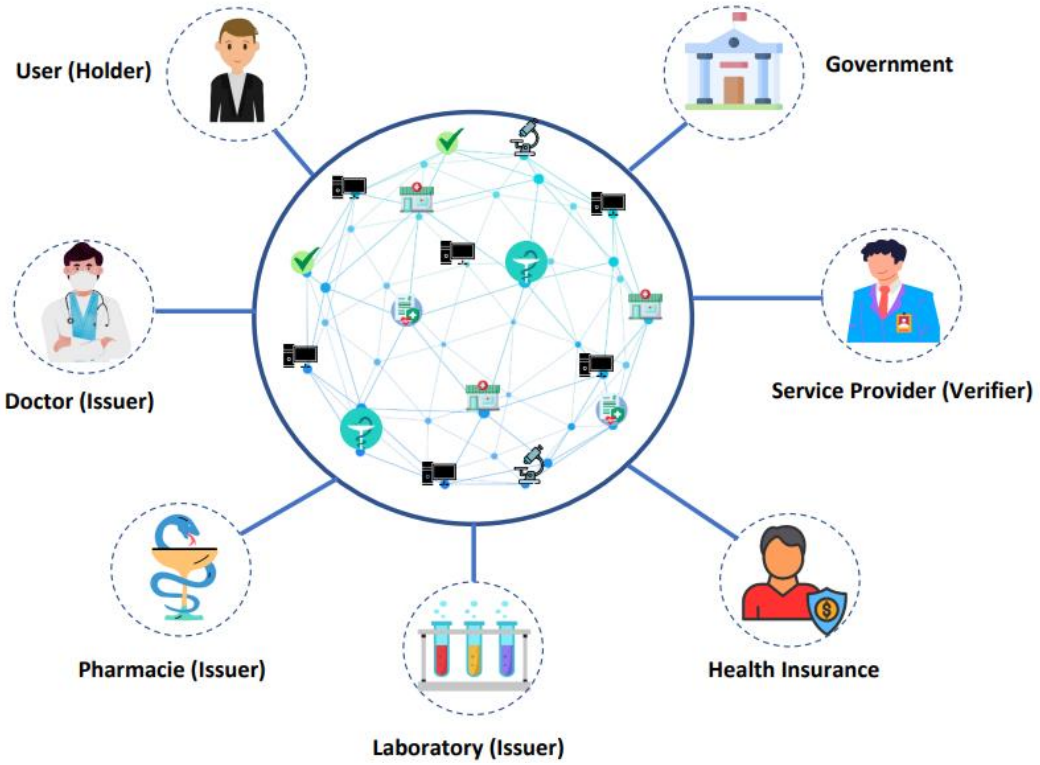
Passeport Médical

Acteurs :



1- **Utilisateur (Holder) : un individu qui possède un passeport médical contenant des informations importantes sur sa santé.**
2- **Émetteur (Issuer) : un professionnel de la santé qui fournit les informations médicales de l'utilisateur pour la création du passeport médical, signe le passeport et le transmet à l'utilisateur.**
3- **Vérificateur (Verifier) : une autorité ou une organisation qui vérifie la validité d'un passeport médical lorsqu'il est présenté par l'utilisateur.**
4- **Assureur : une entreprise qui fournit une assurance santé à l'utilisateur.**
5- **Gouvernement : l'entité responsable de la réglementation et de la supervision du système de santé.**

Interfaces :

1- **Page d'accueil : interface pour accéder aux différentes fonctionnalités de l'application. Les utilisateurs peuvent se connecter à leur compte, s'inscrire pour un nouveau compte ou récupérer leur mot de passe.**
2- **Interface d'enregistrement : interface permettant aux utilisateurs de saisir et de stocker leurs informations, qui sont stockées sur IPFS sous forme encryptée.**
3- **Interface d'émission : interface qui permet aux émetteurs d'ajouter des données médicales sur les patients et de générer leurs passeports médicaux.**
4- **Interface de vérification : interface permettant aux vérificateurs de vérifier la validité d'un passeport médical présenté par l'utilisateur.**
5- **Interface d'assurance : interface permettant aux utilisateurs de gérer leur assurance santé, notamment de demander un remboursement pour des dépenses médicales.**
6- **Interface de gouvernement : interface permettant au gouvernement de superviser le système de santé, notamment de collecter des données statistiques sur les utilisateurs et les émetteurs.**

Rôles :

1- **L'utilisateur utilise l'interface d'enregistrement pour stocker ses informations personnelles et l'interface d'assurance pour gérer son assurance santé.**
2- **L'émetteur utilise l'interface d'émission pour ajouter les informations médicales de l'utilisateur et émettre un passeport médical pour l'utilisateur.**
3- **Le vérificateur utilise l'interface de vérification pour vérifier la validité d'un passeport médical présenté par l'utilisateur.**
4- **L'assureur utilise l'interface d'assurance pour gérer les remboursements pour les dépenses médicales des utilisateurs. L'assureur peut accéder aux données médicales de l'utilisateur pour vérifier les informations médicales nécessaires pour le remboursement.**
5- **Le gouvernement utilise l'interface de gouvernement pour superviser le système de santé et collecter des données statistiques sur les utilisateurs et les émetteurs.**

Nous aurons besoins de deux applications différentes :

1- **L'application principale de passeport médical qui sera développée pour stocker et gérer les données médicales des utilisateurs, permettre la gestion des autorisations d'accès et faciliter les interactions entre les différents acteurs du système.**
2- **Une application de gestion d'identité décentralisée (DID) pour permettre aux utilisateurs de créer et de contrôler leur identité numérique, ainsi que de gérer leurs clés de chiffrement. Exemple : « uPort, ,Veramo, Serto, BrightID »**

➔ **La liaison entre l'application à développer et l'application DID se fait généralement par l'intermédiaire d'un protocole standardisé pour la gestion des identités décentralisées tel que le protocole DID.**

Le protocole DID permet de créer, résoudre, mettre à jour et supprimer des identités décentralisées sur la blockchain Ethereum. L'application DID est utilisée pour la création et la gestion des identités décentralisées (DID) des utilisateurs, tandis que l'application à développer est utilisée pour stocker les données médicales et gérer les autorisations d'accès aux données.

Lorsqu'un utilisateur crée son DID, il peut utiliser son DID pour s'authentifier auprès de l'application à développer et accéder à ses données médicales. L'application à développer vérifie l'identité du DID à l'aide de la méthode de résolution DID. Lorsqu'un tiers (comme un émetteur ou un vérificateur) souhaite accéder aux données médicales d'un utilisateur, l'utilisateur peut donner l'autorisation en partageant son DID avec le tiers. Le tiers peut alors vérifier l'identité de l'utilisateur en utilisant la méthode de résolution DID et accéder aux données médicales si l'utilisateur a donné l'autorisation.

La liaison entre les deux applications se fait généralement par l'utilisation de bibliothèques ou de protocoles standardisés. Par exemple, pour lier une application à développer à une solution DID comme uPort ou Veramo, vous pouvez utiliser une bibliothèque comme Ethr-DID, qui fournit une interface pour créer et gérer des identités décentralisées basées sur Ethereum.

L'application à développer peut ensuite utiliser les identités décentralisées créées pour interagir avec des contrats intelligents sur la blockchain Ethereum, tels que le contrat intelligent pour le passeport médical. De cette manière, l'application à développer peut tirer parti des avantages de la technologie de la blockchain et des identités décentralisées pour offrir des fonctionnalités de sécurité et de confidentialité à ses utilisateurs.

⇨ **Le système de passeport médical utilise la blockchain Ethereum, le protocole DID et le contrôle d'accès SSI pour créer un système décentralisé de gestion des données médicales. Les utilisateurs ont le contrôle total sur l'accès à leurs données médicales, tandis que les émetteurs, les vérificateurs et les assureurs peuvent accéder aux données médicales en fonction de leur rôle et des autorisations accordées par l'utilisateur.**

Notions :

Les DID (Identifiants décentralisés) sont utilisés pour identifier les utilisateurs et les émetteurs sur la blockchain Ethereum. Lorsqu'un utilisateur crée un compte, il génère une paire de clés publique-privée qui est utilisée pour créer son DID. Les émetteurs utilisent également leur DID pour émettre des passeports médicaux pour les utilisateurs.

Le système de contrôle d'accès SSI (Self-Sovereign Identity) est utilisé pour contrôler l'accès aux données médicales des utilisateurs. Les utilisateurs peuvent accorder ou révoquer l'accès à leurs données médicales à des tiers, tels que des émetteurs, des vérificateurs ou des assureurs, en utilisant leur identité auto-souveraine.

Le processus d'authentification SSI est réalisé à travers le protocole DID (Decentralized Identifier), qui permet à chaque utilisateur de créer et de contrôler son propre identifiant décentralisé. Les identifiants DID sont stockés sur la blockchain Ethereum et sont vérifiés par les validateurs de réseau pour garantir leur validité.