# Studio tecnologico Identity Trust Fabric

## Diario delle modifiche

|  |  |  |
| --- | --- | --- |
| Data | Descrizione | Autore |
| 12/06/18 | Creazione documento | Simone Ballarin |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Scopo del documento

Nell’ottica di un prossimo sviluppo di un’estensione basata su blockchain dell’attuale servizio ora in produzione MonoKee, questo documento intende valutare in termini di benefici tecnici e tecnologici l’uso della tecnologia Ethereum quale base dell’Identity Trust Fabric (ITF).

## Descrizione prodotto

Il progetto ha come scopo la creazione di un’estensione del servizio MonoKee basato su blockchain. L’estensione offre un sistema di Identity Access Management (IAM) composto da quattro principali fattori:

1. Identity Wallet (IW)
2. Service Provider (SP)
3. Identity Trust Fabric (ITF)
4. Trusted Third Party (TTP)

In sintesi l’estensione dovrà operare al fine di fornire la possibilità ad un utente di registrare e gestire la propria identità tramite l’IW autonomamente, mandare i propri dati (IPP) all’ITF la quale custodirà la sua identità e farà da garante per le asserzioni proveniente dai TTP. Inoltre il SP dovrà essere in grado con le informazioni provenienti da IW e ITF di verificare o meno l’accesso ai propri servizi.

## ITF – Identity Trust Fabric

Sulla base di un primo studio di fattibilità l’unico componente coinvolto nell’uso blockchain è l’Identity Trust Fabric. La sua principale funzione è quella di poter permettere ai vari Service Provider aderenti al servizio di poter verificare le informazioni rilasciate dai vari utenti tramite l’utilizzo del loro personale Identity Wallet (IW). Il componente mantiene al suo interno l’hash della chiave pubblica degli utenti (che rappresenta la loro identità) e le asserzioni fornite dai vari IW che possono essere potenzialmente certificate da una TTP (tramite una firma con la loro chiave privata). Le asserzioni devono poter essere modificate o eliminate in ogni momento, ovviamente ogni alterazione deve essere ogni volta certificata nuovamente. Anche da parte del TTP ci dev’essere la possibilità di revocare la certificazione di un’asserzione.

Una buona implementazione di una ITF deve possedere le seguenti caratteristiche

## Utilizzo di Blockchain per implementare ITF

E’

## 