WORKSHOP GARR 2024

NET MAKERS

Introduzione ai Sistemi di Identità Digitale Basati su Soluzioni Wallet

Giuseppe De Marco
Dipartimento per la trasformazione digitale

Hi, I AM GIUSEPPE DE MARCO

WORK SHOP GARR 2024

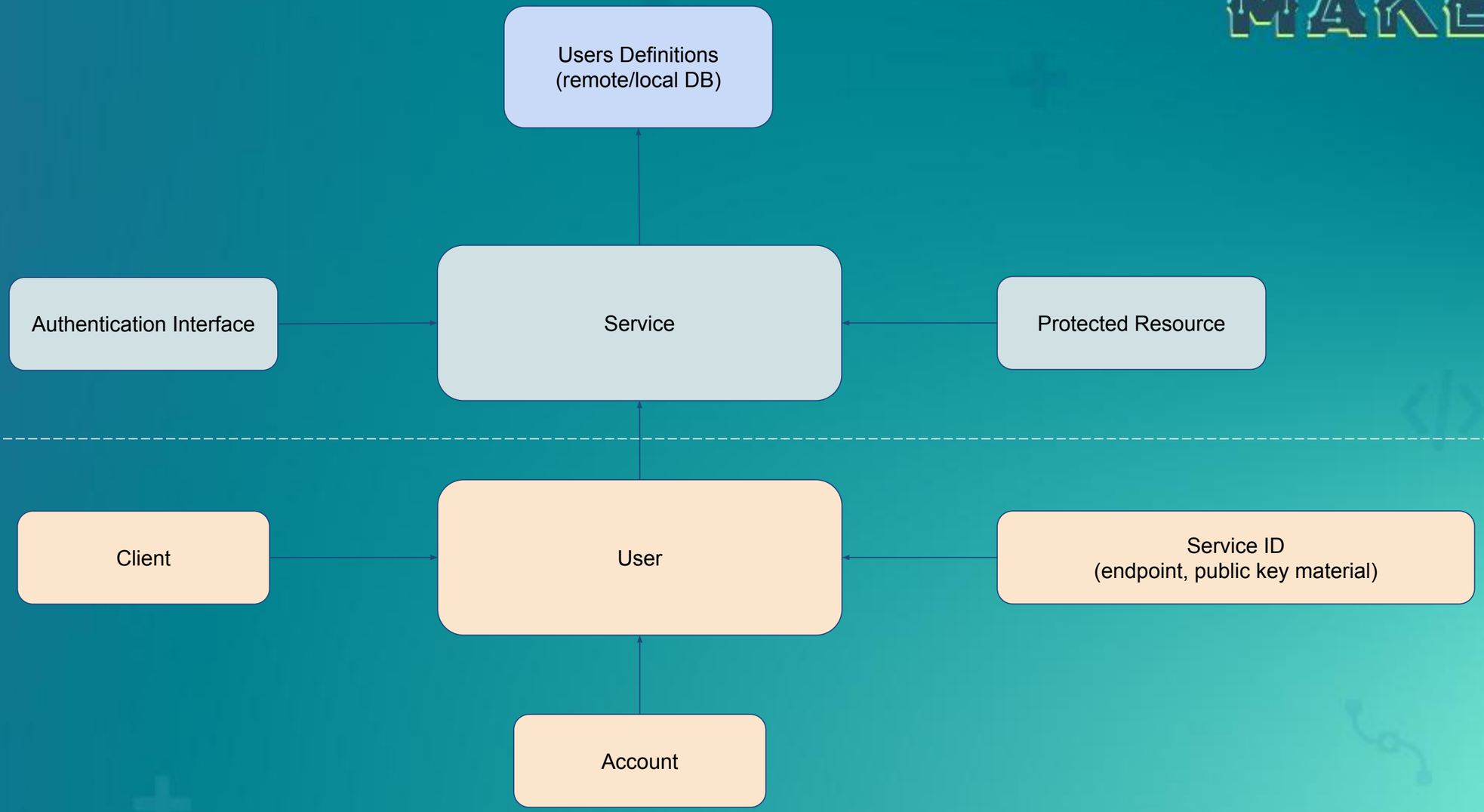
NET MAKERS

Experience in Networking, System Administration, and Software Development.

I have gained **expertise in digital identities** through my work with LDAP and X.500 schemes, and subsequently transitioned to implementing **SAML2 and OpenID Connect 1.0**.

Currently, I **focus primarily on Digital Identity Wallet** Architectures as a government expert for the Department for Digital Transformation. In this role, I also contribute to **standards and technical specifications in this field**.

Authentication System: General Requirements



Tutto Molto Bello, tuttavia …

Il team che amministra il Server governa e o accede a (tutto):

- Definizioni e credenziali di accesso di tutti gli utenti (locali o remote) (… LDAP può fare auth only)
- Credenziali dell'utente che accede al servizio
- Risorsa protetta

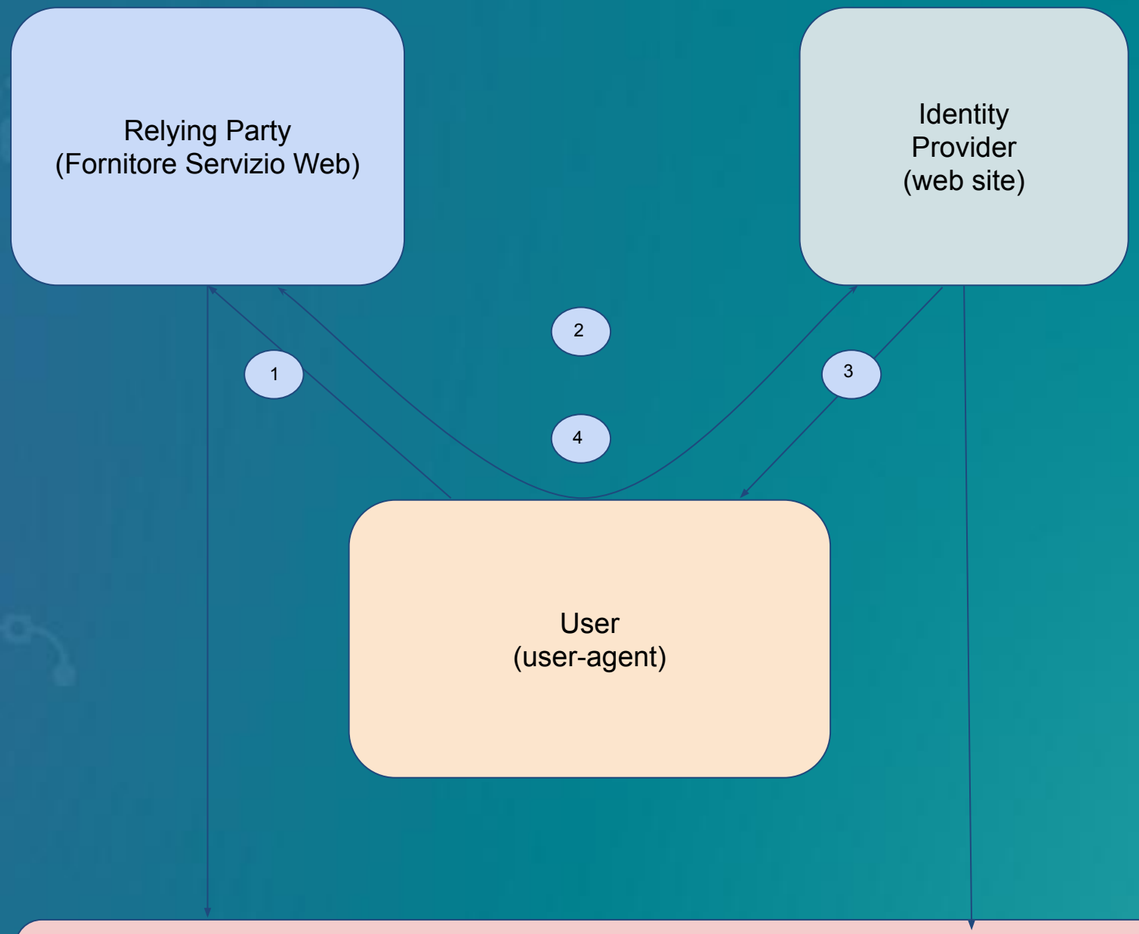
Rischi di Sicurezza:

- Il team che gestisce il front end di autenticazione:
  - ha accesso a tutti i dati del Server
  - può fare audit dei dati in ingresso, intercettare le credenziali e impersonificare un utente senza lasciare alcuna traccia (fattori one-time-use e token non risolvono)

Rischi di Sicurezza e Privacy dei dati connessi alla Scalabilità cross-domain:

- Se il DB utenti è remoto e afferente ad un altro dominio (organizzazione terza):
  - Non è possibile o consigliabile dare accesso alle definizioni degli utenti a terze parti
  - Anche in presenza di contratti e tutele formali, l'abuso tecnicamente è possibile e il rischio evidente

SAML2 or OpenID Connect with Trusted Third Party Model



Modello Federativo e Autorizzativo con Terza Parte Fidata

- Gestore Identità diverso da Risorsa Protetta
- Il RP consente la selezione di molti IDP
- RP produce una richiesta di autenticazione
- Utente consegna la richiesta al IDP
- IDP autentica RP
- Utente immette le sue credenziali su IDP
- IDP autentica Utente
- IDP consegna un token autorizzativo all'Utente
- Utente presenta token al RP
- RP valida token crittograficamente
- RP crea un nuovo account o ricongiunge ad uno preesistente

Problemi Risolti

Modello Federativo (scalabilità cross-domain)

- La terza parte fidata:
  - facilita la nascita di federazioni multilaterali, mediante un Trust Anchor comune è possibile fidarsi di terze parti aderenti alla medesima federazione senza necessariamente stipulare contratti bilaterali
- Discovery Page:
  - L'utente sceglie l'endpoint di autenticazione
- Scalabilità della Fiducia:
  - Delega della fiducia
  - Fiducia transitiva:
    - Esempio: dato che ti fidi di GARR, ti fidi delle organizzazioni da lei fidate, al disotto e nei limiti della sua responsabilità

Trasparenza, Tracciabilità e Non Ripudiabilità

- Gestione del Consenso Utente:
  - Informativa utilizzo e rilascio dei dati
  - Autorizzazione al rilascio e all'uso nel pieno controllo dell'Utente
- Firma elettronica:
  - protegge dal ripudio di una richiesta o di una risposta
- Più parti coinvolte innalzano la garanzia contro eventuali illeciti:
  - un RP può dimostrare l'interazione con un IDP
  - un IDP può dimostrare l'interazione di un Utente con un RP
  - l'Utente può richiedere la cancellazione dei propri dati, IDP e RP difficilmente possono negare di non averli mai ottenuti

Sicurezza: Il RP non ha accesso alle credenziali, non può fare auditing di queste, le credenziali sono usate dall'utente presso il gestore della sua Identità Digitale. Il RP non può auto forgiarsi un Token di accesso.

Tutto Molto Bello, tuttavia ...

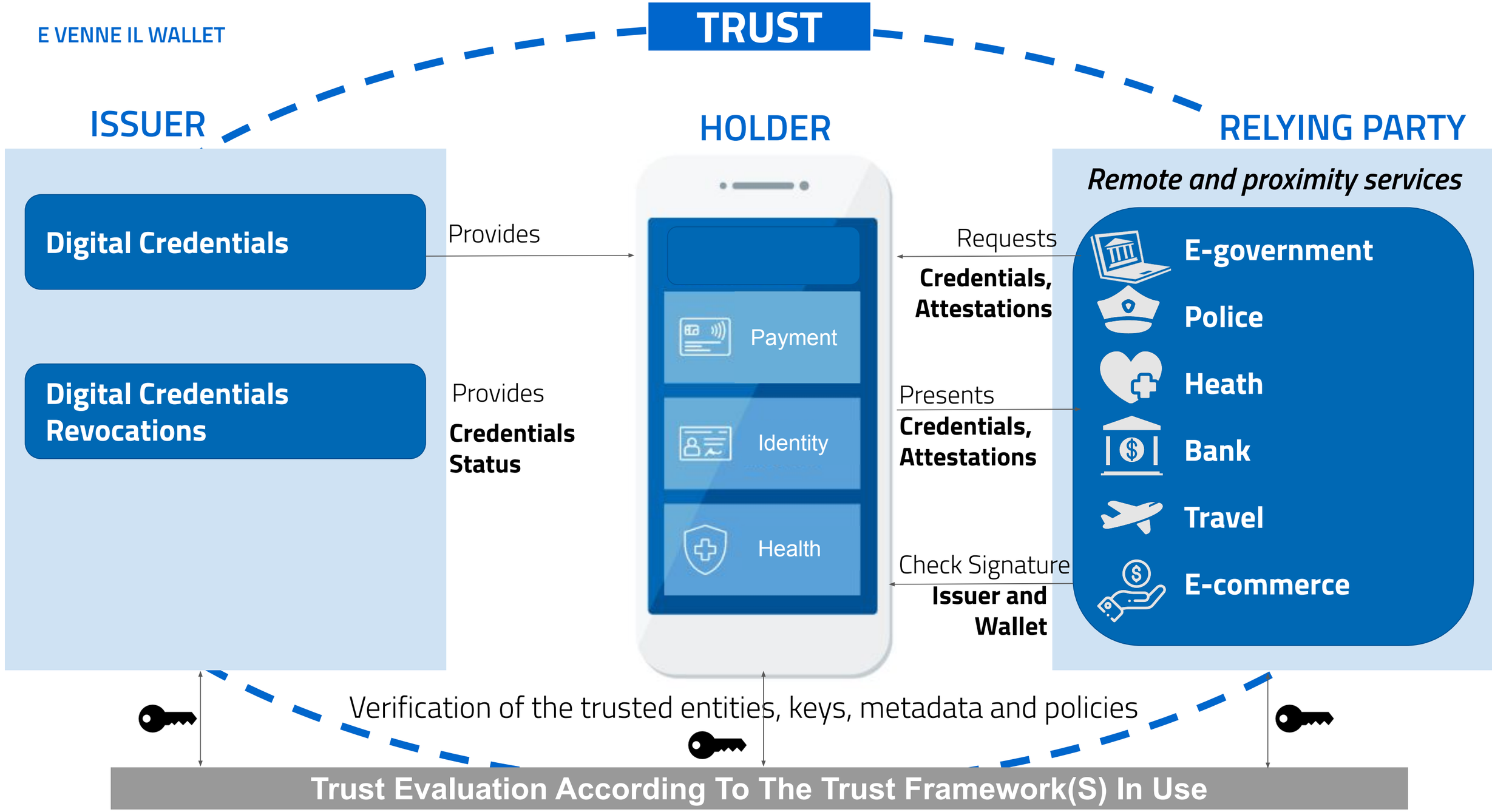
Problemi di Privacy

- Consegna richiesta RP firmata e Gestione del Consenso
  - L'IDP viene sempre a conoscenza del RP presso il quale l'Utente accede:
    - profilazione degli Utenti è possibile

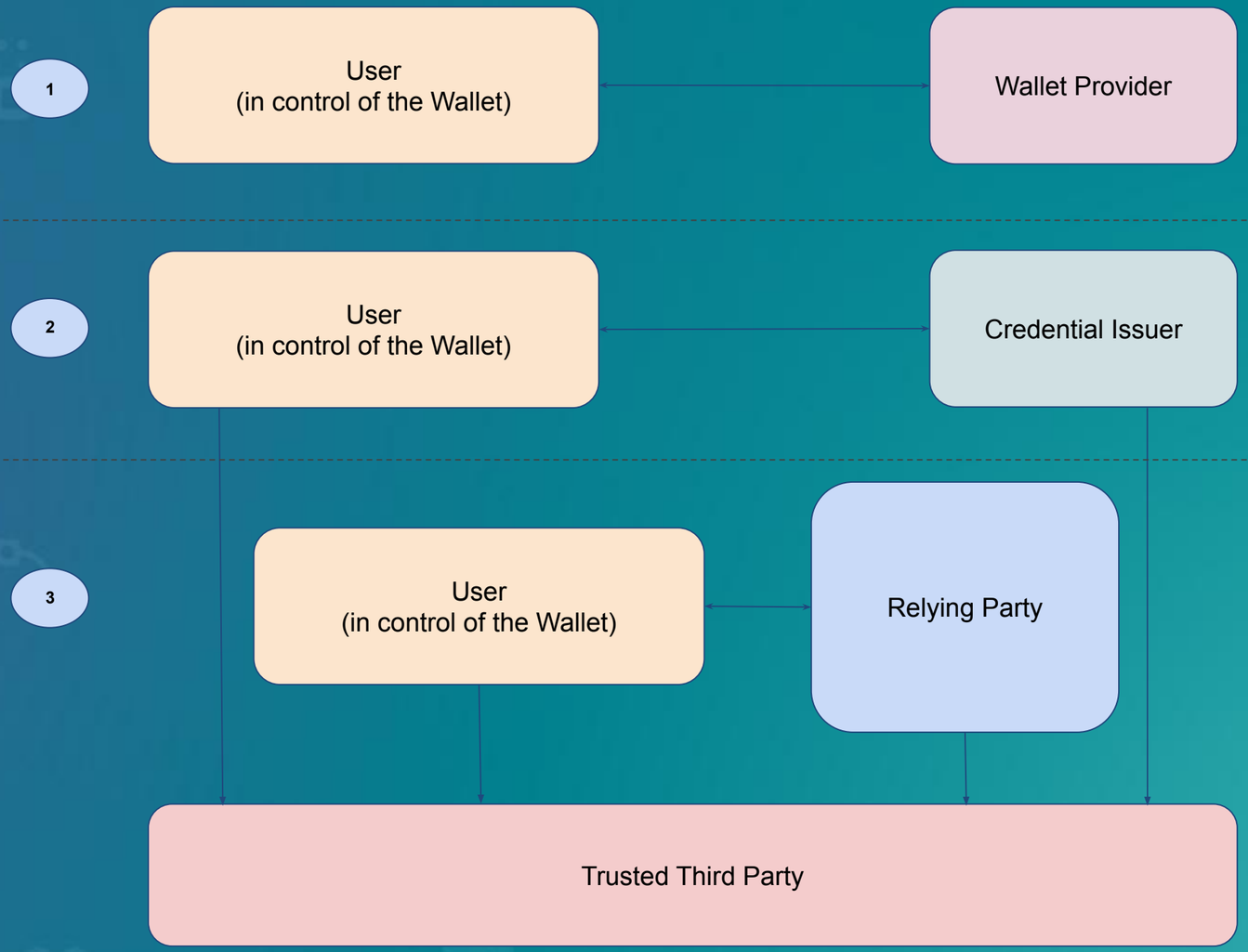
Limiti dei Casi D'uso

- Usabile esclusivamente per l'accesso online ai servizi, non usabile in prossimità (presenza fisica) e in assenza internet

E VENNE IL WALLET



Digital eID Wallet Paradigm in 3 Steps



User establishes trust trust with App Store uses the visual identity of the Wallet Application install and activate it (local authentication).

The User requests a Digital Credential to a Credential Issuer. Wallet Authentication and User Authentication.

The User uses the Wallet to authenticate a Relying Party and theirself to the Relying Party, obtaining the access to the requested protected resource

The RP establishes the trust with the Wallet and with the Credential Issuer, it also checks the revocation of the presented Credentials.

Curiosità del Wallet

Semantica

- Condivisione vs Presentazione
  - Presentare e Condividere sono due casi d’uso completamente differenti
- Holder
  - Utente o Wallet o entrambi?
    - Da letteratura IETF e OpenID: l’Holder è l’Utente.

Privacy

- Paradigma basato sulla rimozione di intermediari e auditors
  - L’uso di proxy geografici non ha senso
  - IAM Proxy all’interno di singoli domini è consigliabile per continuità con sistemi legacy

Tutto Molto Bello, tuttavia ...

Rischi di Sicurezza

- L'uso di Dispositivi Personali aumenta la superficie di attacco. Serve Security Assessment periodico e continuo:
  - Responsabilità del Wallet Provider nel valutare periodicamente lo stato di integrità e sicurezza dei dispositivi personali
    - Controlli della sicurezza locale al dispositivo (API dei vendor sull'integrità dei dispositivi, firma digitale)
- Protezione degli Utenti:
  - Mitigazione: Meccanismi automatici di valutazione della fiducia contro phishing attacks (Policy != Informativa)
- Maggiore complessità può introdurre debolezze implementative:
  - Tanti credential data format
  - Tanti protocolli, remoti e offline
  - LoA transitivo: dal Credential Issuer all'Holder. Il Wallet deve preservare la qualità del LoA proteggendo gli asset critici
- Scarsa Maturità degli standard attuali:
  - Perlopiù draft
  - Bias cognitivo su cosa è Standard e cosa non lo è

Rischi di Privacy

- I meccanismi di controllo delle revoche devono:
  - essere limitati al momento dell'autenticazione dell'utente (altrimenti un RP può sapere quando la tua patente sarà revocata)
  - evitare di informare il Credential Issuer del RP che ha ricevuto le Credenziali

E quindi … Che fare?

È importante

- **Conoscere gli obblighi normativi** e di rilascio, come da regolamento eIDAS. Il paradigma Wallet è un obbligo normativo, affrontiamolo con consapevolezza e preparazione.
- **Comprendere i benefici** e le opportunità del paradigma Wallet, UX migliore rispetto ai sistemi precedenti.
- **Prendere decisioni** su come gestire adeguatamente sicurezza e privacy dei dati.

Todo

- **Partecipare attivamente** alle decisioni (revisioni, commenti, portare la propria voce sui tavoli di standardizzazione)
- Utilizzare algoritmi e approcci stabili:
  - **Favorire l'uso di soluzioni stabili** e concrete piuttosto che visioni o slogan tipicamente "*market & sales*"
- Metterci la testa, **implementare e produrre analisi critiche**, toccare con mano
- **Costruire comunità**, lavorare insieme, costruire una posizione comune, individuare i claim, portare una voce.
- **Realizzare profili implementativi** per la risoluzione dei punti aperti:
  - **Privilegiare sicurezza e privacy** su qualsiasi altro aspetto … Se dovesse venire meno la fiducia il sistema fallirà.

Grazie

Giuseppe De Marco
Dipartimento per la trasformazione digitale