more heirs from the Dropdownlist.
2. The name of each heir is visible in the allocated text box.
3. Le client clique sur «  Add a New Heir »
4. The "Create a Heir" form appears.
5. The client fills in the fields.
6. Inherit it is in the list.
7. The customer can choose it.

***Standard Scenario 10.2.3 - Heirs are not listed***

1. Le client clique sur «  Add a New Heir »
2. The "Create a Heir" form appears.
3. The client fills in the fields.
4. Inherit it is in the list.
5. The customer can choose it.

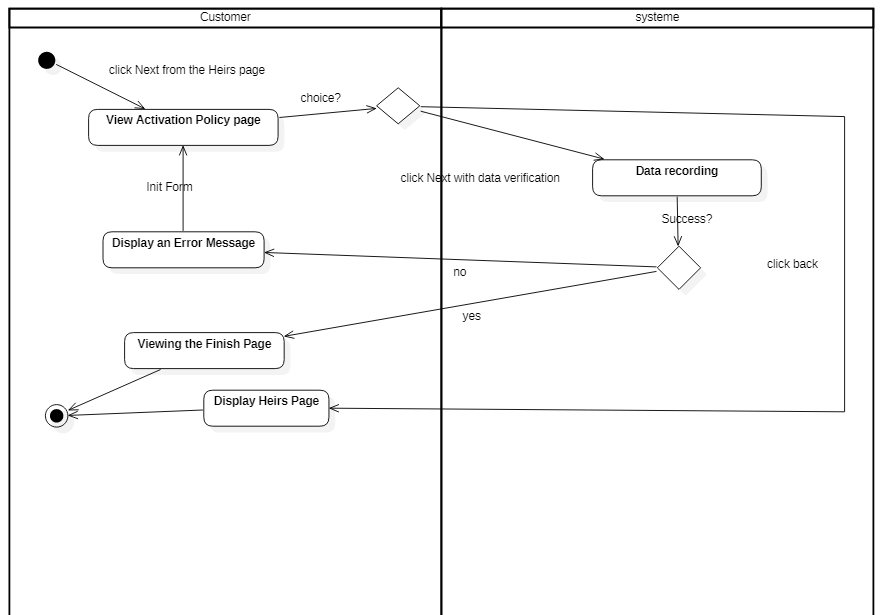
**Annex 14 : << Interface Activation of inactivity Policy >>**



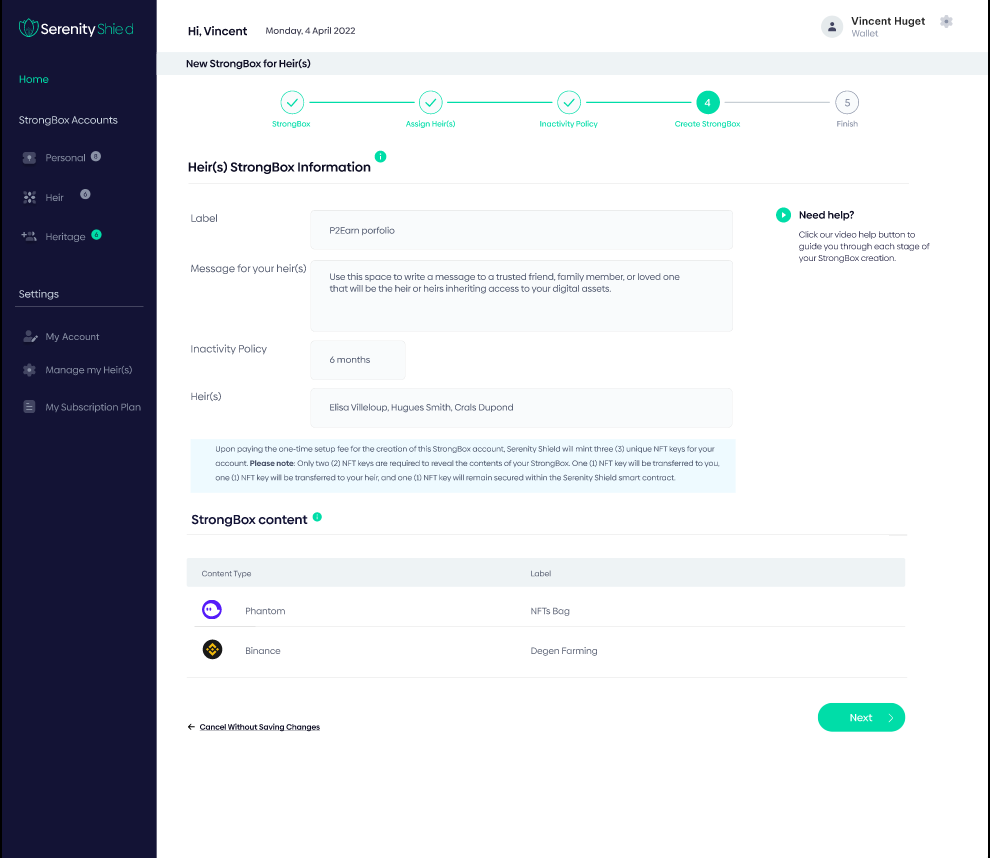
***Standard Scenario 11.3 – Choice of inactivity period.***

1. The customer must choose a period predefined by our system.

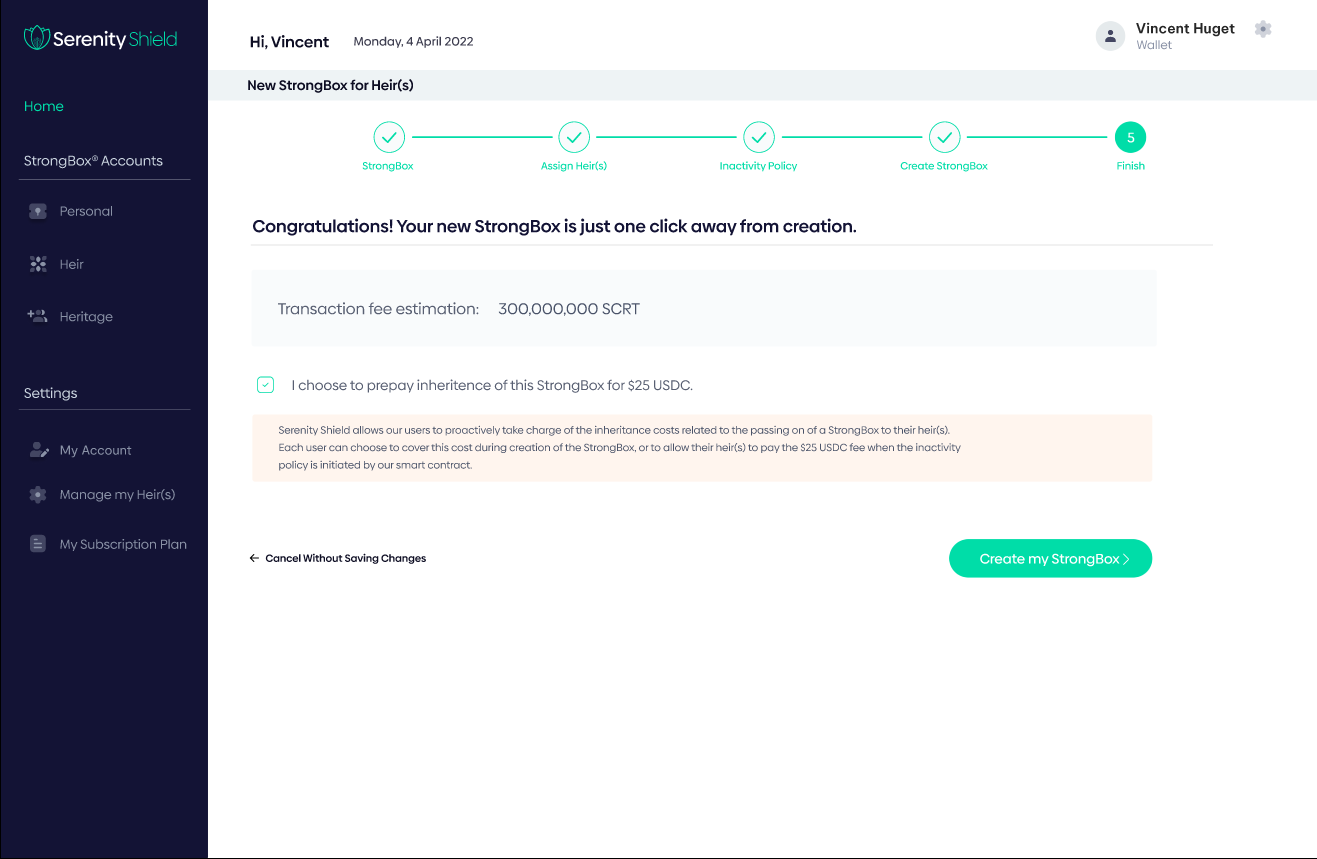
**Annex 15 : << Diagram Policy Activation >>**



**Annex 16 : << Interface Resume >>**



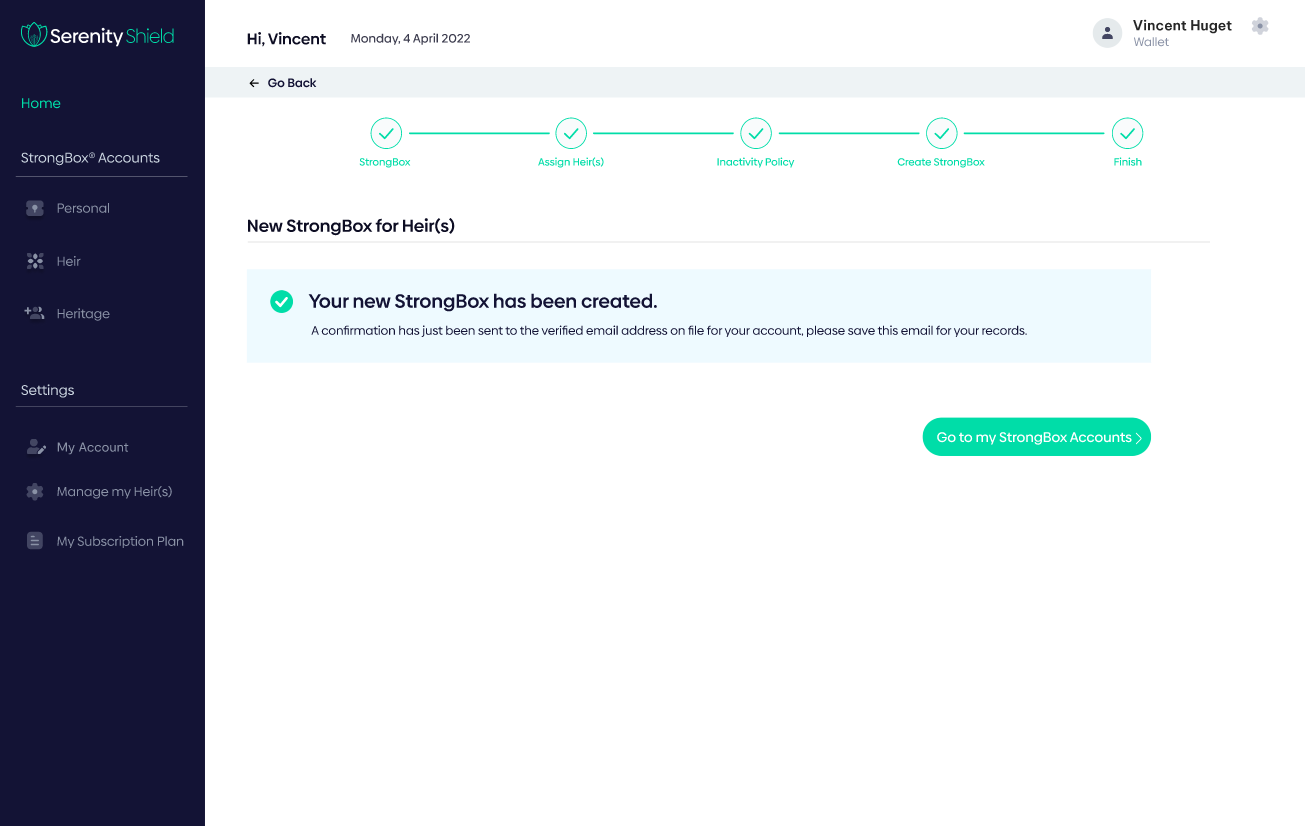
**Annex 17 : << Interface Estimation >>**



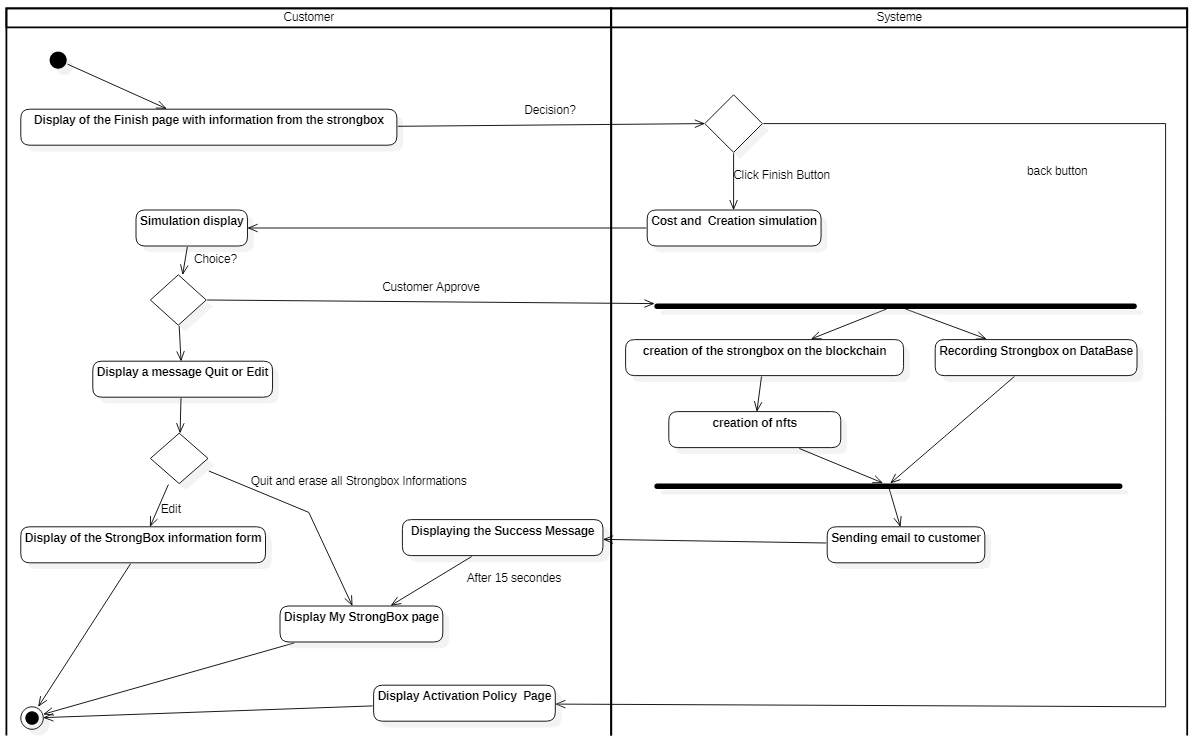
An estimation of the Gaz fees necessary to create the smart contract on Secret Network is displayed in real time to inform the user about the cost.

These fees are already paid in the initial cost subscription, hence, the user don’t have to pay something else.

**Annex 18 : << Interface finish >>**

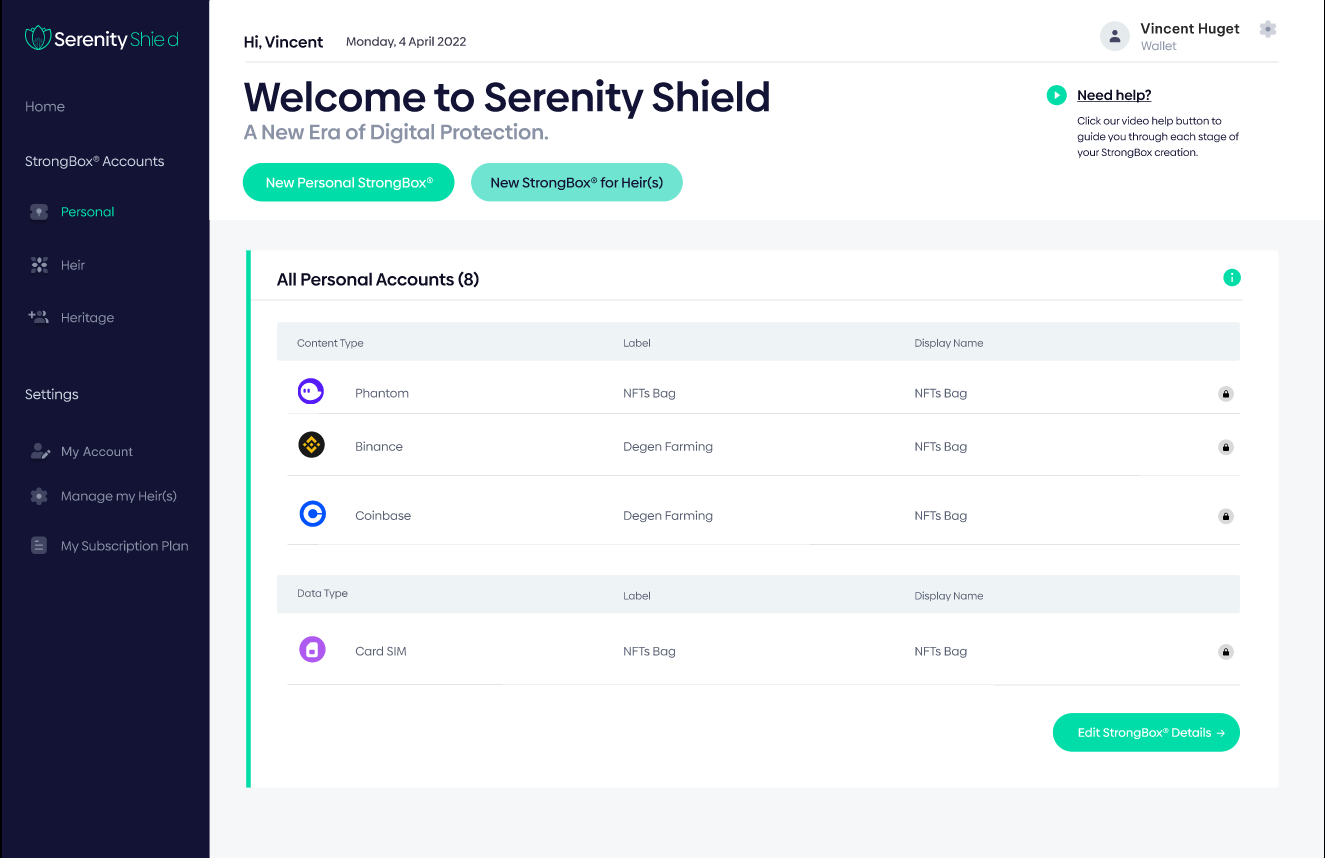


**Annexe 19 : << Diagram Finish >>**



**2.4. Personal**

**Annex 20 : << Personal >>**



**«Personal»** use cases

***Standard Scenario 11 - Click on the New Strongbox button.***

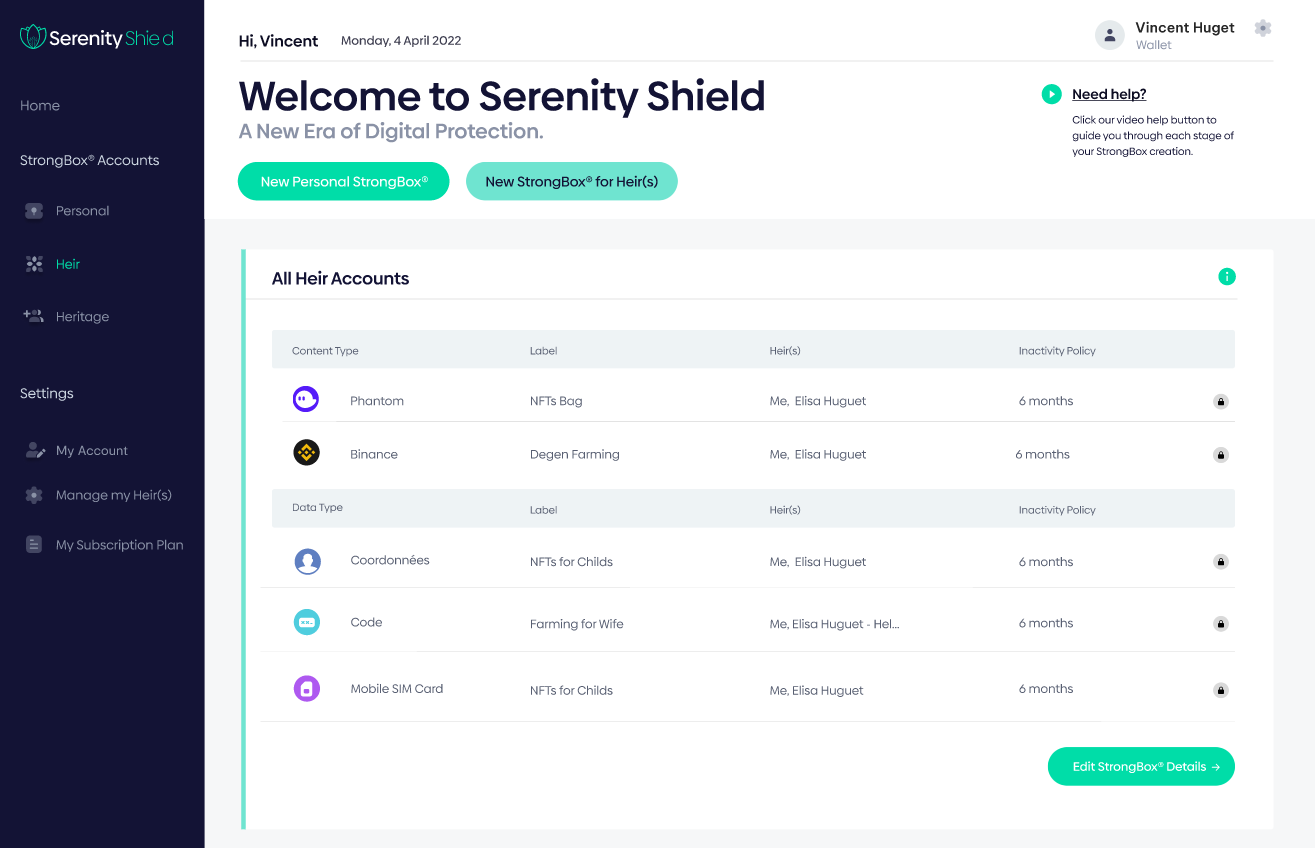
1. See standard scenario 10.

***Standard Scenario 12 - Click on a row in the My Strongboxes list.***

1. See standard scenario 06.
2. The customer will be able to Edit, Delete and Insert a Solo Strongbox from its Menu.

**2.5. Heir(s)**

**Annex 21 : << Heir(s) >>**



**«Heir(s) »** Use Cases

***Standard Scenario 13 - Click on the New Strongbox button.***

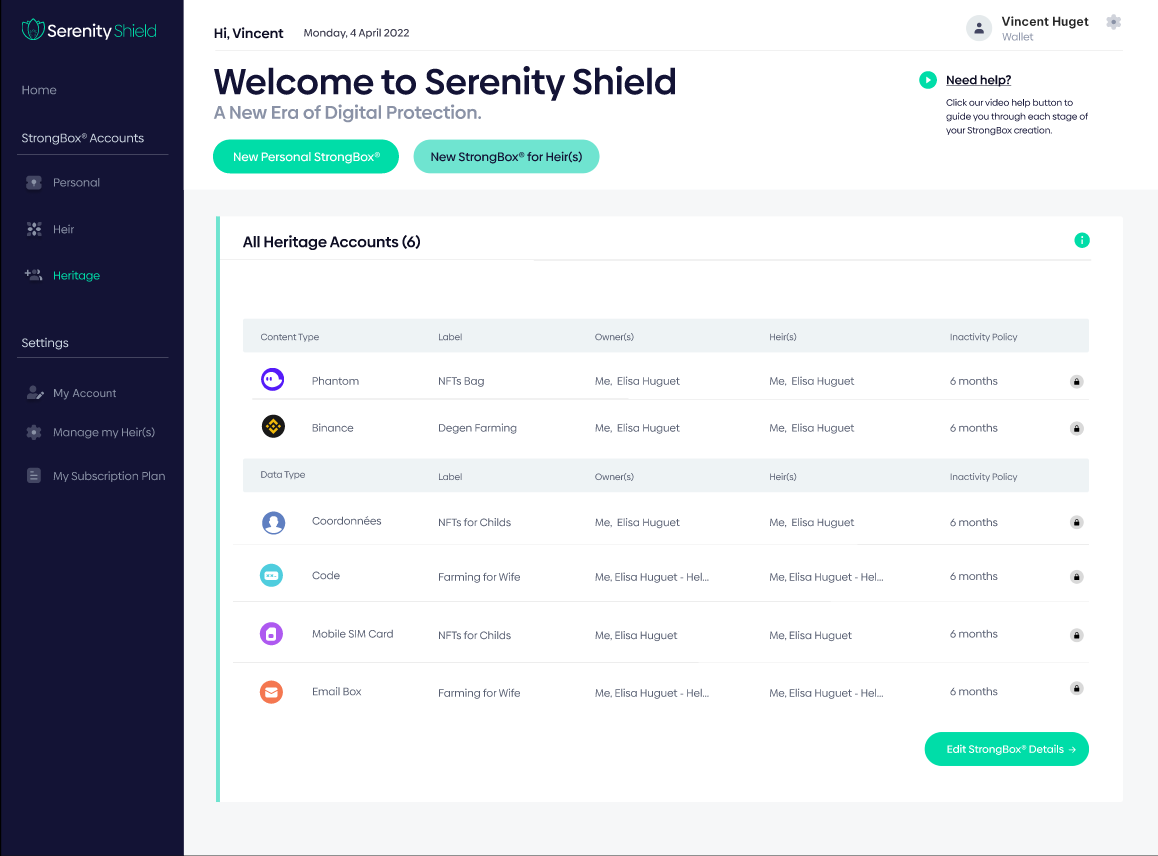
1. See standard scenario 10.

***Standard Scenario 14 - Click on a row in the My Strongboxes list.***

1. See standard scenario 07.
2. The customer will be able to Modify, Delete and Insert a Strongbox For Heir from this Menu.

**2.6. Heritage**

**Annex 22 : << Heritage >>**



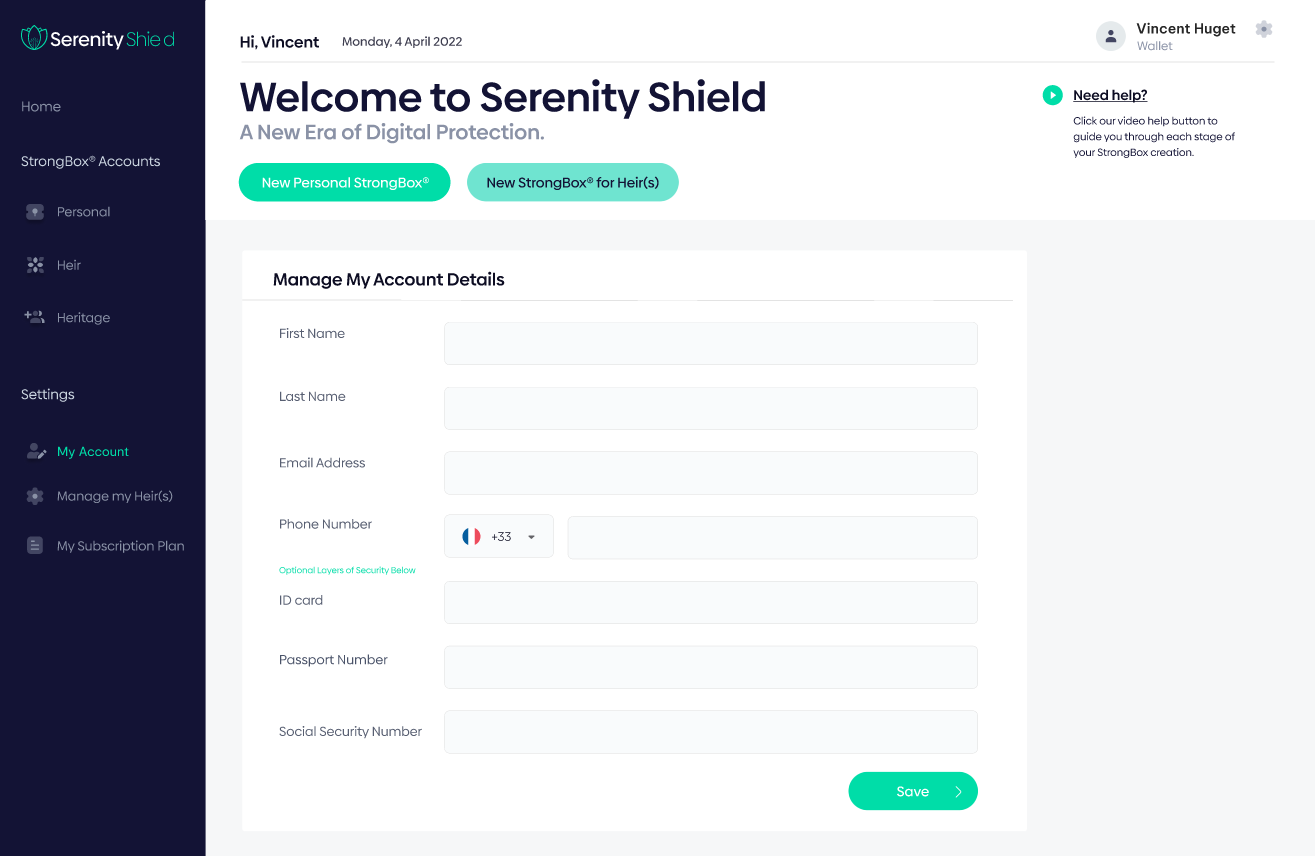
**"Heritage"** Use Case

***Standard Scenario 15 - Clicks one of the rows in the lists.***

1. The customer will be able to see the detail of the Strongbox or it has been defined as inherit.
2. The Customer only has a right to read.

**2.7. My Account**

**Annex 23 : << My Account >>**



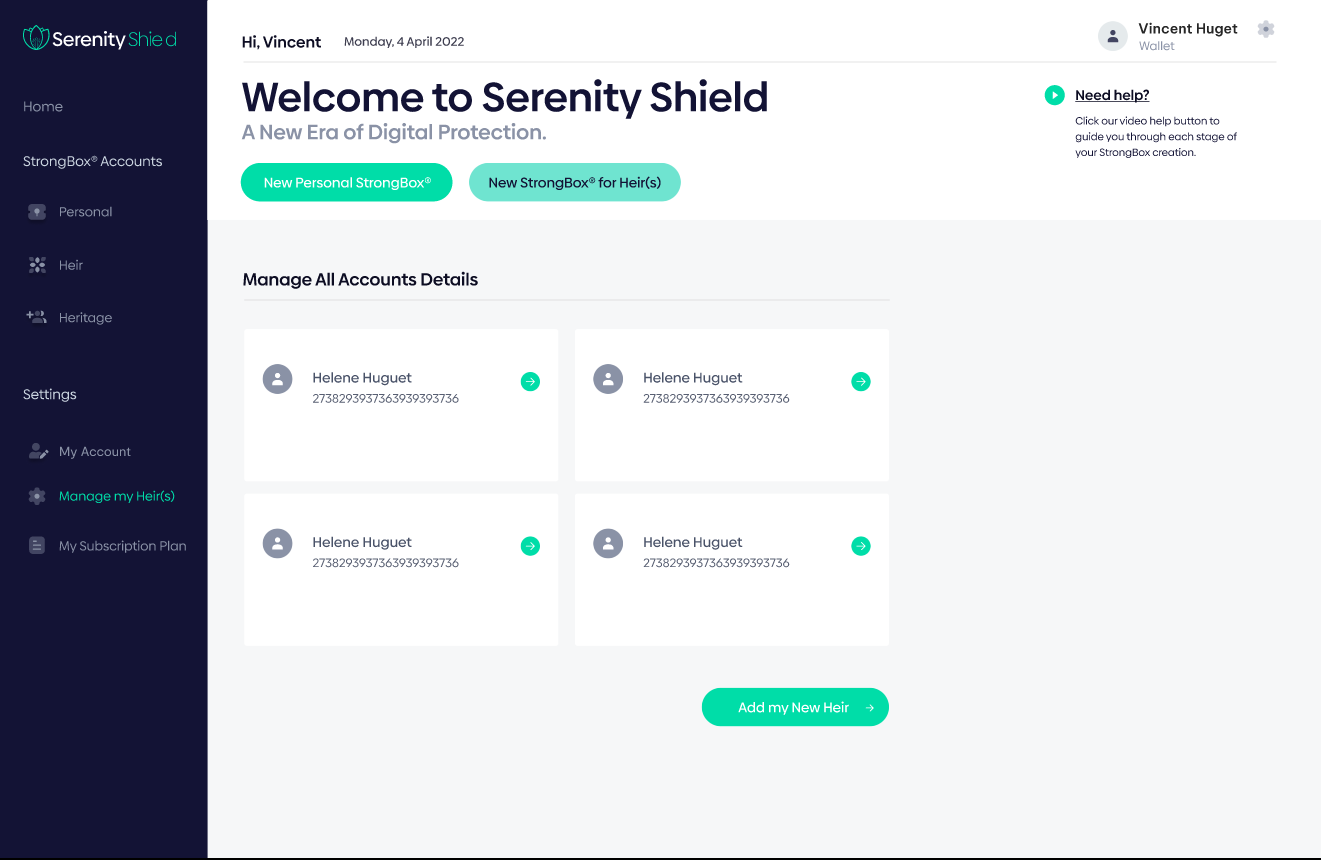
**"My Account"** use case

***Standard Scenario 16 -Filling in the fields concerning your account.***

1. The customer sees his fields pre-filled, he can modify them (only the Fields Social Security, ID number and Passport Number are Optional).

**2.8.** **Manage My Heir(s)**

**”Manage My Heir(s)”- Use Case**

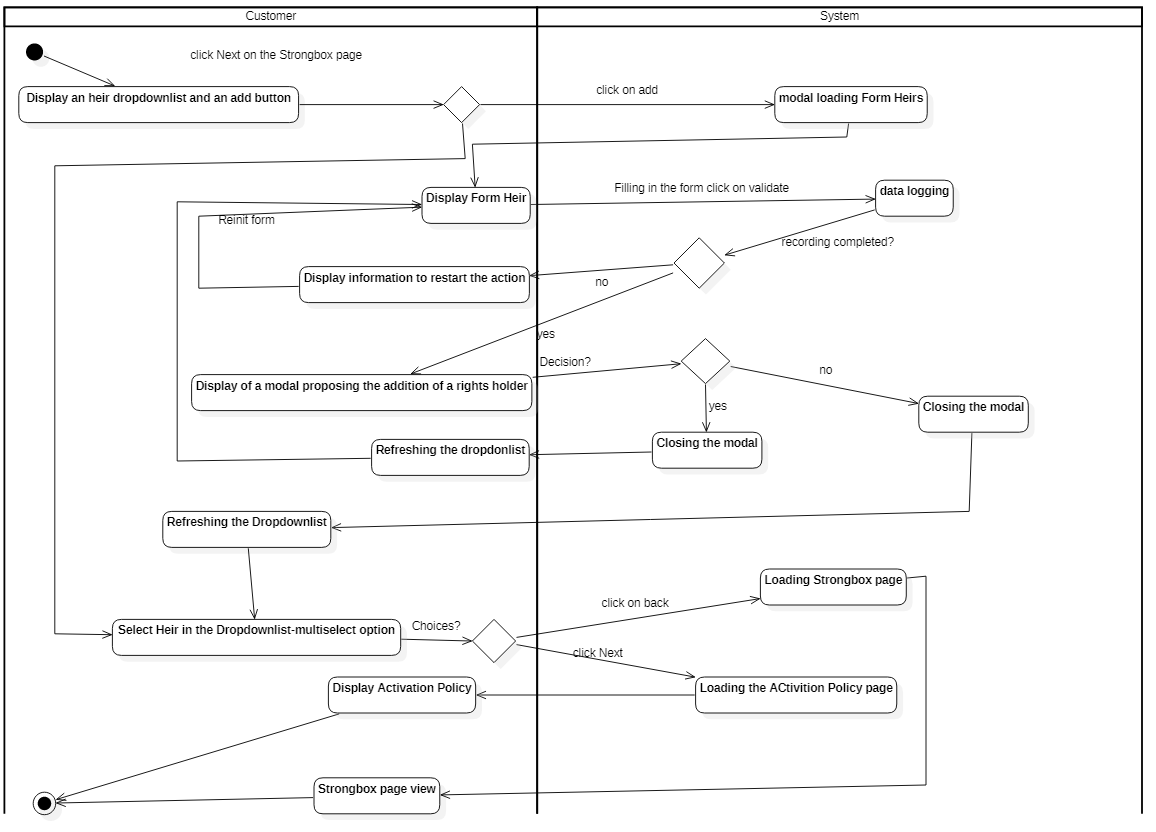


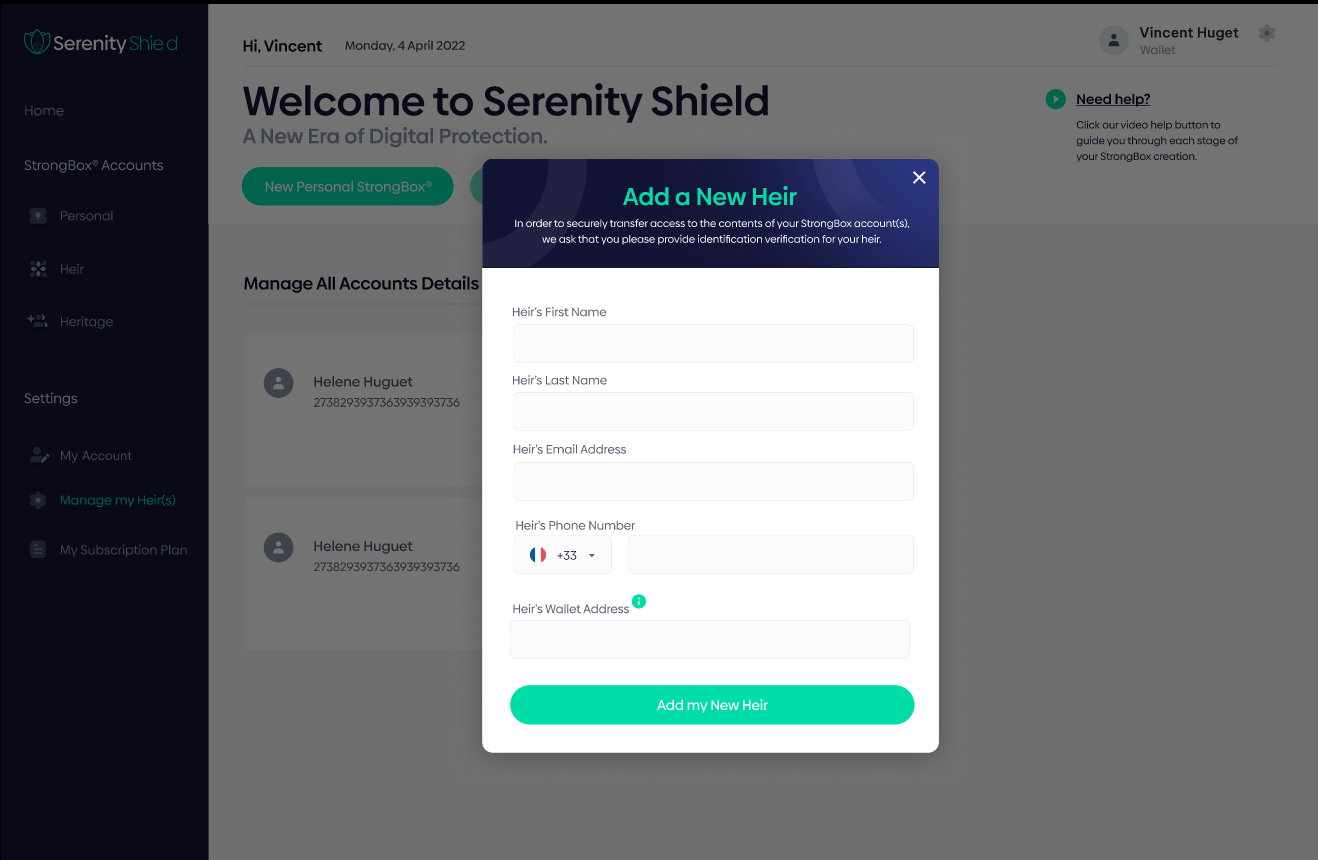
***Standard Scenario 17 -click on “Add heir(s)”.***

1. The customer sees the file of his heirs and can add others.
2. The Customer must fill in all the fields concerning his heir.

This diagram illustrates how the add-on works logically.

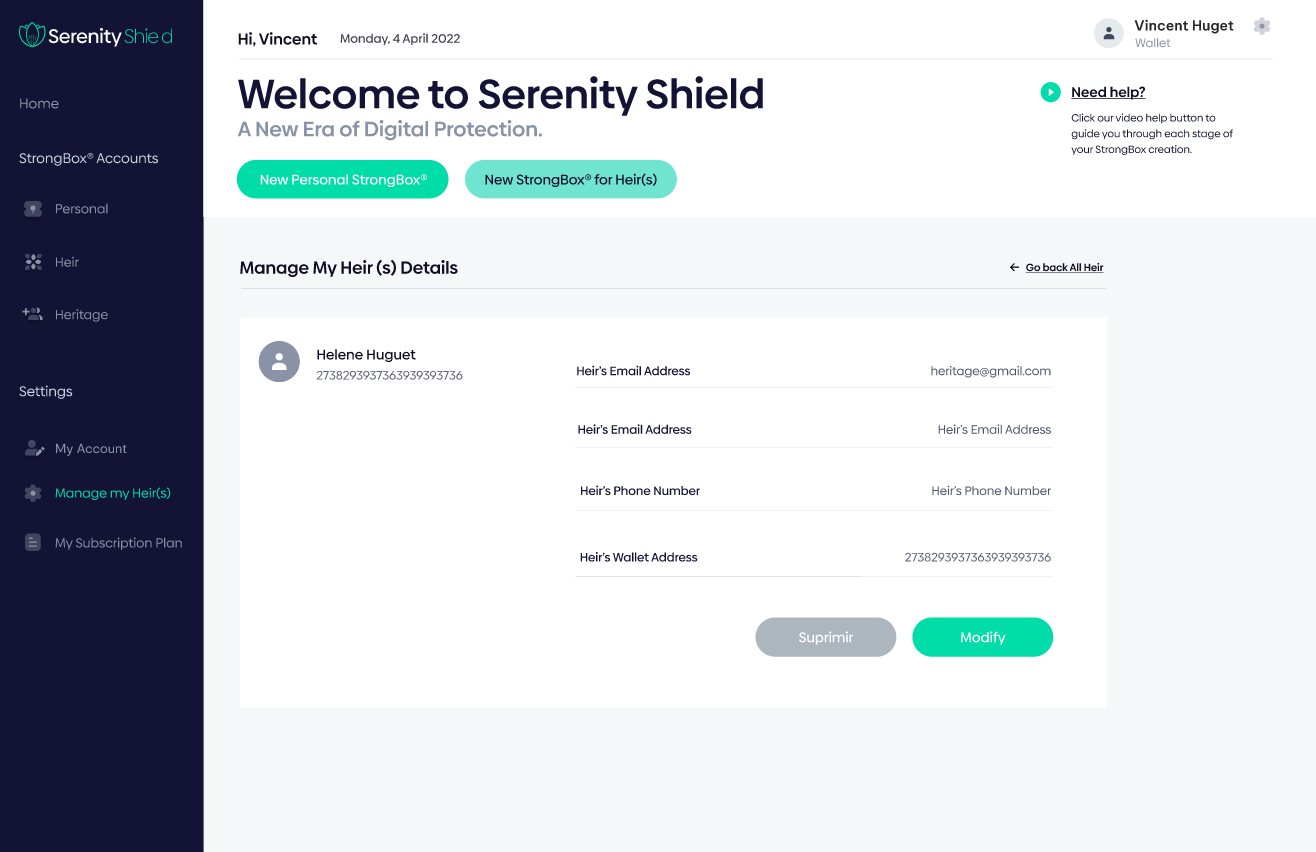
**Annex 11 : << Add Heirs** **diagram >>**





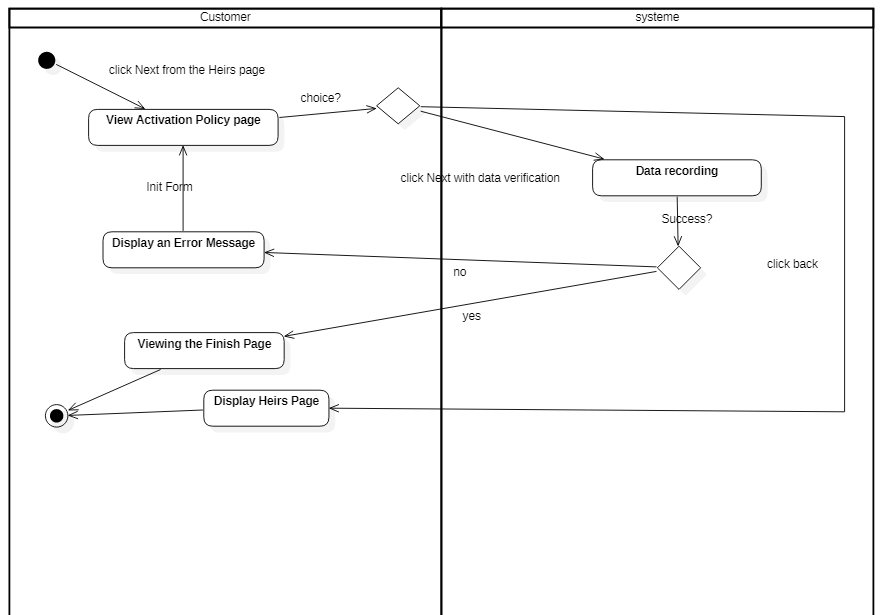
***Standard Scenario 18 -Update an Heir***

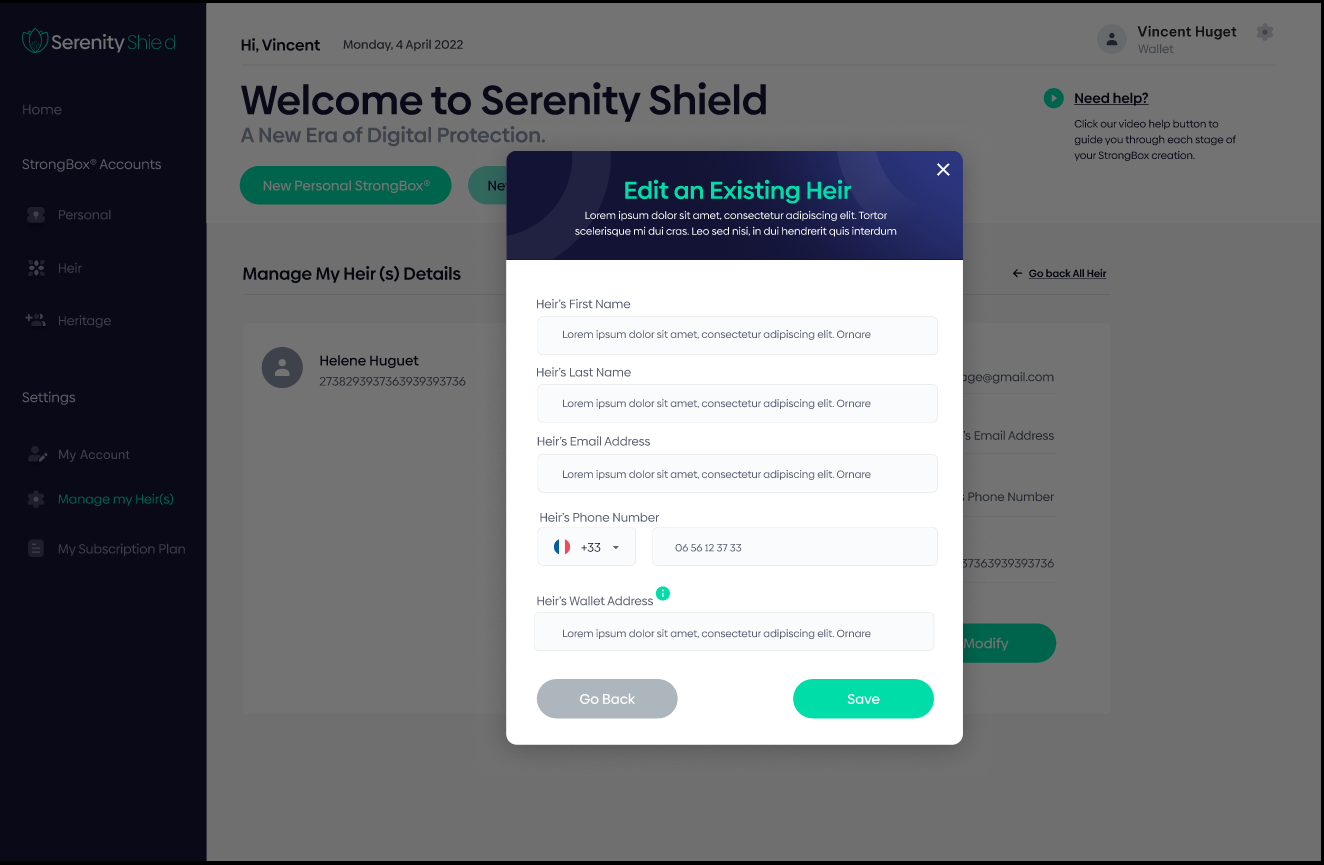
1. The customer sees the file of his heirs and can add others.
2. The Customer click on a heir file
3. He can “modify” and Save



This diagram illustrates the change

**Annex 12 : << Diagram the Heirs modification >>**



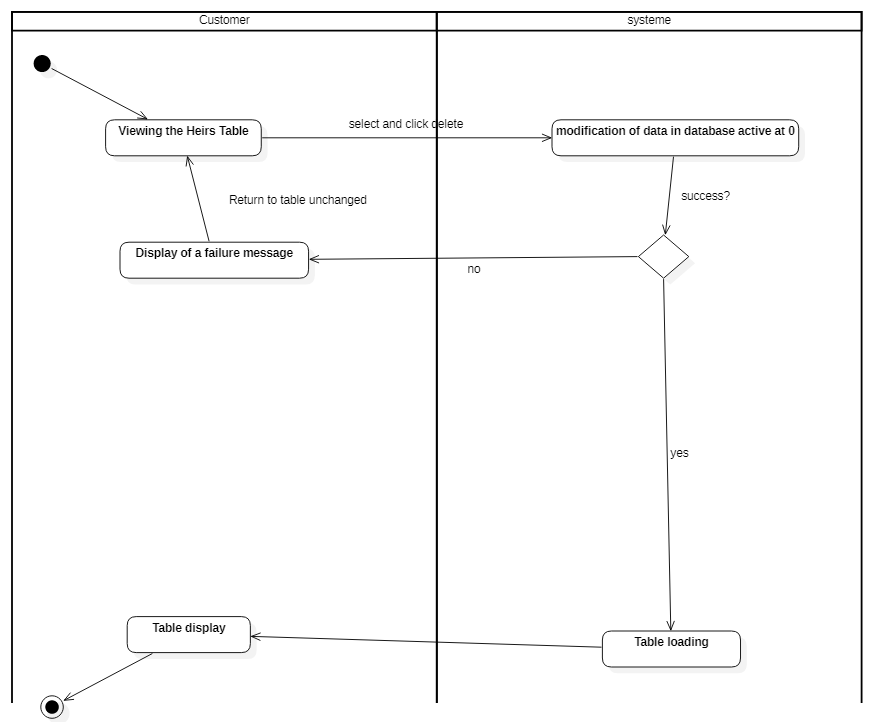


***Standard Scenario 19 -Delete an Heir***

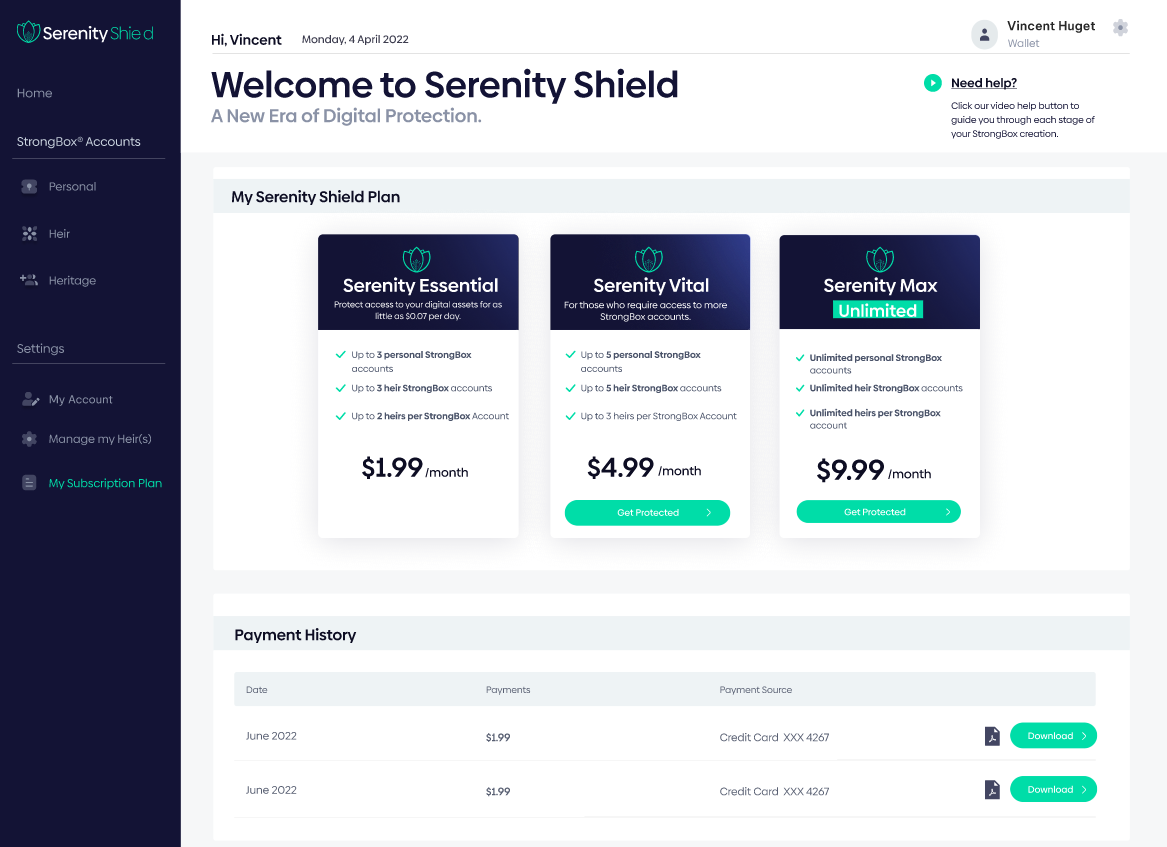
1. The customer sees the file of his heirs and can add others.
2. The Customer click on a heir file
3. He can “Delete” and Save

This diagram illustrates the deletion

**Annex 13 : << Heirs removal diagram >>**



**2.9.** **My Subscription Plan**



**Use Case - "****My Subscription Plan" Menu**

***Standard***  Scenario ***20 - Choosing the "*My Subscription Plan*" menu - Reading a message***

1. The Customer may choose his purchase plan in this Menu.
2. The Customer will be able to consult his purchase history.

**3. Data Dictionary**

**3.1 Users (Customers and Heirs)**

Les données relatives à la gestion des utilisateurs sont :

|  |  |
| --- | --- |
| Firstname | VARCHAR 255 |
| Lastname | VARCHAR 255 |
| Email | VARCHAR 255 |
| Phone Number | VARCHAR 255 |
| ID Number (optional) | VARCHAR 255 |
| Social Security Number (optional) | VARCHAR 255 |
| Passport number (optional) | VARCHAR 255 |

DEFINITION

1. Firstname: Represents the user name.
2. Lastname: Represents the user's first name.
3. Phone Number: is the user's phone number .
4. Email: is the user's email address.
5. ID Number: is the identity card number.
6. Social Security Number: is the socialsecurity node.
7. Passport number: is the passport number.

**3.2** **StrongBoxes**

Data relating to strogboxes are :

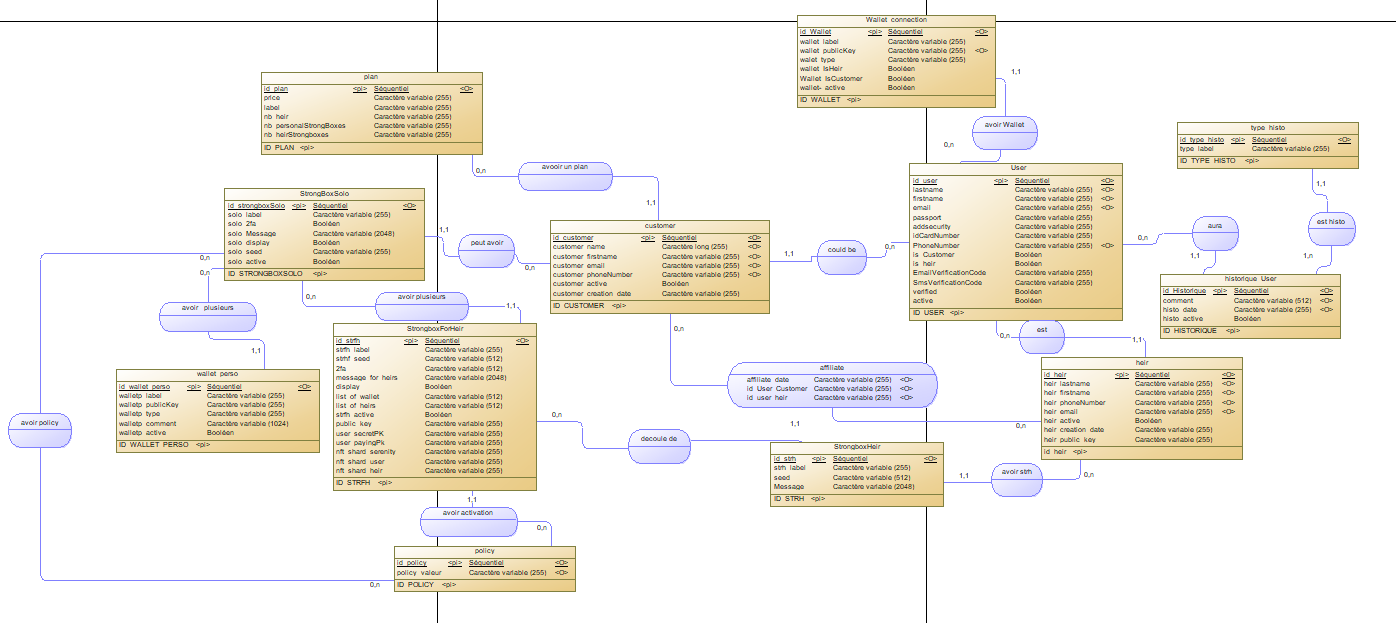
|  |  |
| --- | --- |
| Label | VARCAHAR 255 |
| List of Strongbox Type | VARCAHAR 512 |
| Seed | VARCAHAR 512 |
| 2FA System | BOOLEAN |
| Message for Heir | VARCAHAR 2048 |
| Display | BOOLEAN |
| List of Heirs | VARCAHAR 512 |
| Policy Activation | INTEGER |

DEFINITION

1. Label: represents the name of the strongbox.
2. List of Strongbox Type: Represents a list of strongbox type.
3. Seed: is the key phrase of the strongbox.
4. 2FA System:is the boolean for strongbox security.
5. Message for Heir: is the message for heritiers.
6. Display: is a boolean to show or not the strongbox.
7. List of Heirs: represents a list of strongbox heirs.
8. Policy Activation: represents a duration before activating the strongbox

* **4 Conceptual data model:**

**Annexe 24 : << Conceptual data model >>**



THANKS