Un sistema di logging basato su blockchain: l'esperienza del progetto Konfido (e la GDPR)

11 Aprile 2018

IOThings 2018

Blockchain Now

Paolo Campegiani
Innovation Strategist
pca@bit4id.com

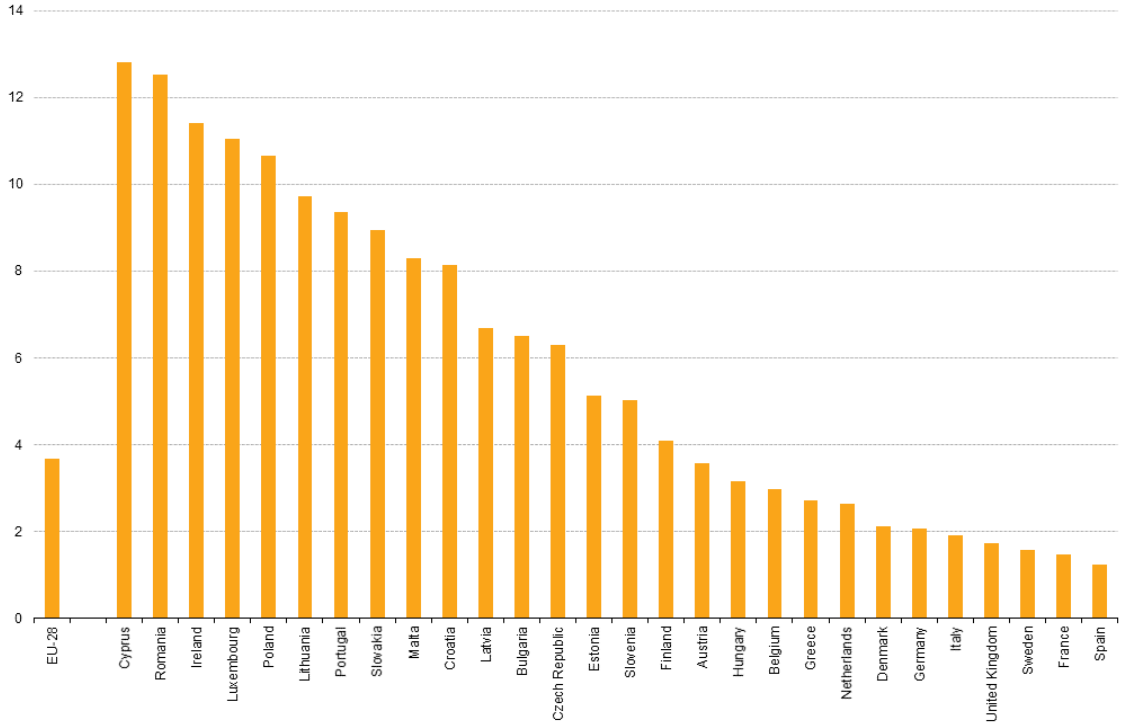
Il progetto Konfido

Visione: sviluppare una soluzione complessiva per servizi di eHealth europei che siano interoperabili e sicuri.

Cofinanziato dal programma Horizon 2020 dell'Unione Europea (grant 727528).

www.konfido-project.eu

Mobilità dei cittadini europei e cure sanitarie



Source: Eurostat (Census hub HC28)

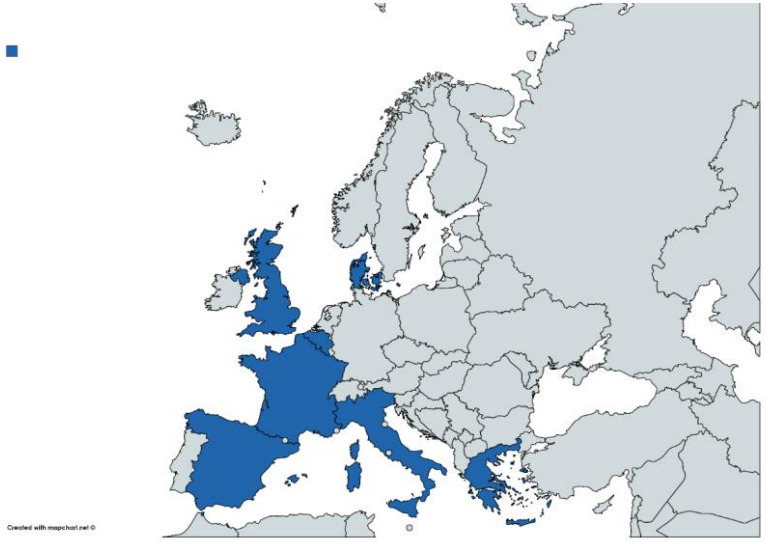
Europei che vivono in una nazione diversa da quella di nascita

In totale si tratta di circa 15 milioni di Europei stabilmente all'estero, a cui si aggiungono i temporanei (turismo, lavoro).

Come possono accedere ai dati sanitari del paese di origine?

Garantire l'accesso a questi dati consente di migliorare la mobilità tra paesi europei.

Partner di progetto



15 partner

7 nazioni

2 piloti

Obiettivi e sfide di progetto

Migliorare la sicurezza del sistema di interscambio di dati sanitari *già esistente*

Gestire gli aspetti legali ed etici

Garantire l'interoperabilità e la scalabilità

Sperimentare tecnologie di sicurezza:

- **eIDAS authentication**
- **SGX Secure computation**
- **Photonic Physical Unclonable Function Authentication**
- **Homomorphic Encryption**
- **Real time System Information and Event Monitoring**
- **Disruptive logging system based on blockchain**

Contesto operativo

Lo scambio di dati sanitari tra paesi UE avviene tra nodi di interfacciamento nazionali.

Ogni nodo certifica la validità delle richieste provenienti dal Paese e si interfaccia con il sistema nazionale per soddisfare le richieste provenienti dall'estero. Le richieste provenienti dall'estero sono considerate affidabili quando provenienti da un nodo certificato.

Ogni nodo è sotto la responsabilità di un Paese membro.

Rischi

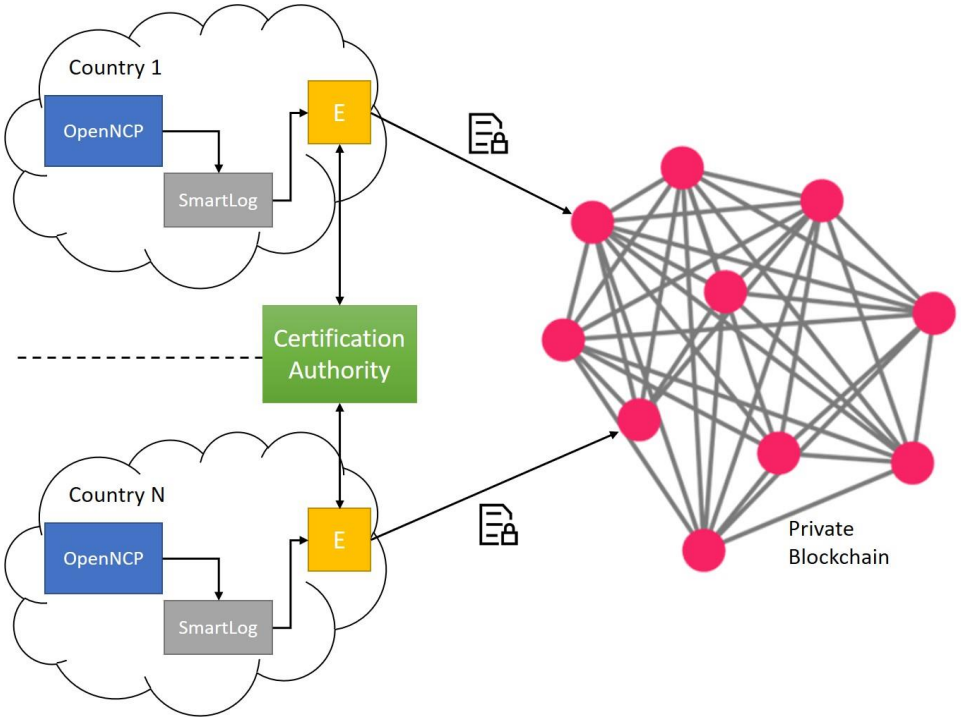
I nodi sono cooperanti ma non è detto che lo siano per sempre.

I nodi possono essere compromessi.

I nodi si interfacciano con una infrastruttura nazionale complessa che può non funzionare correttamente.

<u>Ogni nodo deve poter dimostrare la correttezza del proprio operato in modo autonomo ed indipendente dagli altri.</u>

Blockchain logging



Ogni nodo gestisce un proprio log.

I log che sono rilevanti vengono salvati su una blockchain.

In che formato vengono archiviati i log?

Requisiti e soluzione

I dati di log non possono essere salvati in chiaro (lo scambio di dati tra due Paesi riguarda solo loro).

Ogni Paese deve essere in grado di accedere ai propri dati in modo autonomo (non possiamo assumere la cooperazione tra Paesi).

I dati vengono cifrati in modo tale che:

1) Siano accessibili solo ai due Paesi coinvolti nello scambio di dati
2) Siano accessibili da ciascuno di questi in modo autonomo

Risultati ottenuti

1) La crittografia abbinata all'identità digitale consente di estendere l'utilizzo dei blockchain in ambiti altrimenti non percorribili.

2) E' possibile creare un sistema di logging che conservi traccia delle attività tra soggetti non necessariamente cooperanti.

3) Questo approccio si può adottare anche su sistemi già esistenti richiedendo solo minime estensioni.

Questioni aperte

Come si bilancia l'immutabilità del blockchain con i diritti dell'individuo riconosciuti nella GDPR? (tema aperto anche nel comitato di standardizzazione ISO TC/307 su blockchain e distributed ledger)

Data una possibile soluzione tecnica, come si può garantire che continui ad essere valida negli anni a venire?

E' forse il caso di pensare ad una interpretazione specifica della GDPR per blockchain e DLT?

www.bit4id.com

Paolo Campegiani
Innovation Strategist
pca@bit4id.com