

EUDI – Cattiva Politica, Cattiva Tecnologia

Daniele Palombi¹ Valerio Prosseda²

¹20squares, Institute for Categorical Cybernetics

²CyberEthics Lab.

EUDI, cos'è e perché?

- Un insieme di specifiche per l'implementazione di un sistema di identità digitale e un portafoglio digitale personale per i cittadini, i residenti e le imprese dell'UE

EUDI, cos'è e perché?

- Un insieme di specifiche per l'implementazione di un sistema di identità digitale e un portafoglio digitale personale per i cittadini, i residenti e le imprese dell'UE

EUDI, cos'è e perché?

- Un insieme di specifiche per l'implementazione di un sistema di identità digitale e un portafoglio digitale personale per i cittadini, i residenti e le imprese dell'UE
- Archiviare e condividere in modo "sicuro" l'identità digitale personale:
 - Documenti d'identità (CdI, patente, etc..)
 - Contratti (e.g. assicurazione di un veicolo)
 - Altri titoli personali (tessera della palestra, biglietti del treno, etc..)

**Chi sono gli
Stakeholders?**

Gli Stati Membri

- Legalmente obbligati a fornire almeno una applicazione per il portafoglio digitale agli utenti finali.

Gli Stati Membri

- Legalmente obbligati a fornire almeno una applicazione per il portafoglio digitale agli utenti finali.
- Incaricano i Wallet Provider per lo sviluppo delle applicazioni per il portafoglio digitale

Gli Stati Membri

- Legalmente obbligati a fornire almeno una applicazione per il portafoglio digitale agli utenti finali.
- Incaricano i Wallet Provider per lo sviluppo delle applicazioni per il portafoglio digitale
- Incaricano le Autorità Certificatrici locali per l'emissione e certificazione di documenti digitali

Chi sono gli Stakeholders?

I Wallet Providers (WP)

- Entità di terze parti incaricate da uno Stato Membro

Chi sono gli Stakeholders?

I Wallet Providers (WP)

- Entità di terze parti incaricate da uno Stato Membro
- Sviluppano e mantengono le applicazioni per il portafoglio digitale

I Wallet Providers (WP)

- Entità di terze parti incaricate da uno Stato Membro
- Sviluppano e mantengono le applicazioni per il portafoglio digitale
- Forniscono assistenza tecnica agli utenti finali e agli altri stakeholders

Chi sono gli Stakeholders?

Le Autorità di Certificazione (CA)

- Incaricate da uno Stato Membro

Chi sono gli Stakeholders?

Le Autorità di Certificazione (CA)

- Incaricate da uno Stato Membro
- Emettono documenti digitali per gli utenti finali

Chi sono gli Stakeholders?

Excursus: Tipi di Documenti Digitali

- **Credenziali Digitali:** Documenti digitali che identificano l'utente (e.g. CdI)

Excursus: Tipi di Documenti Digitali

- **Credenziali Digitali:** Documenti digitali che identificano l'utente (e.g. CdI)
- **Electronic Attestations of Attributes (EAAs):** Documenti digitali non identificativi di importanza minore (e.g. biglietti del treno, abbonamento alla palestra)

Excursus: Tipi di Documenti Digitali

- **Credenziali Digitali:** Documenti digitali che identificano l'utente (e.g. CdI)
- **Electronic Attestations of Attributes (EAAs):** Documenti digitali non identificativi di importanza minore (e.g. biglietti del treno, abbonamento alla palestra)
- **Qualified Electronic Attestations of Attributes (QEAs):** Documenti digitali non identificativi *ufficiali*, distribuiti da CA ritenute affidabili e soggette a maggiori controlli (e.g. documenti fiscali)

I Service Providers (SP)

- Entità di terze parti, private o pubbliche, che utilizzano informazioni dal portafoglio
- Richiedono all'utente finale di autenticarsi tramite il portafoglio digitale per accedere ai loro servizi

Chi sono gli Stakeholders?

~~Le Vittime~~ Gli Utenti Finali

- Cittadini europei, residenti, business

Chi sono gli Stakeholders?

~~Le Vittime~~ Gli Utenti Finali

- Cittadini europei, residenti, business
- Obbligati a usare una delle applicazioni fornite dal loro stato di residenza

Chi sono gli Stakeholders?

~~Le Vittime~~ Gli Utenti Finali

- Cittadini europei, residenti, business
- Obbligati a usare una delle applicazioni fornite dal loro stato di residenza
- Utilizzano un'app per il portafoglio digitale per autenticarsi presso i SP

**Quali sono i
problemi?**

Quali sono i problemi?

Le App “Sovrane”

- Dove sono e chi gestisce i data centers?
 - e.g. la proposta originale per il [PSN](#)

Quali sono i problemi?

Le App “Sovrane”

- Dove sono e chi gestisce i data centers?
 - e.g. la proposta originale per il [PSN](#)
- Quali sono le garanzie di privacy delle applicazioni?
 - Open Source
 - Traccianti Google/Apple

Quali sono i problemi?

Le App “Sovrane”

- Dove sono e chi gestisce i data centers?
 - e.g. la proposta originale per il [PSN](#)
- Quali sono le garanzie di privacy delle applicazioni?
 - Open Source
 - Traccianti Google/Apple
- Frammentazione delle implementazioni e specifiche lasche
 - e.g. Zero-Knowledge Proofs

Quali sono i problemi?

Excursus: DC4EU & EBSI

- **EBSI**: Infrastruttura europea *permissioned* per servizi blockchain. Ogni Stato Membro gestirà almeno un nodo.

Quali sono i problemi?

Excursus: DC4EU & EBSI

- **EBSI**: Infrastruttura europea permissioned per servizi blockchain. Ogni Stato Membro gestirà almeno un nodo.
- **DC4EU**: Progetto pilota per l'uso del portafoglio EUDI nel settore dell'istruzione e della sicurezza sociale. Utilizzerà EBSI nel contesto del portafoglio EUDI.

Quali sono i problemi?

Serviva proprio una Blockchain?

- In breve: No

Quali sono i problemi?

Serviva proprio una Blockchain?

- In breve: No
- EBSI propone un database distribuito + un modello di esecuzione di smart contracts senza nessun tipo di finalità economica (i.e. la principale caratteristica delle Blockchain)

Serviva proprio una Blockchain?

- In breve: No
- EBSI propone un database distribuito + un modello di esecuzione di smart contracts senza nessun tipo di finalità economica (i.e. la principale caratteristica delle Blockchain)
- Al giorno d'oggi, la tecnologia Blockchain non può supportare il volume di transazioni che deriverebbe da una tale piattaforma

Serviva proprio una Blockchain?

- In breve: No
- EBSI propone un database distribuito + un modello di esecuzione di smart contracts senza nessun tipo di finalità economica (i.e. la principale caratteristica delle Blockchain)
- Al giorno d'oggi, la tecnologia Blockchain non può supportare il volume di transazioni che deriverebbe da una tale piattaforma
- Sistema decentralizzato \neq Un numero ristretto di nodi controllati da un consorzio

Quali sono i problemi?

Le CA nel Browser

- I browser saranno obbligati a includere le CA come entità "trusted"

Quali sono i problemi?

Le CA nel Browser

- I browser saranno **obbligati** a includere le CA come entità "trusted"
- L'ETSI proibirà ai browser di richiedere alle CA misure di sicurezza aggiuntive oltre a quelle specificate dall'ETSI stesso

Le CA nel Browser

- I browser saranno **obbligati** a includere le CA come entità "trusted"
- L'ETSI proibirà ai browser di richiedere alle CA misure di sicurezza aggiuntive oltre a quelle specificate dall'ETSI stesso
- Un ulteriore possibile punto di fallimento nella sicurezza sul web

Quali sono i problemi?

Self Sovereign Identity: una soluzione filosofica?

Gli utenti sono sovrani della propria identità:

- l'utente deve essere centrale nell'amministrazione della propria identità

Quali sono i problemi?

Self Sovereign Identity: una soluzione filosofica?

Gli utenti sono sovrani della propria identità:

- l'utente deve essere centrale nell'amministrazione della propria identità
- prevenire le violazioni dei diritti umani da parte dei potenti e sostenere i diritti dell'individuo a essere se stesso e ad associarsi liberamente

Quali sono i problemi?

Self Sovereign Identity: una soluzione filosofica?

Gli utenti sono sovrani della propria identità:

- l'utente deve essere centrale nell'amministrazione della propria identità
- prevenire le violazioni dei diritti umani da parte dei potenti e sostenere i diritti dell'individuo a essere se stesso e ad associarsi liberamente
- deve essere trasportabile ed interoperabile; non può essere vincolata a un solo sito o locale

Quali sono i problemi?

Self Sovereign Identity: una soluzione filosofica?

eIDAS2 propone un *hit or miss*:

- i principi della SSI (e.g. Christopher Allen) sono distorti e adattati a uno schema più centralizzato

Quali sono i problemi?

Self Sovereign Identity: una soluzione filosofica?

eIDAS2 propone un *hit or miss*:

- i principi della SSI (e.g. Christopher Allen) sono distorti e adattati a uno schema più centralizzato
- in particolare sono ri-toccati concetti e principi come *controllo, accesso, trasparenza, interoperabilità e consenso*

GRAZIE !

Quali sono i problemi?

Referenze & Link Utili

- **What is EBSI:** <https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/What+is+ebsi>
- **eIDAS 2.0 Provisional Agreement – Implications for Web Browsers and Digital Certificate Trust:** <https://docs.google.com/document/d/1sGzaE9QTs-qorr4BTqKAe0AaGKjt5GagyEevDoavWU0/edit#heading=h.dydk4j82t0ww>
- **The Path to Self-Sovereign Identity:** <https://www.lifewithalacrity.com/article/the-path-to-self-sovereign-identity/>
- **Article 45 Will Roll Back Web Security by 12 Years:** <https://www.eff.org/deeplinks/2023/11/article-45-will-roll-back-web-security-12-years>
- **Last Chance to fix eIDAS: Secret EU law threatens Internet security:** <https://last-chance-for-eidas.org/>
- **EU Digital identity: 4 projects launched to test EUDI Wallet:** <https://digital-strategy.ec.europa.eu/en/news/eu-digital-identity-4-projects-launched-test-eudi-wallet>
- **What is the EU Digital Identity Wallet:** <https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/What+is+the+wallet>
- **Cloud PA, ecco i paletti del Parlamento a Google, Microsoft e AWS:** <https://www.startmag.it/innovazione/cloud-pa-ecco-i-paletti-del-parlamento-a-google-microsoft-e-aws/>