ONG BITCOIN ARGENTINA

\Orchestrating a brighter world NEC

Introducción

Proyecto DIDI – Barrio 31

- El objetivo del proyecto es contribuir, en un principio, con la comunidad vulnerable del Barrio 31, para fomentar la Digitalización de sus habitantes y brindarles una herramienta para la carga de sus datos personales, experiencia laboral y estudios realizados; con el objetivo de ayudarlos a mejorar su inserción Laboral, bancarización e inclusión social en distintos Organismos; entre otros beneficios asociados a la necesidad de cada Usuario.

- La herramienta consta en desarrollar una App Android, basándose en tecnologías de Blockchain aplicado en Identidad Digital; pensado para la fácil adopción de Usuarios y Organismos Certificantes.

DIDI Identidad Digital para la Inclusión

Blockchain para habilitar un sistema social y económico naturalmente inclusivo y descentralizado.

Beneficios:

- Registro Electrónico de usuarios (online, offline, on-chain y off-chain).
- Identidad y Soberanía Digital de cada usuario.
- Descentralización de la Información de Usuarios y Organismos.
- Fácil usabilidad y adopción para Usuarios y Entidades interesadas.
- Certificados Digitales.
- Certificar la procedencia y validez de los datos de Usuarios.
- Organismos podrán validar la Identidad Digital y Datos de los usuarios solicitantes.
- Bajar Costos eliminando intermediarios.
- Seguridad: Encriptación Llave Publica y Privada. Criptografía.
- Tokenización de activos/productos y nuevas implementaciones.
- Estándares W3C.

ONG BITCOIN ARGENTINA

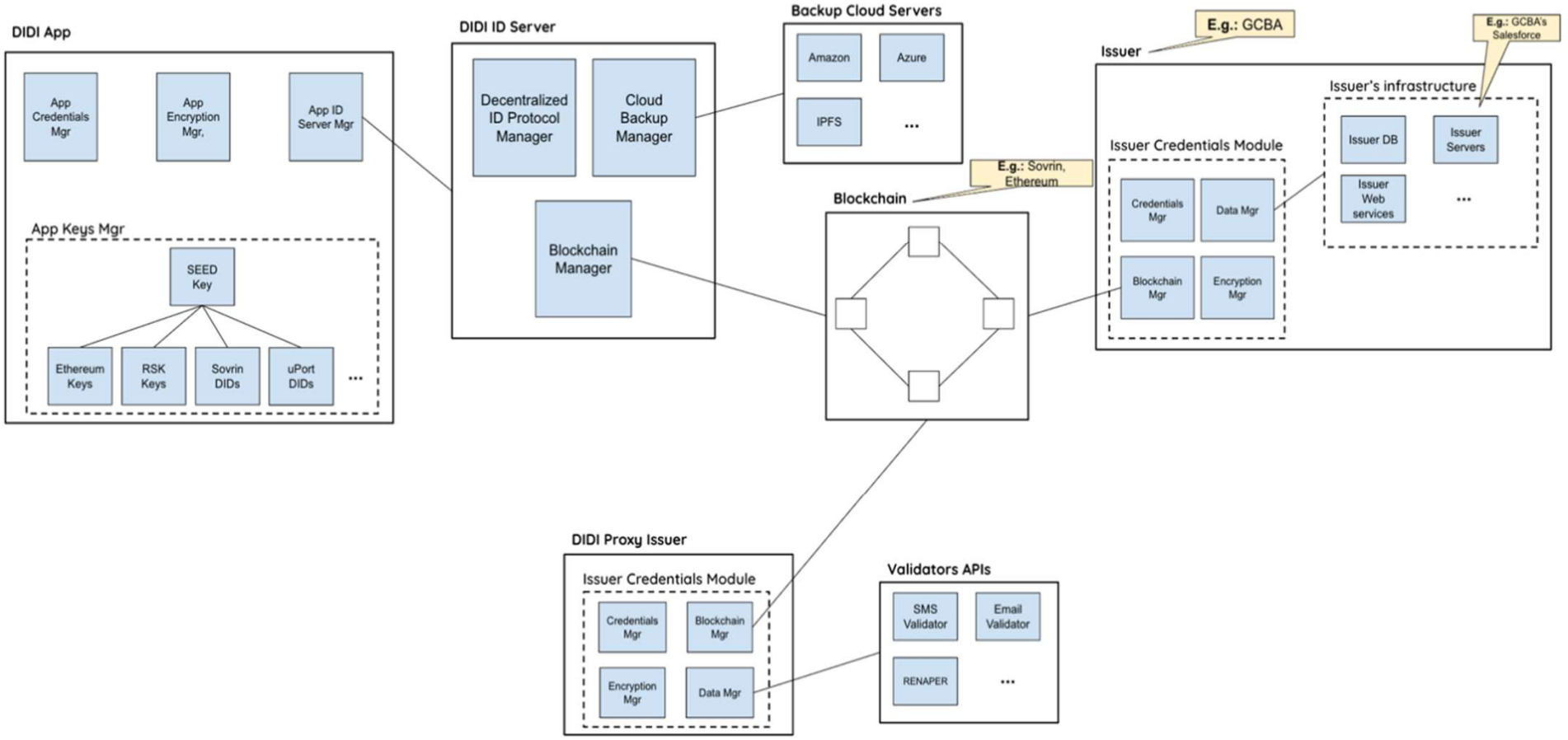
Orchestrating a brighter world NEC

Arquitectura

Resumen Ejecutivo

Diagrama de Arquitectura – Proyecto DIDI

ONG BITCOIN ARGENTINA



Resumen Arquitectura – Proyecto DIDI

Los distintos módulos serán los encargados de interactuar entre la App (usuario final) y las diversas entidades que componen este sistema.

Características del módulo:

Este módulo será compuesto por una serie de Managers para cada interacción que tendrá el sistema:

- **Cloud Backup Manager**: Interactúa con el Backup Cloud que gestiona las Copias de Seguridad de cada usuario.
- **Decentralized ID Manager**: Encargado de realizar todas las acciones pertinentes al Protocolo de Identidad Descentralizada utilizado; mediante la herramienta de uPort.
- **Blockchain Manager**: Gestiona las interacciones entre las siguientes tecnologias de Smart Contracts con Bockchains, en el Sistema.

  - **RSK Rootstock**: Smart Contract Platform Secured by the Bitcoin Network. Plataforma P2P sobre Bitcoin que permite la ejecución de contratos inteligentes.

  - **BFA Blockchain:** ***(Opcional en esta etapa)*** Red de Nodos Blockchain como base de datos distribuida y descentralizada, contributiva y abierta para organismos de investigación de BC en Argentina.

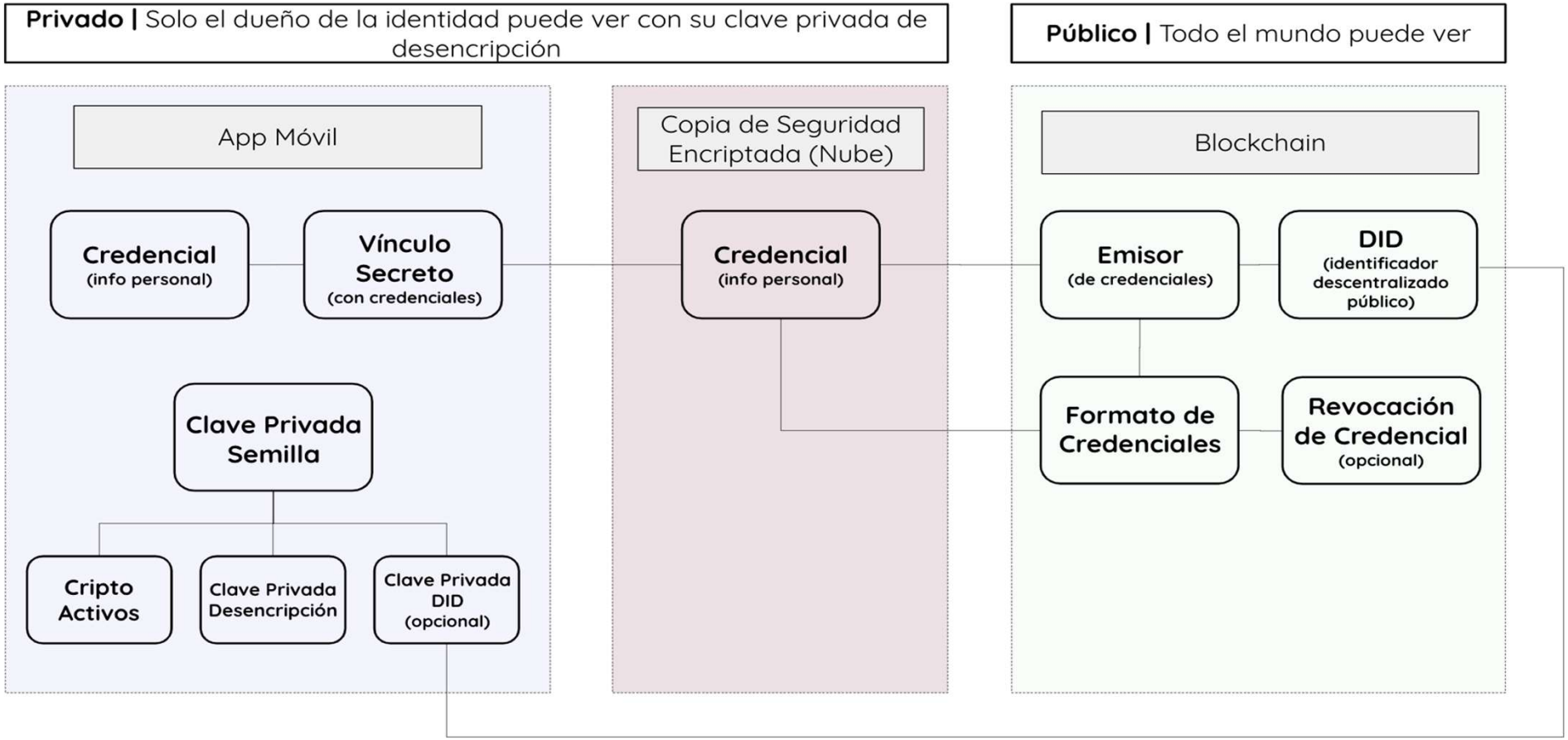
  - **BID LAC-Chain**: ***(Opcional en esta etapa)*** blockchain pública-permisionada, para que cualquier entidad pueda unirse a esta Blockchain Pública, con permisos previos del BID. Proyecto de red BC, aun no operativa plenamente por su recientemente lanzamiento, con alguna contribución de "Alastria España".

(en esta etapa NEC implementará 1 de estás 3 tecnologías)

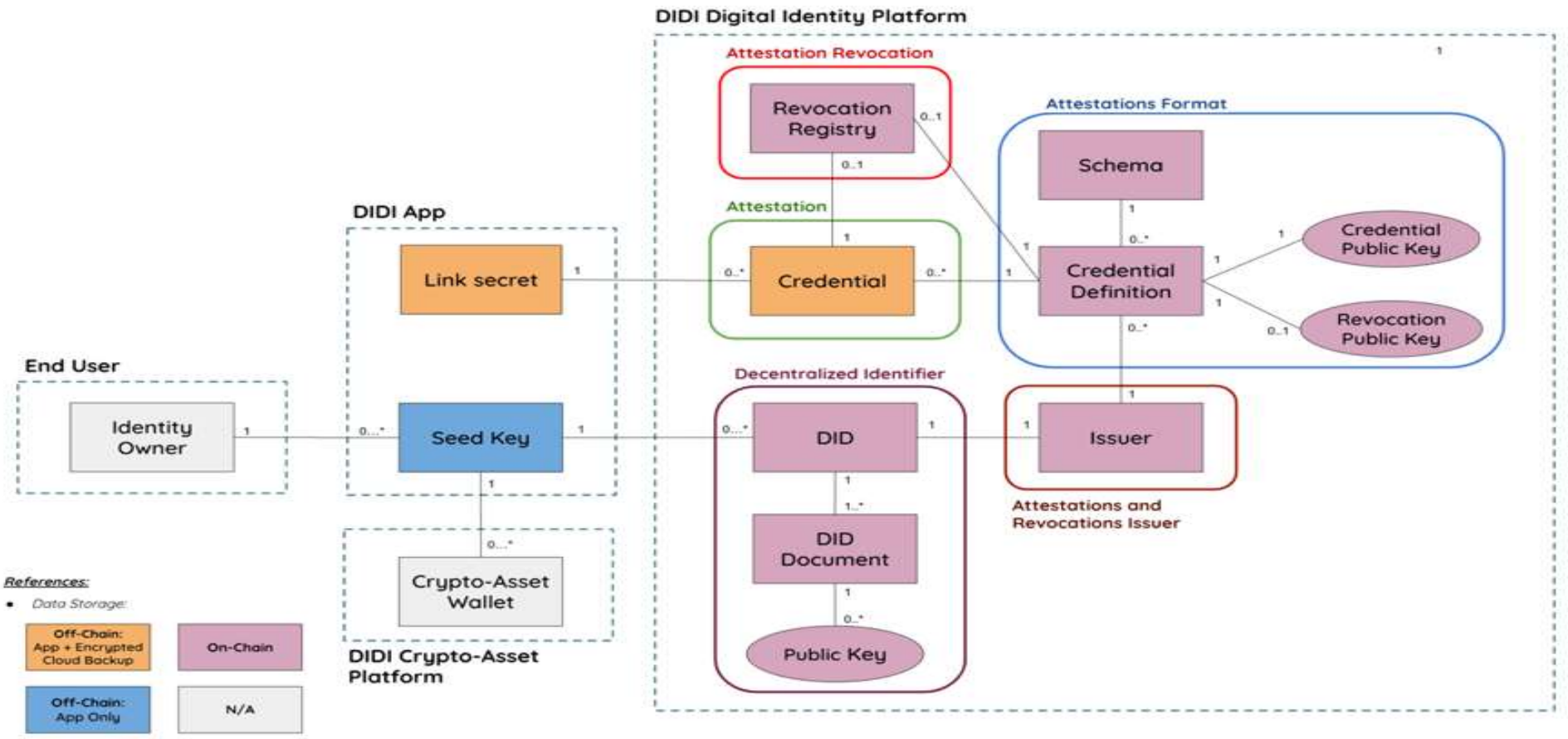
- **Proxy Credentials Issuance Manager**: Este Manager se encargará de gestionar todas las interacciones con los módulos y actores que emitan credenciales. Por ejemplo: Certificaciones financieras generadas por el uso de la Billetera, Certificaciones de validación de información (Número Telefónico, Correo Electrónico), Certificado de DNI (RENAPER), etc.

Flujo Funcional – Proyecto DIDI

ONG BITCOIN ARGENTINA



DER – Proyecto DIDI



ONG BITCOIN ARGENTINA

Orchestrating a brighter world NEC

Alcance Funcional - Etapa 1

Resumen Ejecutivo

Objetivo y Alcances - Etapa 1

El objetivo de esta etapa será realizar una primera implementación de la Plataforma de Identidad Digital Soberana que podrá ser utilizada para tener acceso a servicios por parte, principalmente, de comunidades vulnerables e informales.

Esta plataforma de Identidad Digital Soberana estará integrada a un Módulo de Billetera y un Módulo de Pesos Digitales, no son parte del alcance de este proyecto.

Las funcionalidades y módulos a desarrollar en esta primera etapa son:

- **Módulo Backend Server**
- **Módulo Backup Cloud**
- **Módulo Emisor de Credenciales**
  - Server Genérico
  - Implementación Usuario emisor de Credenciales para GCBA ***(Opcional en esta etapa)***.
  - Implementación DECODES Proxy Issuer ***(Opcional en esta etapa)***.
  - Sistema de Gestión de Credenciales Genérico (Web).
- **Aplicación Móvil**
  - Registración
  - Login
  - Generación y Recuperación de Copia de Seguridad
  - Homepage
  - Perfil del Usuario
    - Compartir información
  - Credenciales y Certificados
    - Compartir Credenciales y Certificados

ONG BITCOIN ARGENTINA

Orchestrating a brighter world NEC

Front-End:
App Android

Etapa 1

Front-End: App Android

# CU	Casos de uso	Descripción	Responsable
1	Registración	La primera vez de cada usuario se generará: - Credenciales de Identidad Digital - Validación de datos biométricos - Validación de Celular - Validación de Email - Generación de Nombre de Usuario - Generación de Contraseña de recuperación de Backup	NEC
2	Validación de Usuario	El usuario ya se encuentra registrado en la App.	NEC
3	Login	Login de usuarios a la App.	NEC
4	Perfil de Usuario (Visualización + ABM)	El usuario realiza modificaciones de su perfil registrado en la APP. - Resumen de la información del usuario. - Compartir Información vía QR, Whatsapp, SMS, Email. - Cambio Email (Revalidación) - Cambio Número de Teléfono (Revalidación) - Cambio de Contraseña (Revalidación)	NEC
5	Generación Backup	Para salvar los contenidos más sensibles y credenciales.	Decodes
6	Recuperación Backup	Para restaurar los contenidos más sensibles y credenciales.	Decodes
7	Homepage	Acciones principales y contenidos.	Decodes
8	Compartir: Credenciales y Certificados	Compartir Credenciales y/o Certificado vía: - QR - Whatsapp - SMS - Email	NEC

App Móvil - Front End

Se debe desarrollar una aplicación móvil para el sistema operativo Android, la cual será el punto de entrada de los usuarios a la plataforma de identidad soberana.

Funcionalidades y Pantallas Requeridas en esta etapa:

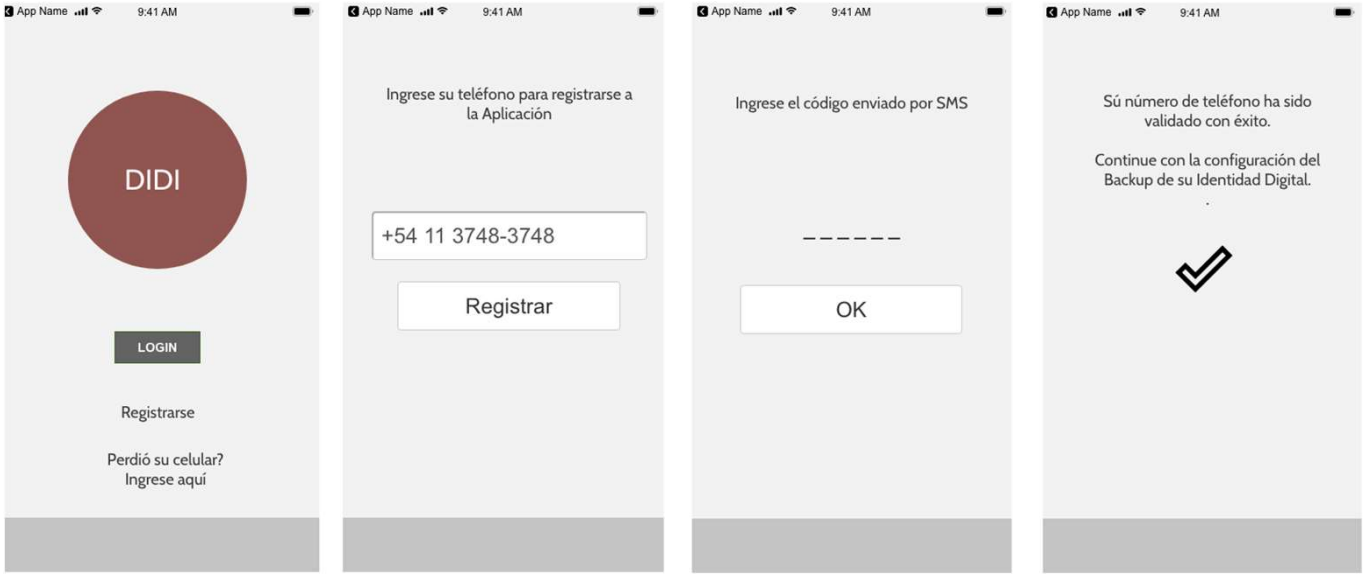
- ➔ Registración
- ➔ Generación y Recuperación de Copia de Seguridad
- ➔ Homepage con acciones principales y contenidos.
- ➔ Mi Perfil: Resumen de la información del usuario.
  - ◆ Compartir Información vía QR, Whatsapp, SMS, Email.
  - ◆ Cambio Email (Revalidación)
  - ◆ Cambio Número de Teléfono (Revalidación)
  - ◆ Cambio de Contraseña (Revalidación)
- ➔ Credenciales & Certificados
  - ◆ Compartir Credenciales o Certificado vía QR, Whatsapp, SMS, Email.

Aplicación Móvil - Wireframes

A continuación se presentan los wireframes iniciales donde se puede observar la orientación del flujo visual de la aplicación. Estos Wireframes luego serán desarrollados por UX/UI para asegurarnos su facilidad de uso y claridad.

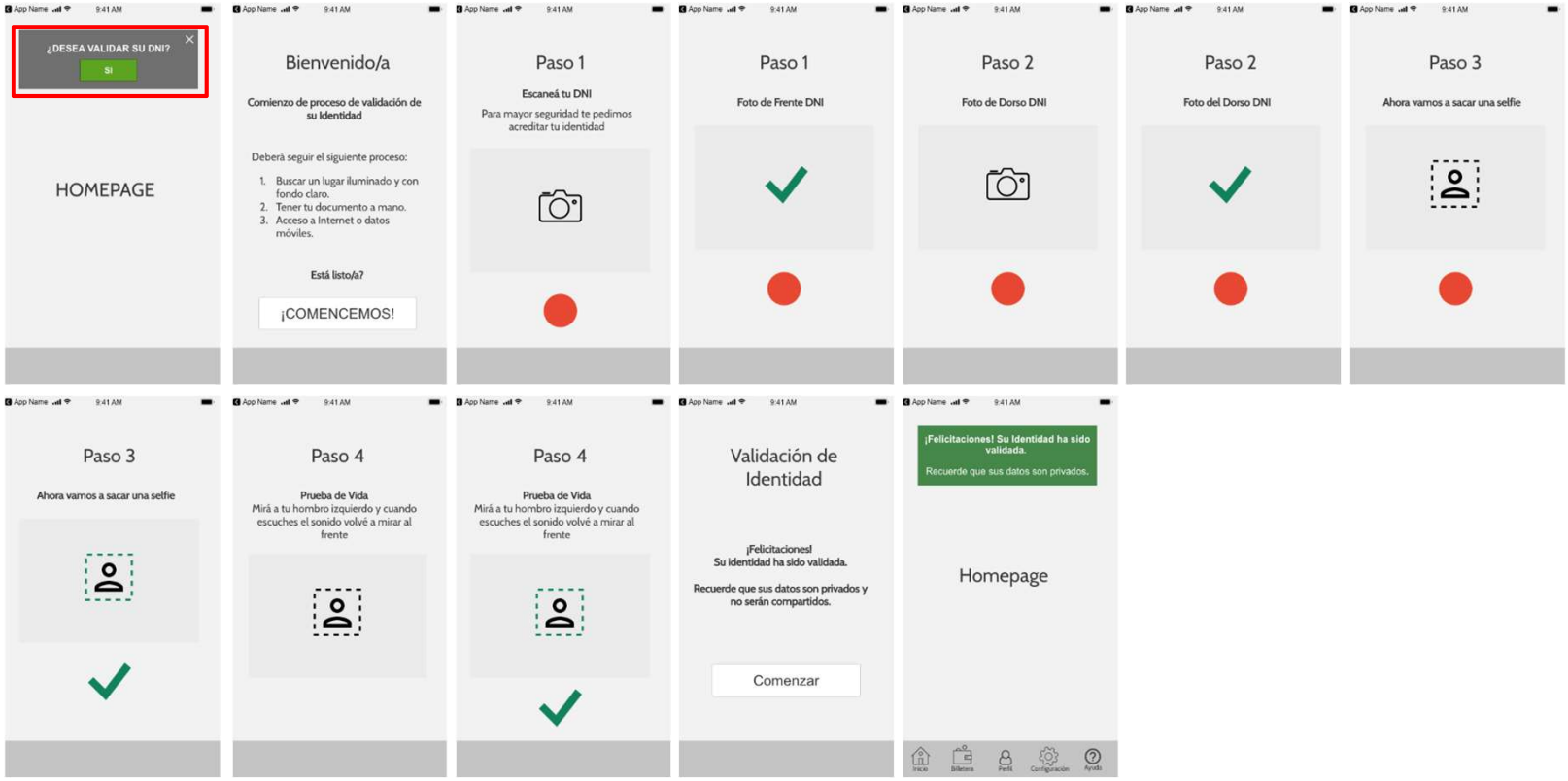
No se incluyen los Wireframes de Certificados y Credenciales ya que están aún en progreso.

Registración



Aplicación Móvil - Wireframes

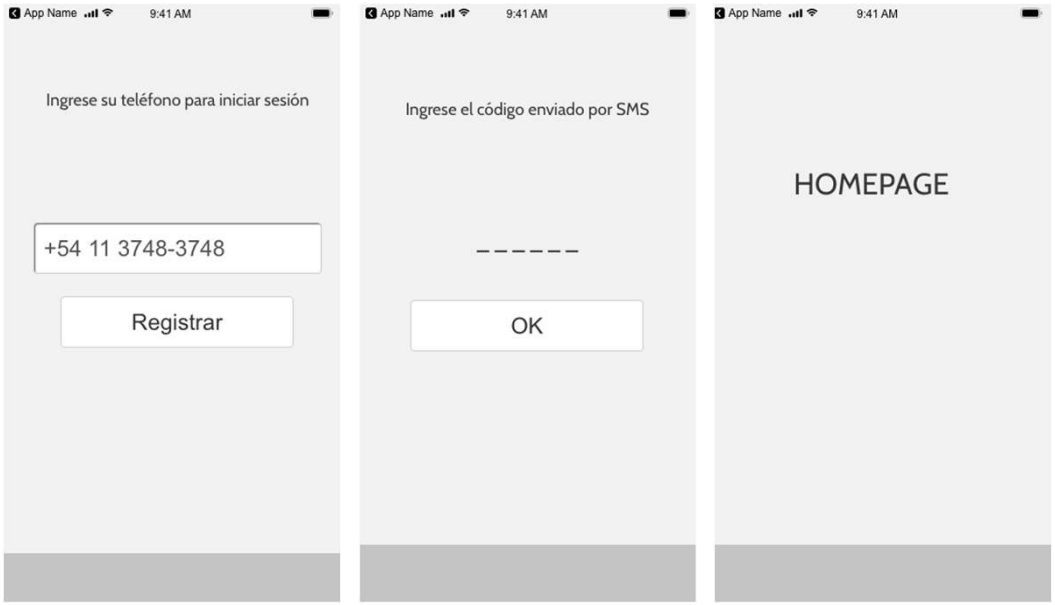
Validación DNI



Aplicación Móvil - Wireframes

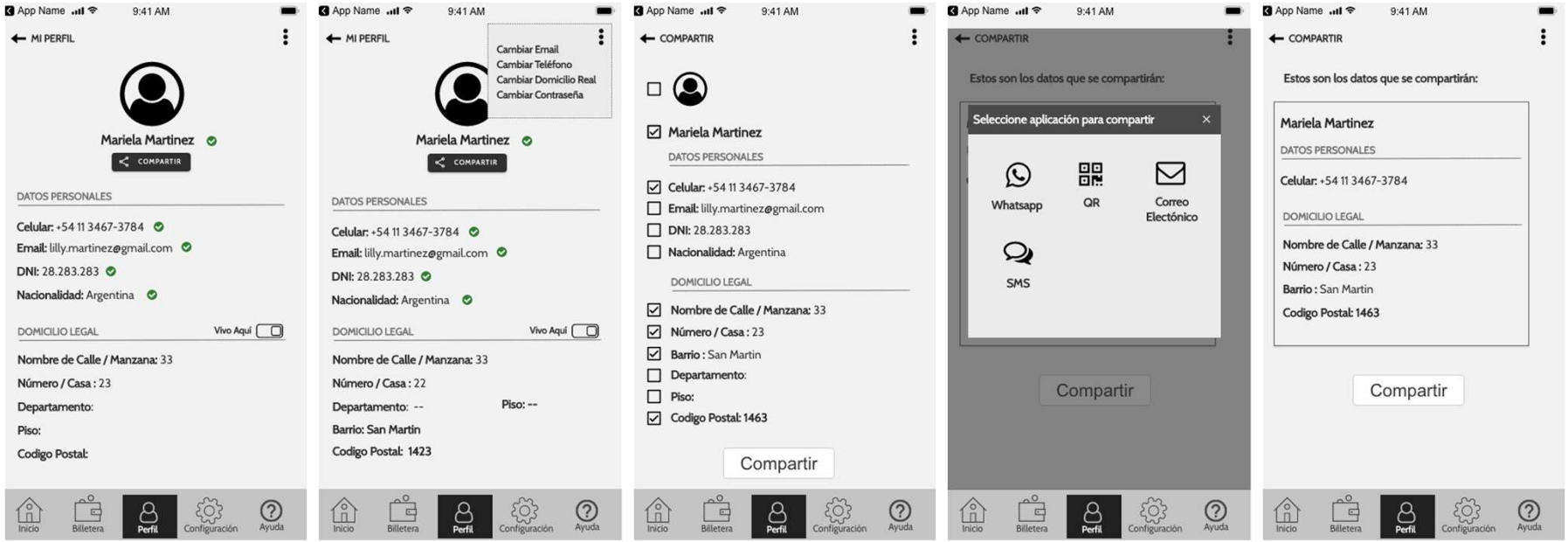
ONG BITCOIN ARGENTINA

Login



Aplicación Móvil - Wireframes

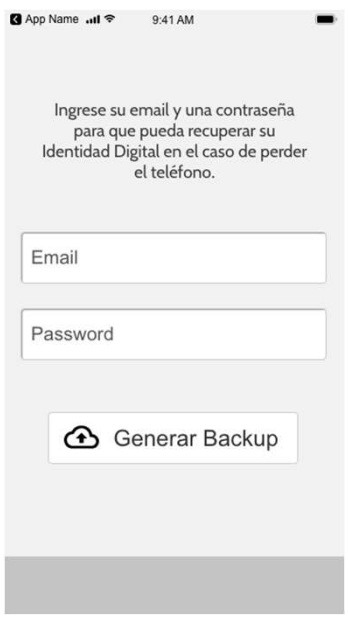
Mi Perfil

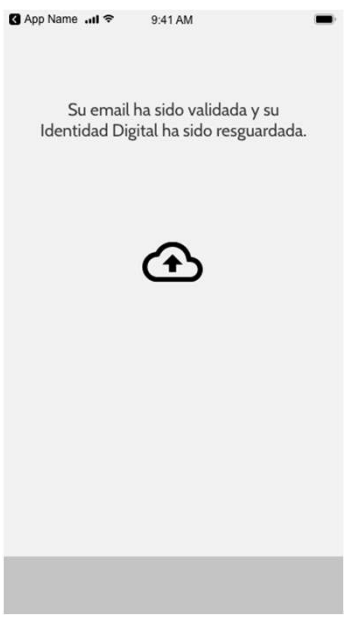


Aplicación Móvil - Wireframes

ONG BITCOIN ARGENTINA

Registración - Generación de Copia de Seguridad

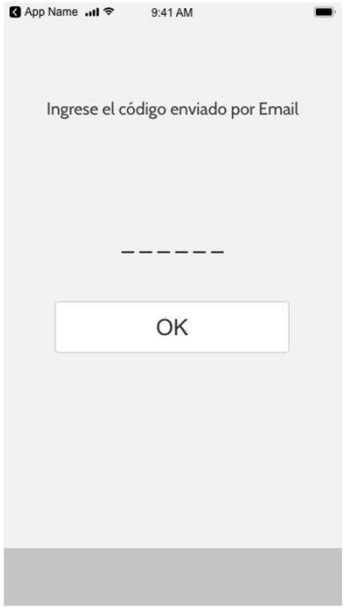




Aplicación Móvil - Wireframes

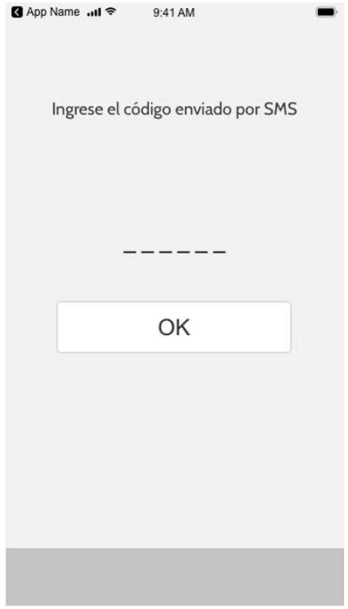
ONG BITCOIN ARGENTINA

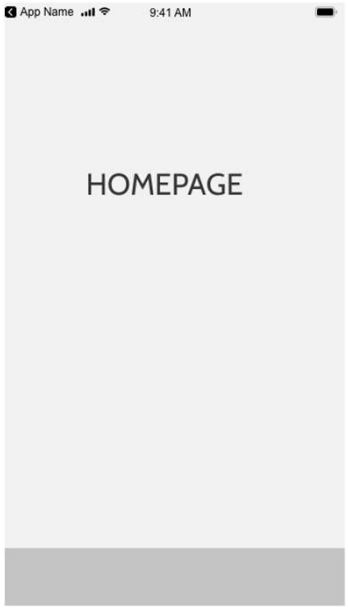
Recuperación de Password



Aplicación Móvil - Wireframes

Recuperación de Copia de Seguridad





ONG BITCOIN ARGENTINA

Orchestrating a brighter world NEC

Back-End:
Server - App Android & Blockchain

Etapa 1

Back-End: Server - App Android & Blockchain

# CU	Casos de uso	Descripción	Responsable
9	Registración (Identidad Digital - BlockChain)	La primera vez de cada usuario se generará: - Credenciales de Identidad Digital (Blockchain)	NEC
10	Registración (Datos Biométricos - Artificial Intelligence)	La primera vez de cada usuario se generará: - Validación de datos biométricos (Servicios de Inteligencia Artificial)	NEC
11	Registración (de Validaciones)	La primera vez de cada usuario se generará: - Validación de Celular - Validación de Email	NEC
12	Registración (de cuenta para Cloud Backup)	La primera vez de cada usuario se generará: - Generación de Nombre de Usuario - Generación de Contraseña de recuperación de Backup - Se dará de alta el registro del Usuario en el Cloud BackUp (Ver CU “Generacion Backup”)	Decodes NEC
13	Validación de Usuario	El usuario ya se encuentra registrado en la App (Blockchain)	NEC
14	Login	Login de usuarios a la App (Blockchain)	NEC
15	Perfil de Usuario (Visualización)	- Resumen de la información del usuario. - Compartir Información vía QR, Whatsapp, SMS, Email. -	NEC
16	Perfil de Usuario (ABM)	El usuario realiza modificaciones de su perfil registrado en la APP (Blockchain) - Cambio Email (Revalidación) - Cambio Número de Teléfono (Revalidación) - Cambio de Contraseña (Revalidación)	NEC
17	Generación Backup	Para salvar los contenidos más sensibles y credenciales (en Cloud Backip)	Decodes NEC
18	Recuperación Backup	Para restaurar los contenidos más sensibles (Blockchain + Cloud Backip)	Decodes NEC
19	Homepage	Acciones principales y contenidos	NEC
20	Compartir: Credenciales y Certificados	Compartir Credenciales y/o Certificado vía: - QR - Whatsapp - SMS - Email	NEC

Módulo Backend Server

- No almacenará ningún tipo de información privada de los usuarios finales. Si el Servidor recibe alguna información, deberá ser encriptada y la enviará a quien corresponda sin conocer el contenido de la misma para evitar ser un punto de falla y vulnerabilidad del sistema.

- Deberá utilizar el protocolo IDS(Intrusion Detection System) propuesto por uPort sobre redes Blockchain EVM-compatible.

- La Arquitectura de la App deberá ser diseñada como multi-blockchain.

- Blockchain no será utilizada para almacenar información privada ni derivados de la misma.

- Este módulo también será encargado de verificar si las apps que quieran interactuar con él, están habilitadas o no a hacerlo para poder comunicarse.

A través de uPort, las apps de los distintos Issuers (por ej. GCBA o Renaper) deberían publicar sus Smart Contracts; si cumplen las condiciones se conectan, sino estan Disabled.

ONG BITCOIN ARGENTINA

Orchestrating a brighter world NEC

Front-End:
Web-Server Emisor de Credenciales

Etapa 1

Front-End: Web-Server Emisor de Credenciales

# CU	Casos de uso	Descripción	Responsable
21	Web – Issuer Credentials Module	Módulo Web Server, para la Generación de Usuarios Admin de Credenciales. Cada Issuer podrá Generar/Emitir Credenciales (ej. certificados/títulos) en forma de plantillas pre-formateadas. Nota: En etapas posteriores el módulo tendrá un ABM de Usuarios y permitirá una mayor customización de roles y permisos, por ejemplo: Sólo Visualización, Emisor de Credenciales, etc.	NEC
22	Web de Usuario Principal de Gestión de Credenciales	Cada Issuer que emita Credenciales, tendrá un Usuario Admin Principal que: - Podrá emitir un Certificado (crear un Template con los ítems del certificado), donde definirá los datos requeridos. - Podrá aprobar credenciales. - Podrá revocar credenciales. - Podrá emitir credenciales a través de su DID público a nombre de personas/entidades representados también por los DIDs públicos de las mismas. - Cumplirá los estándares de “Verifiable Credentials” definido por W3C a través de la implementación de uPort.	NEC

Módulo Emisor de Credenciales - Frontend

El Front End será una página web con acceso permitido para el Administradores (Emisores de Certificados).

Características del módulo:

- ➔ Este módulo deberá ser instalado por cada emisor en su propio servidor.
- ➔ Un usuario principal para esta etapa: Administrador, el cual será autogenerado durante la instalación. En etapas posteriores el módulo tendrá un ABM de Usuarios y permitirá una mayor customización de roles y permisos, por ejemplo: Sólo Visualización, Emisor de Credenciales, etc.
- ➔ El usuario principal podrá crear un Template por certificado donde definirá los datos requeridos.
- ➔ El usuario principal podrá aprobar los certificados.
- ➔ Podrá emitir credenciales a través de su DID público a nombre de personas/entidades representados también por los DIDs públicos de las mismas.
- ➔ Se debe cumplir con los estándares de “Verifiable Credentials” definido por W3C a través del uso de uPort.

ONG BITCOIN ARGENTINA

Orchestrating a brighter world NEC

Back-End:
Web-Server Emisor de Credenciales & Blockchain

Etapa 1

Back-End: Web-Server Emisor de Credenciales & Blockchain

# CU	Casos de uso	Descripción	Responsable
23	Web Server – Issuer Credentials Module (Identidad Digital - BlockChain)	Módulo Web Server, para la Generación de Usuarios Admin de Credenciales. Cada Issuer al crear su usuario, será Administrador por default, para poder Generar/Emitir Credenciales (ej. certificados/títulos) en forma de plantillas pre-formateadas que deberán cumplirse a modo de “Smart-Contract” con Blockchain. Nota: En etapas posteriores el módulo tendrá un ABM de Usuarios y permitirá una mayor customización de roles y permisos, por ejemplo: Sólo Visualización, Emisor de Credenciales, etc.	NEC
24	Web Server de Gestión de Credenciales (Usuario Admin por cada Issuer)	Cada Issuer que emita Credenciales, tendrá un Usuario Admin Principal que: - Podrá emitir un Certificado (crear un Template con los ítems del certificado), donde definirá los datos requeridos. - Podrá aprobar credenciales. - Podrá revocar credenciales. - Podrá emitir credenciales a través de su DID público a nombre de personas/entidades representados también por los DIDs públicos de las mismas. - Cumplirá los estándares de “Verifiable Credentials” definido por W3C a través de la implementación de uPort.	NEC
	Emisor de Credenciales GCBA	Implementación de Usuario Admin, Emisor de Credenciales (con el template especifico) para GCBA. (Opcional en esta etapa)	NEC
25	DECODES Proxy Issuer	Issuer Credential Molule que permitirá la implementación de: - Credentials Manager - Blockchain Manager - Encryption Manager - Data Manager (Opcional en esta etapa)	NEC

Módulo Emisor de Credenciales

Este módulo será necesario para que los Emisores de Credenciales firmadas digitalmente (por ejemplo, GCBA) puedan realizar esa tarea.

Características del módulo:

- ➔ Este módulo deberá ser instalado por cada emisor en su propio servidor, el cual deberá interactuar en un entorno seguro con los sistemas y bases de datos de los mismos.
- ➔ Para ello se debe desarrollar un "Server Genérico" de este módulo que pueda luego se utilizado por los futuros emisores de credenciales (haciendo los ajustes necesarios según las particularidades de cada emisor).

- ➔ Se deberá implementar una versión del "Server Genérico" anteriormente mencionado, factible de poderse instalar por cada Entidad que quisiera emitir un certificado:

  Modulo DECODES/BID (Proxy Issuer): Este módulo servirá para gestionar y validar los certificados emitidos:
  - Certificado de Validación de Email
  - Certificado de Validacion de Telefono
  - Certificado de DNI (integrado a RENAPER)
  - Certificado Financiero a partir de uso de la APP (Ronda)
  - Cetificado emitido por Emisor de Credenciales web (ver Proxima diapo).

ONG BITCOIN ARGENTINA

Orchestrating a brighter world NEC

Back-End:
Módulo Backup Cloud Server

Etapa 1

Back-End: Módulo Backup Cloud Server

# CU	Casos de uso	Descripción	Responsable
26	Sistema Cloud de Backup	Los Servers podrían ser: - Azure - Amazon - IPFS (Inter Planetary File System) - Otros…	Decodes
27	Registración (de cuenta para Cloud Backup)	La primera vez de cada usuario se generará: - Generación de Nombre de Usuario - Generación de Contraseña de recuperación de Backup - Se dará de alta el registro del Usuario en el Cloud BackUp (Ver CU “Generacion Backup”)	Decodes NEC
28	Generación Backup	Para salvar los contenidos más sensibles y credenciales (en Cloud Backip)	Decodes NEC
29	Recuperación Backup	Para restaurar los contenidos más sensibles (Blockchain + Cloud Backip)	Decodes NEC

Módulo Backup Cloud

Este módulo se encargará de realizar la gestión de las copias de seguridad de los usuarios de la app. Por ejemplo, si un usuario perdiera acceso a su celular, podrá recuperar su información accediendo a este Módulo mediante un proceso de verificación vía SMS o Email.

Características del módulo:

- ➔ La copias de seguridad contendrán toda la información privada de los usuarios de la app. Esta información debe estar ser guardada encriptada con la clave pública de los usuarios finales. Y sólo podrán ser desencriptados con la clave privada de los mismos.

(ver diapositiva 13, "Recuperación de Copia de Seguridad")

- ➔ NEC y Consensys, definiran en conjunto el estándar de seguridad necesarios para el almacenamiento de esta información en la nube, como por ejemplo en las tecnologias Cloud de Azure/AWS, etc.

ONG BITCOIN ARGENTINA

Orchestrating a brighter world

NEC