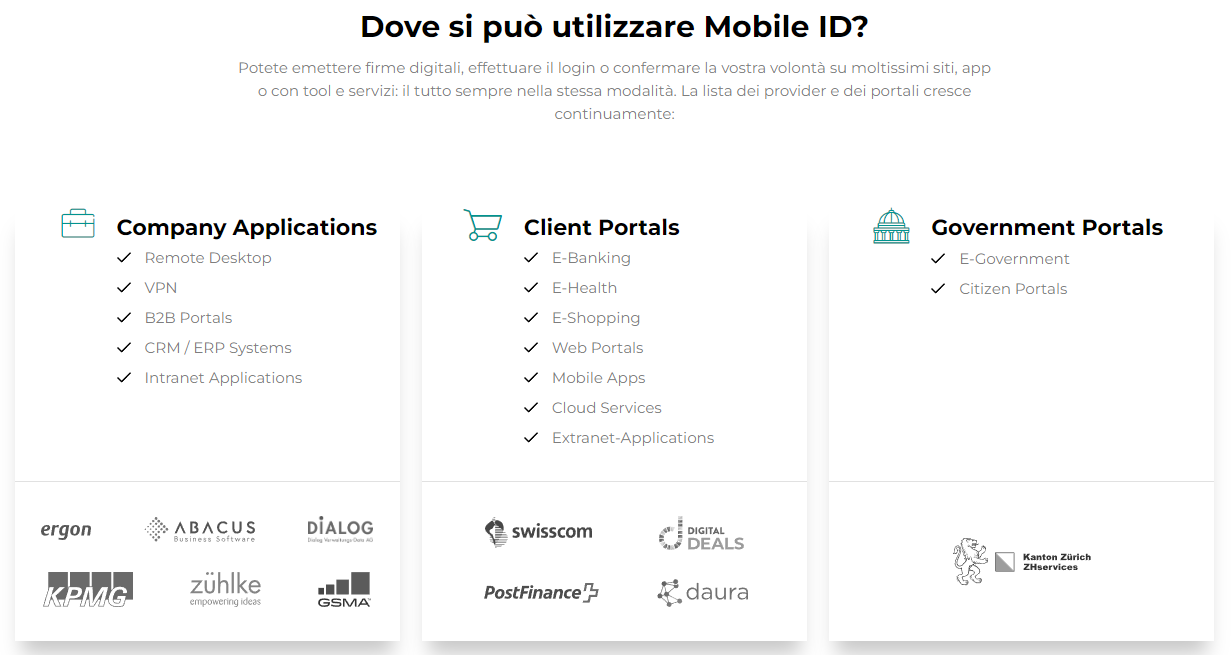
**Report Progettino di autenticazione**

# User multi-factor authentication

## Architettura Mobile ID

Mobile ID permette all’utente di autenticarsi ai servizi online tramite il suo cellulare. Per utilizzarlo è necessario possedere una carta SIM compatibile con Mobile ID, i maggiori operatori offrono SIM compatibili.

Mobile ID può essere impiegato per il Login, per la firma digitale e per confermare una decisione. È una delle autenticazioni a due fattori più sicure al mondo.



Fonte: <https://www.mobileid.ch/it/clienti-privati>

Naturalmente è possibile offrire questa autenticazione ai nostri clienti qualora fossimo noi un’azienda fornitrice di prodotti e servizi (B2B o B2C). (<https://www.mobileid.ch/it/clienti-commerciali>)



Fonte: <https://www.mobileid.ch/it/clienti-commerciali>

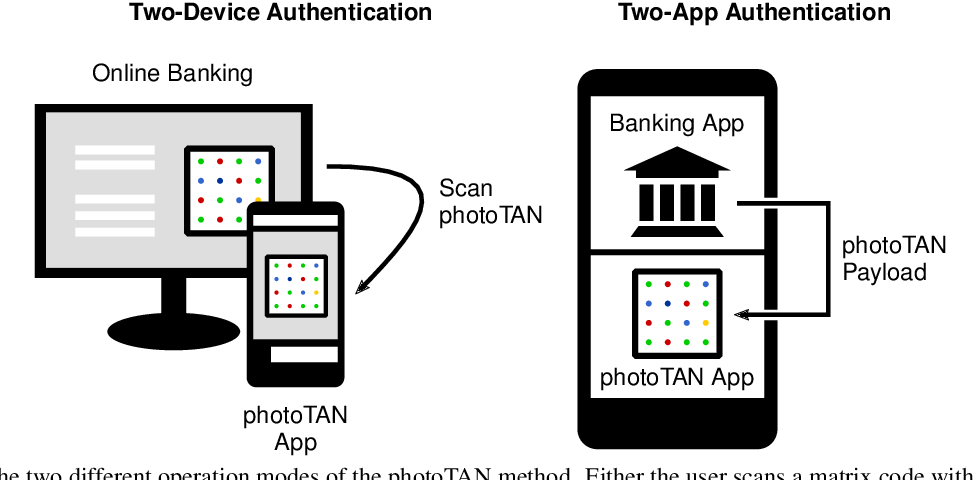
## Architettura con autenticazione mTAN

In questo tipo di autenticazione l’accesso al servizio viene completato tramite l’invio di un codice di conferma via SMS. Questo codice è valido solo per un tempo limitato, solitamente nell’ordine dei minuti.

Inizialmente l’utente inserisce le proprie credenziali (e-mail e password per esempio) dopodiché viene richiesto l’inserimento del numero di cellulare cui inviare il codice per completare l’accesso.

## Architettura Photo-TAN

In questo tipo di autenticazione l’accesso al servizio viene completato tramite l’invio di un mosaico contenente un codice allo schermo dell’utente. L’utente inquadra il mosaico con il proprio cellulare o un apposito lettore decodificando e visualizzando il codice di accesso occultato.



Fonte: <https://www.semanticscholar.org/paper/On-App-based-Matrix-Code-Authentication-in-Online-Haupert-M%C3%BCller/5750f41cf39fd16f75a42b7a736ff2e95bfa5419>

## Architettura biometrica per mobile banking

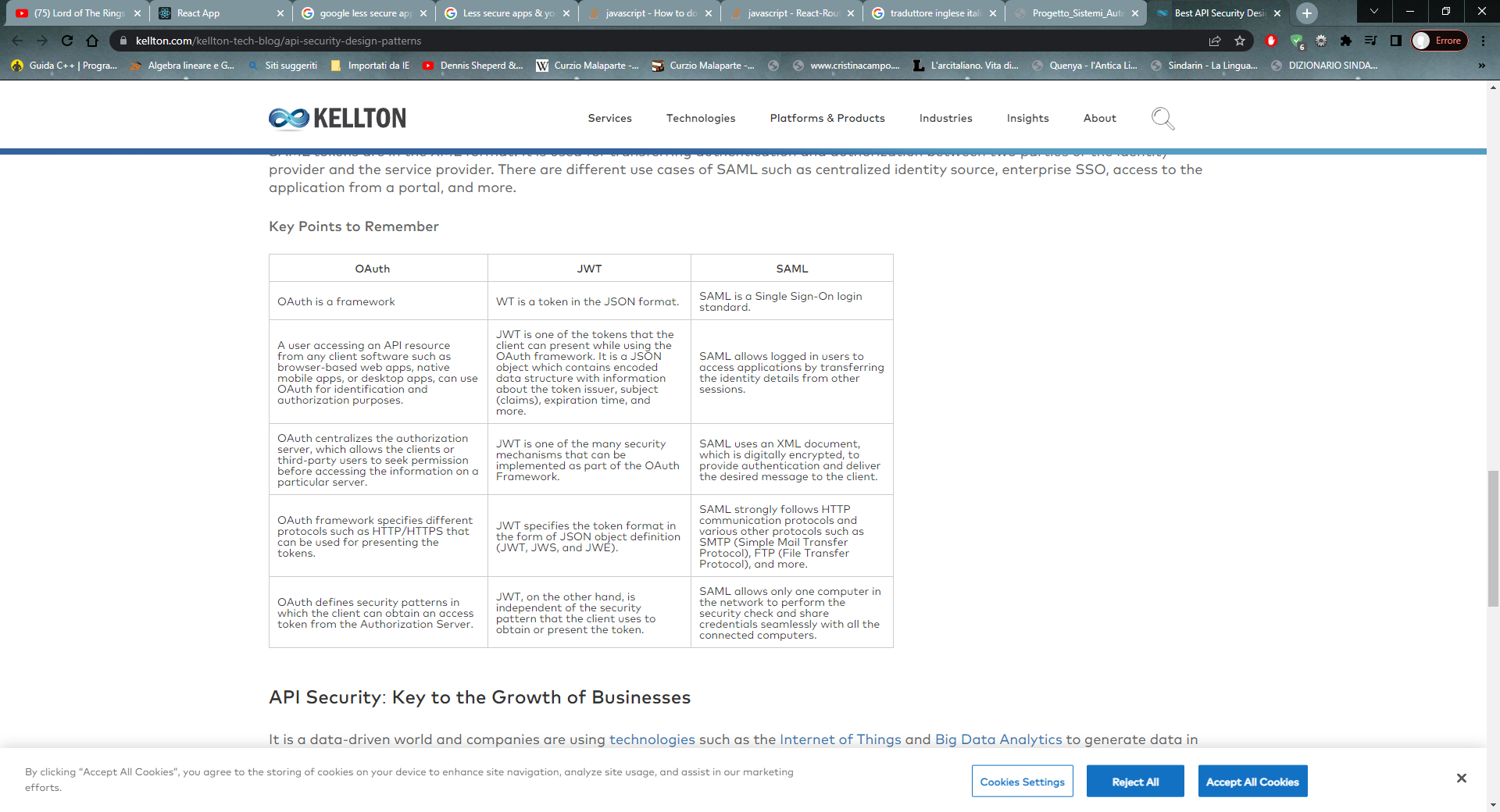
L’autenticazione biometrica sfrutta una “firma” fisica univoca dell’utente.

Questo può avvenire tramite

* Riconoscimento del viso
* Riconoscimento delle impronte digitali
* Riconoscimento degli occhi
* Riconoscimento vocale

Sebbene questi sistemi siano spesso molto sicuri, eventuali fattori esterni possono disturbare il riconoscimento: sole, disturbi sonori, condizioni delle dita, ecc... Inoltre quando il riconoscimento non è programmato correttamente esso può essere superato.

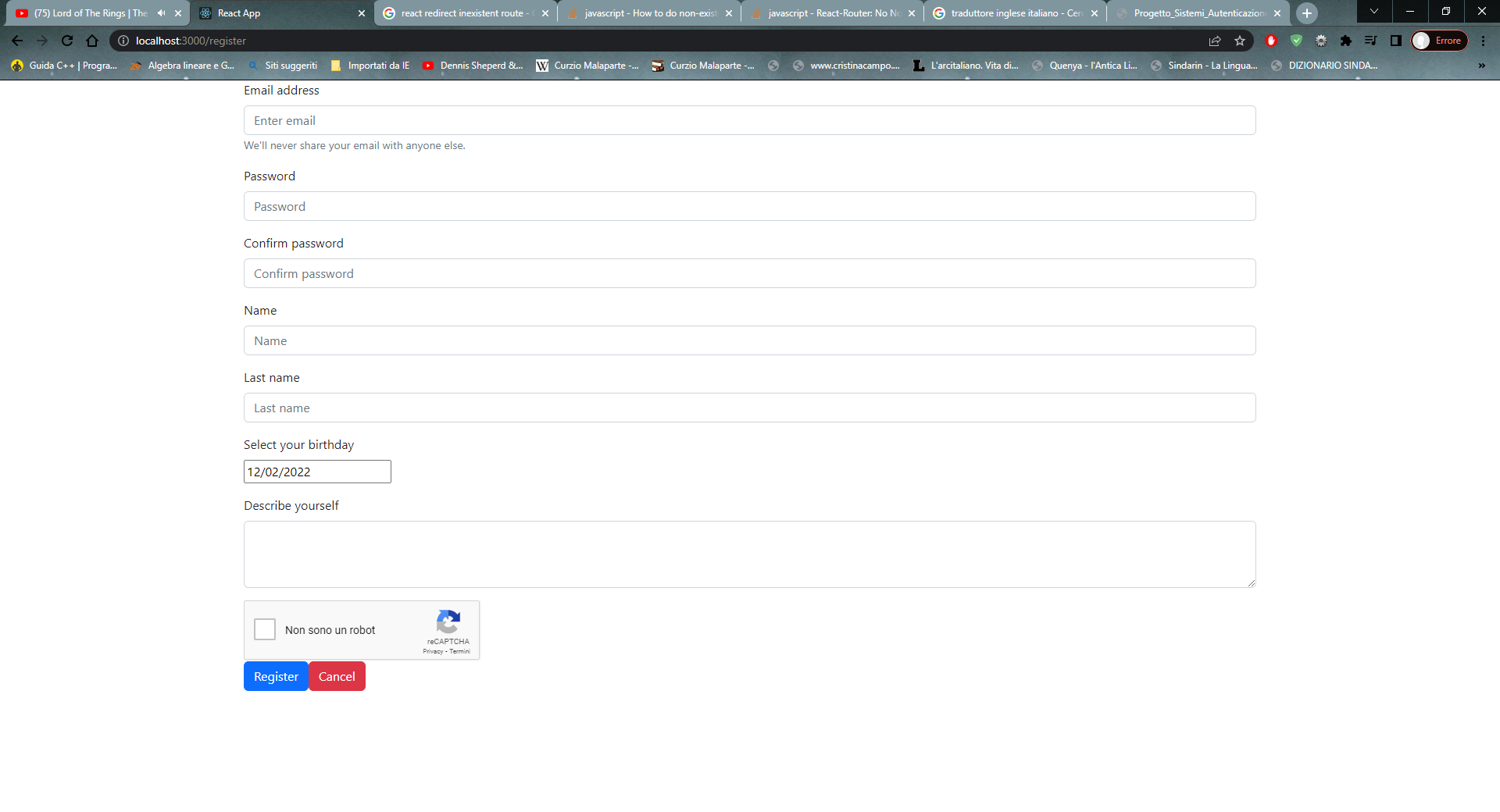
# API sicura

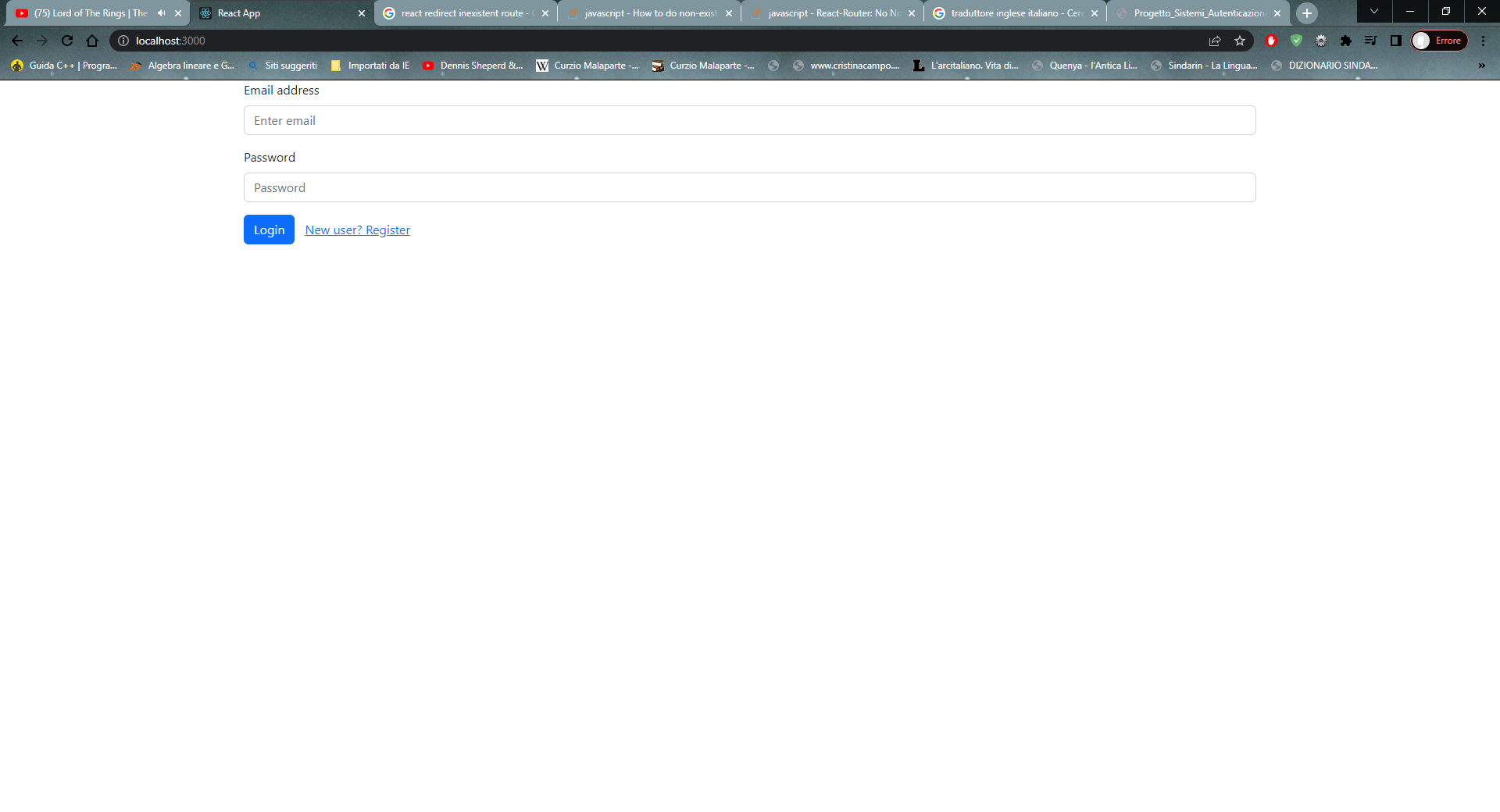


# Progetto JWT

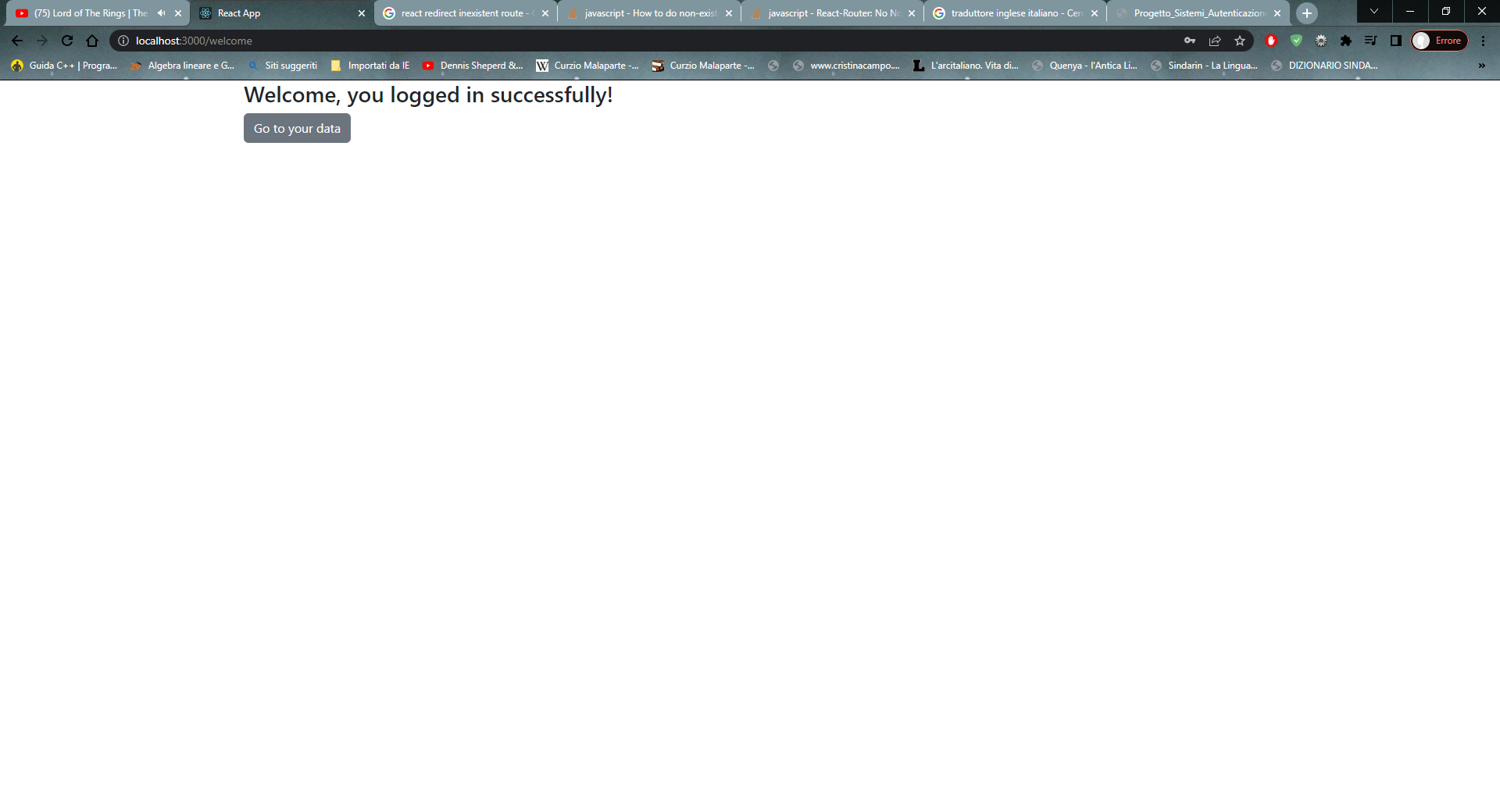
## Panoramica

Il progetto è composto da un sistema di registrazione all’interno del quale è possibile registrare un nuovo utente.

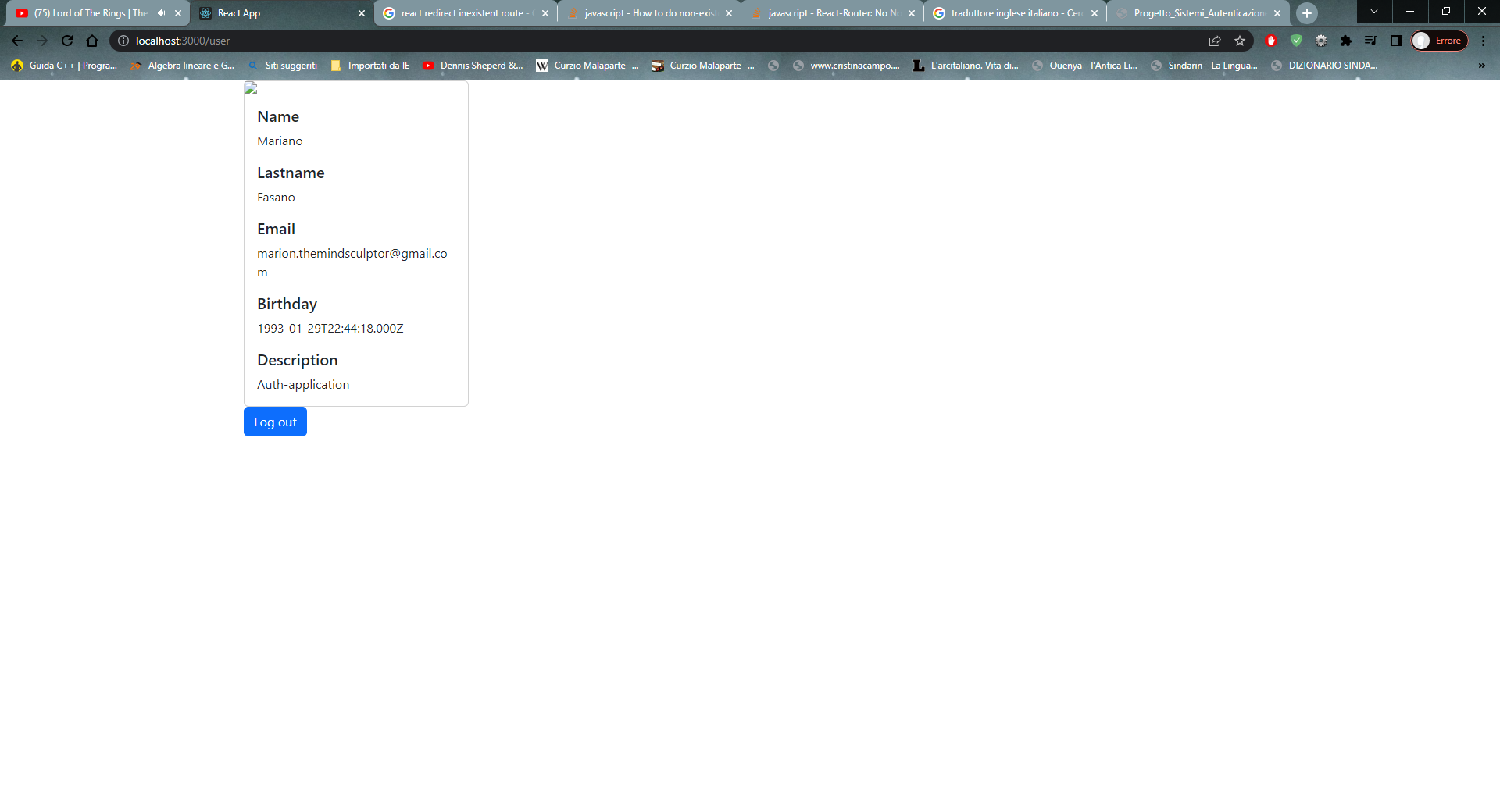
Successivamente l’utente viene autenticato tramite un form di login. Se l’utente è presente nel database e la password è corretta il backend genera e restituisce un token che viene memorizzato all’interno del browser.

Per merito di questo token, jwt, l’utente viene autorizzato ad accedere ad alcune pagine e ad alcuni dati, nello specifico a dati memorizzati al momento della registrazione.

Dal momento che un utente è in possesso del token non potrà più ritornare alla pagina di login, a meno che non effettui un log out. Questo per evitare che ci si possa autenticare più volte. Esso viene indirizzato a una pagina di benvenuto.



Selezionando il pulsante sarà possibile leggere i dati dell’utente, come si può osservare nell’immagine sottostante.



Nel momento in cui l’utente esegue il log out i dati memorizzati localmente sul browser, legati al token, vengono cancellati e si viene indirizzati alla pagina di login.

Il progetto di laboratorio è stato realizzato impiegando le seguenti tecnologie

* Visual Studio Code, come ambiente di sviluppo
* React, per il frontend
* Nodejs ExpressJs, per il backend
* MySQL, in qualità di database

Oltre al principale gruppo sopraccitato, sono state impiegate ulteriori librerie a supporto.

Backend

* **Bcrypt**, necessaria per criptare la password dell’utente
* Body-parser
* Cors
* Dotenv
* **Jsonwebtoken**, utile per creare il token, assegnarvi un payload e verificare i token estratti dall’header
* Mysql2
* Nodemailer
* Nodemon, riavvia automaticamente il backend in caso di modifica del codice
* **Sequelize**, ORM impiegato per l’interazione con il database, molto Js style

Frontend

* **Axios**, per effettuare le chiamate al backend
* Bootstrap
* React
* React-bootstrap
* React-datepicker
* React-dom
* React-google-recaptcha
* **React-hook-form**, per la validazione dei campi, tramite schema yup, lato client
* React-router, implementare il routing lato client (React)
* React-router-dom
* Yup, per gli schemi di validazione

## Funzionamento del token

Ad autenticazione compiuta, il backend fornisce e invia un token che il frontend memorizza nel browser. Nelle successive richieste per le quali si necessita di un’autorizzazione si inserisce nel header, per esempio di axios, il token come Bearer token. Successivamente il backend estrarrà e verificherà il token. Da esso è possibile estrarre il payload nel quale è contenuto l’indirizzo e-mail dell’utente loggato.

Al log out si cancella il token lato browser.

Miglioramenti e sviluppi futuri

Escluso il token e gli accorgimenti per evitare autenticazioni doppie è stato aggiunto l’indirizzamento predefinito nel caso l’utente cerchi di raggiungere delle route lato client inesistenti.

Se per esempio si cercasse di raggiungere “/nome-di-route-inesistente" l’utente verrebbe indirizzato alla route root di login, la quale, se l’utente fosse in possesso del token, indirizzerebbe a sua volta alla pagina di benvenuto.

Si sono aggiunti due controlli aggiuntivi a livello di sicurezza, entrambi in fase di registrazione. Il primo è un recaptcha di Google con lo scopo di evitare registrazioni automatiche di utenti, mentre il secondo consiste in una e-mail di verifica dell’account.

Entrambi i sistemi hanno incontrato dei problemi durante l’implementazione. Il recaptcha sembra non raggiungere la verifica dell’API di google, dalla quale si dovrebbe ottenere, fra altre informazioni, un campo “success” di tipo booleano che ci indica se la verifica è andata a buon fine. Tuttavia secondo un console.log() del campo menzionato ciò che si ottiene è un “undefined”. Rimane da indagare sul motivo di questo non funzionamento, poiché un primo test su un progetto esterno ha avuto esito positivo (tuttavia impiegava tecnologie differenti). L’e-mail di verifica ha incontrato qualche difficoltà poiché da maggio 2022 (<https://support.google.com/accounts/answer/6010255?hl=en> ) Google non supporta più applicazioni di terze parti che permettono un livello di sicurezza inferiore e molti esempi di implementazione sono precedenti a quella data. In un caso l’e-mail è stata spedita ed è arrivata al destinatario, non riuscendo però a completare il controllo per la verifica. In quel caso era stato un problema legato alla gestione della route, mentre l’invio è stato infine permesso grazie all’abilitazione della verifica in due passaggi e alla scelta di una password per delle app (ed è stata la password utilizzata per l’invio della mail). Un ultimo test non ha portato inconvenienti per il recaptcha e abbiamo potuto registrare l’utente, mentre l’e-mail di conferma pare essere partita ma mai giunta all’utente. Perciò la verifica dell’account tramite e-mail rimane parzialmente incompleta.

Questi sono in breve alcune problematiche ancora in fase di risoluzione.

Un ulteriore controllo mancante è la validazione dei campi lato server, al momento avviene solo lato client ed è funzionante. Inoltre sarebbe anche da implementare la scadenza (expiration time) del token.

# Framework OAUTH2

## OAUTH2

OAuth 2.0 authorization framework è un protocollo standard open source per l’autorizzazione che si basa su SSL. Permette agli sviluppatori di implementare facilmente un sistema sicuro che fornisce flussi di autorizzazioni alle risorse protette, alle applicazioni web, applicazioni mobile e applicazioni desktop, come ad esempio la condivisione di risorse tra due siti web distinti. Queste autorizzazioni vengono concesse senza immettere le proprie credenziali e le comunicazioni avvengo tutte con il protocollo HTTP.

In pratica il sistema è molto semplice, OAuth introduce un livello di autorizzazione fornendo un determinato ruolo al proprietario di una risorsa e un altro ai clienti che richiedono tale risorsa. Quando un cliente richiede una risorsa, ospitata su un server e controllata da un proprietario, OAuth fornisce a tale richiesta un token di accesso.

Il token di accesso ricevuto da OAuth ha diversi attributi, tra cui ad esempio la sua scadenza. L’applicazione che ha creato il token- Il formato del token è JSON Web Token (JWT).

Il token inoltre ha anche dei permessi che vengono chiamati Scopes.

L’invio del token da parte del client verso il server può essere fatto in due modalità distrinte:

1. Attraverso bear token, ovvero tramite GET o POST, esempio:  
   GET / http/1.1  
   Host: supsi.ch  
   Authorization: Bear token
2. MAC (Message Authentication Code), calcolato tramite gli elementi della richiesta e inoltrato all’intestazione dell’auatorizzazione.

I ruoli di OAuth sono essenzialmente 4:

* Proprietario della risorsa
* Server che ospita la risorsa
* Cliente (applicazione)
* Server di autorizzazione (OAuth)

## Differenze tra OAuth e JWT

La principale differenza per iniziare è che JWT (Json Wen Token) è solo un formato di token firmato digitalmente (il client non li può modificare), fornisce infatti un sistema compatto per trasmettere i dati, mentre OAuth definisce un protocollo di autenticazione e trasmissione del token.

I JWT vengono generati dal server e inviati al client, dopo di che il client lo archivia in modo che possa essere riutilizzato ad ogni richiesta che il client fa al server. Dunque non bisogna fare nessuna interrogazione al database.

I JWT non hanno la complessità di OAuth, infatti sono solo un token in formato Json, dunque una semplice stringa. Ciò rende JWT più veloce da verificare.

La sicurezza di OAuth è maggiore, infatti è testato praticamente in tutti i casi limite di sicurezza.

Si può utilizzare OAuth anche assieme a JWT per avere un livello maggiore di sicurezza!

# Autenticazione JWT – pratica

Eventuali rischi legati all’impiego dei token jwt è che qualcuno possa decodificarli e scoprire al suo interno delle informazioni rilevanti. Nel nostro caso la decodifica porterebbe alla luce un indirizzo e-mail. Esso è sì un dato personale e privato dell’utente, però il token non contiene altro di rilevante e a partire dalle e-mail non è in grado di risalire alle altre, quindi un aggressore si ritroverebbe un indirizzo e-mail e niente più.

# Fonti

Capitolo 1:

Mtan <https://www.ebas.ch/it/mobile-tan-mtan-sms-tan/>

Photo tan <https://www.ebas.ch/it/procedura-photo-tan-procedura-con-tan-ottico/>

Mobile id

<https://www.mobileid.ch/it>

<https://www.postfinance.ch/it/privati/prodotti/digital-banking/mobile-id.html>

<https://www.swisscom.ch/it/business/enterprise/offerta/security/application-and-endpoint-security/mobile-id.html>

Biometrica

<https://www.onespan.com/it/topics/biometric-authentication>

Capitolo 2:

<https://www.kellton.com/kellton-tech-blog/api-security-design-patterns>