DataKrypto

DK
Identity

Proteggi il tuo accesso

DK Identity

DK Identity è un'applicazione iOS e Android, che permette l'autenticazione dell'utente tramite QR-Code senza bisogno di digitare alcun tipo di credenziali. Dopo un processo di registrazione all'interno di DK Identity, l'utente può organizzare le proprie credenziali. Queste ultime vengono registrate e cifrate all'interno dell'applicazione stessa e possono essere aggiunte o manipolate dall'utente.
DK Identity invia e riceve dati da un server di autenticazione che a sua volta, attiverà un processo che potrà essere utilizzato per autenticare l'utente all'interno di pagine e applicazioni "web based" o ancora più semplicemente, all'interno del sistema operativo Windows.
Nel caso d'uso del login di Windows, l'applicazione dialoga con un sistema di credenziali personalizzato, che visualizza un QR-Code sullo schermo. Basterà dunque mostrare il QR-Code all'applicazione mobile DK Identity, per eseguire il login automatico e accedere al sistema operativo. Per le pagine web è necessaria un'integrazione affinché tale processo sia reso possibile.

Qualunque sia il caso d'uso, l'applicazione mobile dialogherà sempre con un server di autenticazione appartenente al cliente. In questo modo, qualunque azienda può ottenere il controllo totale su chi accede alla proprietà dell'azienda stessa e potrà revocare l'autorizzazione in qualunque momento, tramite il server di autenticazione.

Patent pending

Download on the App Store

ANDROID APP ON Google play

DataKrypto

Come funziona

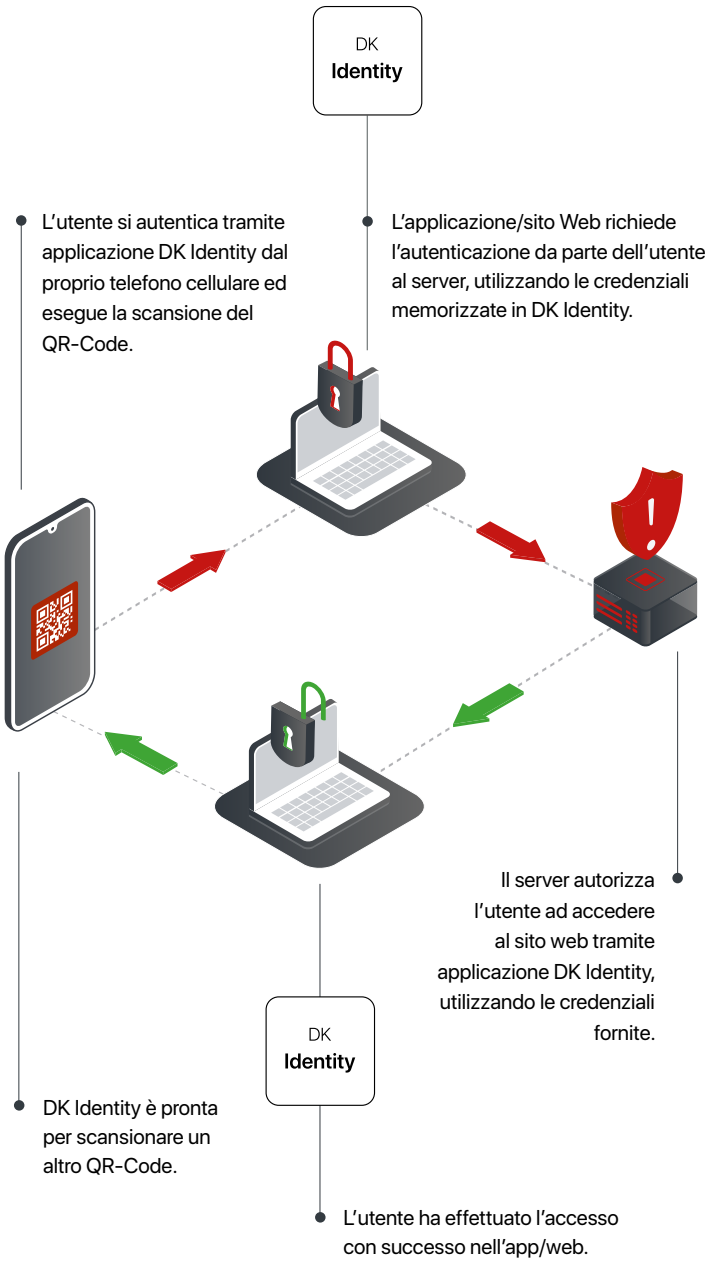
DK Identity

Il primo passo in DK Identity è la registrazione come utente che permette di identificare ed associare l'utente stesso al dispositivo.

Questo processo può riguardare una procedura aziendale personalizzata per autenticare e verificare l'utente o può riguardare un'autenticazione a doppio fattore automatizzata.

Durante il processo di registrazione l'utente può essere anche associato alla sua autenticazione biometrica.

Il risultato di questo processo è una stretta connessione tra l'utente e il dispositivo che utilizza l'autenticazione a doppio fattore e la firma biometrica.



DataKrypto

Caratteristiche

DK Identity

Autenticazione

- Iscrizione:
  1. Autenticazione a doppio fattore veloce e sicura;
  2. Accoppiamento biometrico: accoppiamento stabile tra utente e dispositivo;
  3. Processo aziendale (facoltativo).
- Login:
  1. Login veloce
  2. Login manuale (username + password);
  3. Login biometrico (face-id or fingerprint).

Credenziali

- Memorizzazione di credenziali crittografate.
- Gestione credenziali:
  1. Aggiunta
  2. Modifica
  3. Eliminazione

QR-Code

- Facile da implementare in applicazioni e pagine Web;
- Possibilità di abilitare il login biometrico obbligatorio;
- Possibilità di abilitare il geofencing per il login;
- Possibilità di ricevere l'immagine della persona che effettua il login.

Sicurezza

- Utilizzo di password e criteri complessi;
- Sicuro (RSA 4096 bit, AES-256, SHA-384);
- Gestione delle credenziali (gestore password).

DataKrypto

Installazione

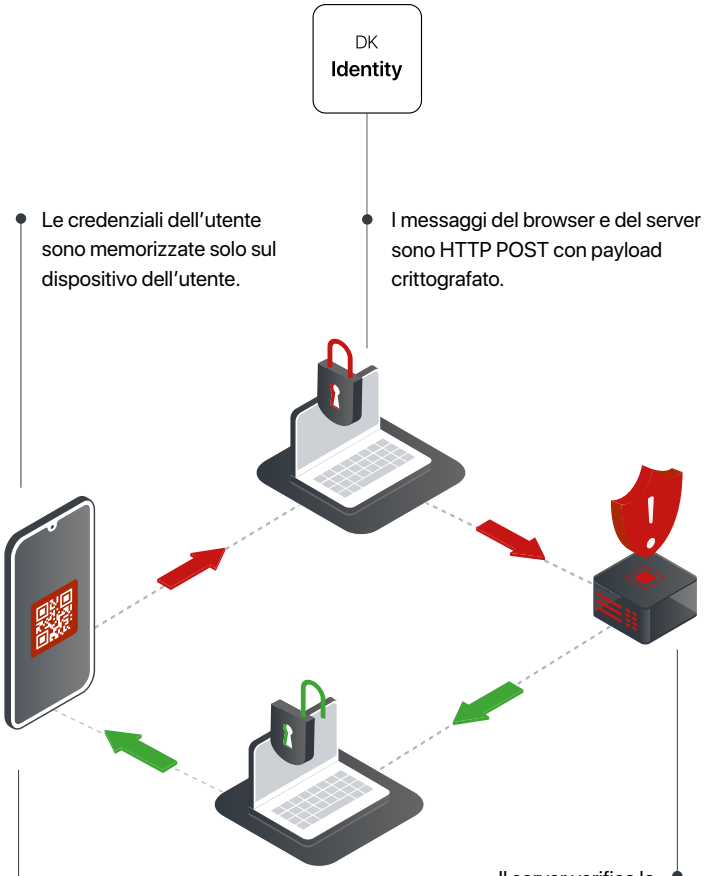
DK Identity

- L'applicazione DK Identity può essere scaricata da Apple Store e Google Play Store;
- Il QR-Code è implementato sul sito tramite librerie proprietarie;
- Ogni QR-Code può essere personalizzato. Uno strumento di configurazione contiene l'impostazione del codice QR;
- La guida per l'utente è disponibile dopo il download.

DataKrypto

Architettura

DK Identity

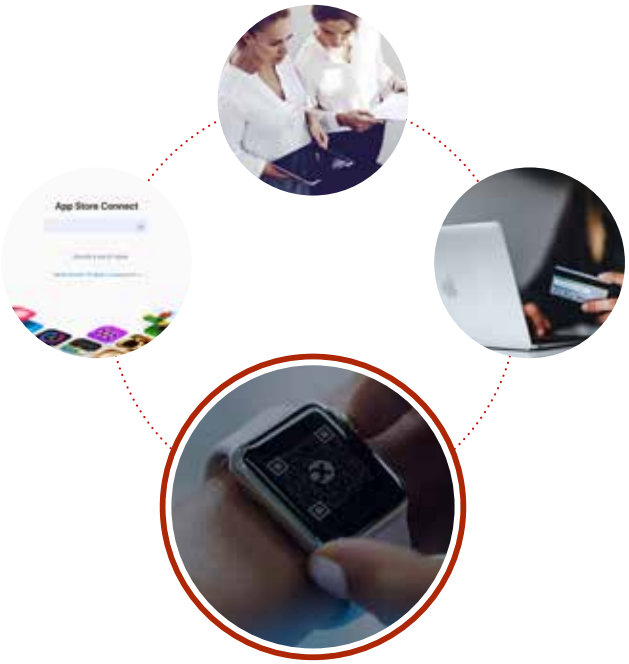


DataKrypto

Applicazioni

DK Identity

Con l'aumento del "remote working", la necessità di accedere in maniera protetta e sicura è diventata un fattore fondamentale per tutte le aziende che oggi dedicano sempre più attenzione al tema della sicurezza. Le credenziali di accesso ai sistemi aziendali sono oggi una delle principali informazioni a rischio di furto.



Healthcare

La tutela dell'accesso del personale ospedaliero ai sistemi informativi del proprio ospedale è fondamentale per il trattamento dei dati sanitari dei propri pazienti, quali cartelle cliniche, anamnesi, terapie. Tutti i dati altamente sensibili sono soggetti a rigide normative per la loro conservazione e integrità.

Enterprise

Le grandi aziende hanno bisogno di controllare migliaia di accessi da parte dei propri dipendenti, spesso in paesi diversi e da remoto. Sapere che ogni dipendente ha a disposizione un'applicazione in grado di rendere sicuro il suo login è un ulteriore elemento di sicurezza per l'azienda.

E-commerce

La gestione di un e-commerce è da tempo un fattore critico di successo per un'azienda. Gli attacchi hacker si susseguono con sempre maggiore frequenza ed è fondamentale mantenere al sicuro tutte le credenziali di accesso ai sistemi di back-end, per evitare l'accesso da parte di persone non autorizzate.

DataKrypto Company
Via Marche, 54 - 00187 Rome, Italy

www.datakrypto.com
email: info@datakrypto.com - tel. +39 06 5413047