FIDO

Un nuovo standard per un
mondo senza password.

Ricordare decine e decine di password per accedere ai nostri servizi online preferiti è un allenamento quotidiano indispensabile per la nostra vita digitale.

Tali password, molto spesso, sono sempre uguali o poco complesse, e ci mettono a rischio rispetto a potenziali attacchi informatici che vediamo proliferare giorno dopo giorno.

Con l'avvento del **GDPR** le aziende hanno dovuto adottare nuove regole, nuove procedure interne e nuove misure di sicurezza per proteggere i dati dei propri clienti e utenti, evidenziando cosi l'importanza di mettere in campo nuove soluzioni e nuove tecnologie per il raggiungimento di tale scopo.

Nel contesto europeo abbiamo visto tracciarsi un percorso ben definito riguardo all'adozione di protocolli e regolamenti condivisi tra gli Stati membri (**eIDAS**, **GDPR**, **PSD2**, etc…) per far sì che possa esserci un'interconnessione tra i servizi digitali dei singoli Paesi e raggiugnere l'obiettivo del Mercato Unico Digitale Europeo.

L'identità personale legata all'utente di un servizio digitale è l'elemento principe su cui negli anni si sono avvicendate varie soluzioni pubbliche e private, con l'obiettivo di risolvere il problema dell'**identificazione certa ed inequivocabile della persona** che è dietro il device e che sta eseguendo le operazioni sui canali digitali.

Come sappiamo, questo sarà sempre un argomento di discussione e che muterà nel tempo con l'evolversi degli strumenti tecnologici.

Sulla base dello stato tecnologico odierno, nel 2009 è nata la "**FIDO Alliance**", fondata da Validity Sensors e Paypal e a cui negli anni si sono aggiunte tutte le maggiori società tecnologiche del mondo (Samsung, Google e Microsoft solo per citarne alcune), con lo scopo di sviluppare uno "**standard**" per **consentire l'identificazione dell'utente senza l'utilizzo di password** e con il supporto dei device posseduti dall'utente (pc, table, smartphone, chiavi di sicurezza).

FIDO E' UNO STANDARD

Cosi come conosciamo il WiFi o il Bluetooth, è opportuno cominciare a conoscere anche l'acronimo **FIDO** (**Fast Identity Online**), uno standard sviluppato e promosso dalla **FIDO Alliance** di cui fanno parte le maggiori aziende tecnologiche (e non) al mondo.

Anche **Myntech**, con l'obiettivo di supportare aziende ed enti pubblici nell'adozione di questo nuovo standard e di fornire soluzioni digitali basate su questo paradigma, **è entrata a far parte dell'Alleanza nel 2020**.

CRITTOGRAFIA

Quello che fa di FIDO uno standard interessante, non è soltanto la possibilità di autenticarsi senza password, ma è soprattutto la metodologia con cui questo avviene e che cambia le regole del gioco in tema di sicurezza informatica.

FIDO sfrutta la crittografia con l'utilizzo di **chiavi pubbliche e private** per effettuare una cosiddetta "**strong authentication**", in particolare, durante il processo di autenticazione, **la chiave privata viene conservata esclusivamente nel device dell'utente, mentre solo la chiave pubblica viene memorizzata dal servizio online.**

PERCHE' E' UNA NOVITA'

Quando oggi ci registriamo ad un servizio digitale, questo non sa se siamo davvero noi o se le nostre password le sta utilizzando un'altra persona per nostro conto.

Con questa metodologia, invece, il servizio digitale può dire con una quasi assoluta certezza che siamo davvero noi e, soprattutto, le nostre password non saranno più conservate dall'azienda che eroga il servizio.

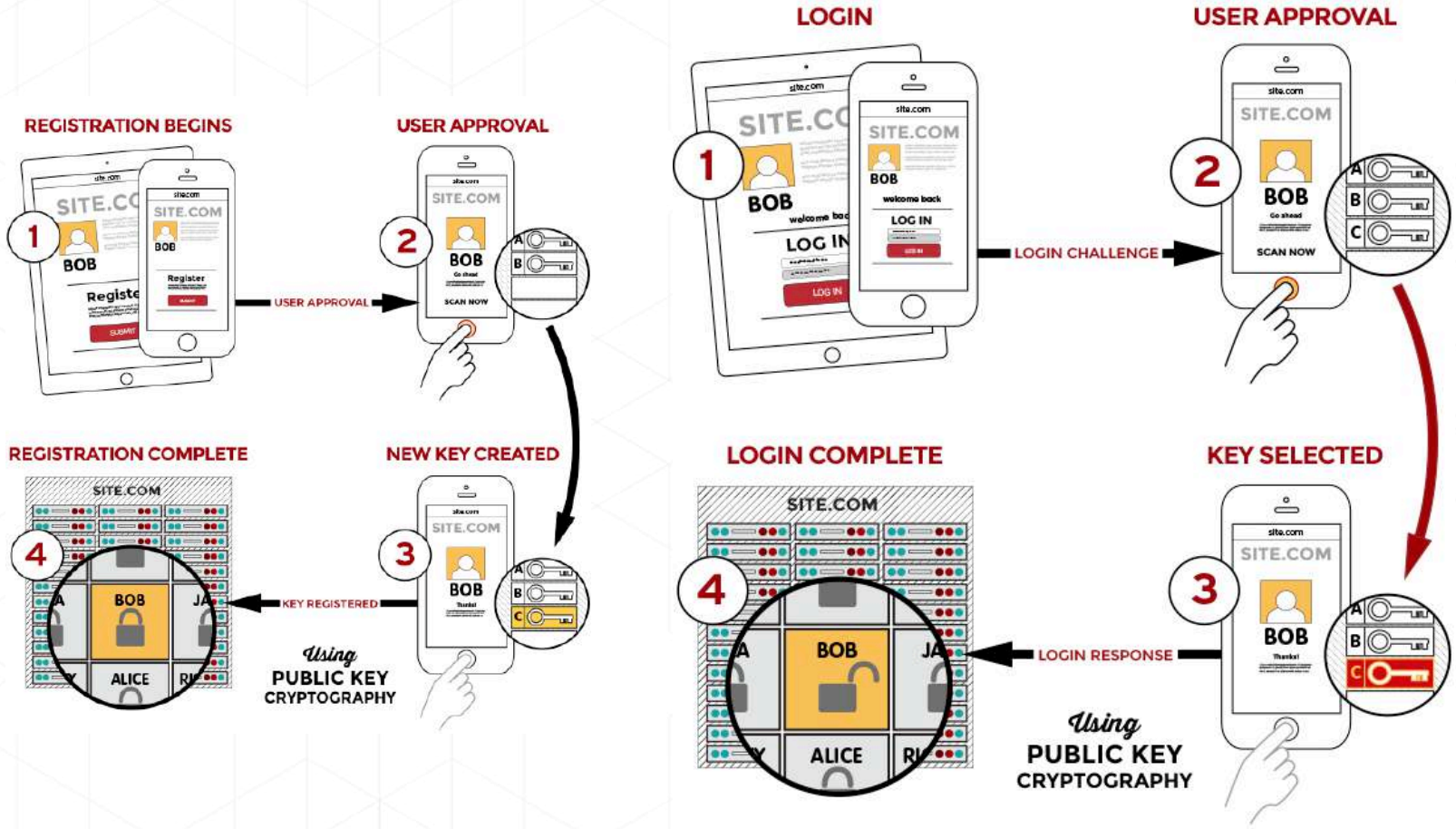
Di conseguenza, da un lato le aziende verranno sollevate finalmente dal gravoso compito di proteggere le password degli utenti, dall'altro lato **gli utenti saranno fisicamente in possesso della propria identità digitale**.

SBLOCCARE IL PROPRIO DEVICE

Una volta che ho deciso di autenticarmi o registrarmi al servizio digitale, FIDO mi chiede di sbloccare il device che sto utilizzando per verificare che sia effettivamente io.

Se sono su un PC o su uno smartphone posso sbloccare il device attraverso un **PIN**, il **FaceID**, il **Fingerprint** o attraverso il **codice di sblocco**; se, invece, ho una **chiave di sicurezza** esterna posso sbloccarlo cliccando il pulsante che è posto su di essa o avvicinarla al device sfruttando la tecnologia **NFC**.

Solo dopo averlo sbloccato, si attiverà il meccanismo per cui la mia chiave privata dialogherà con la mia chiave pubblica in possesso del servizio digitale.

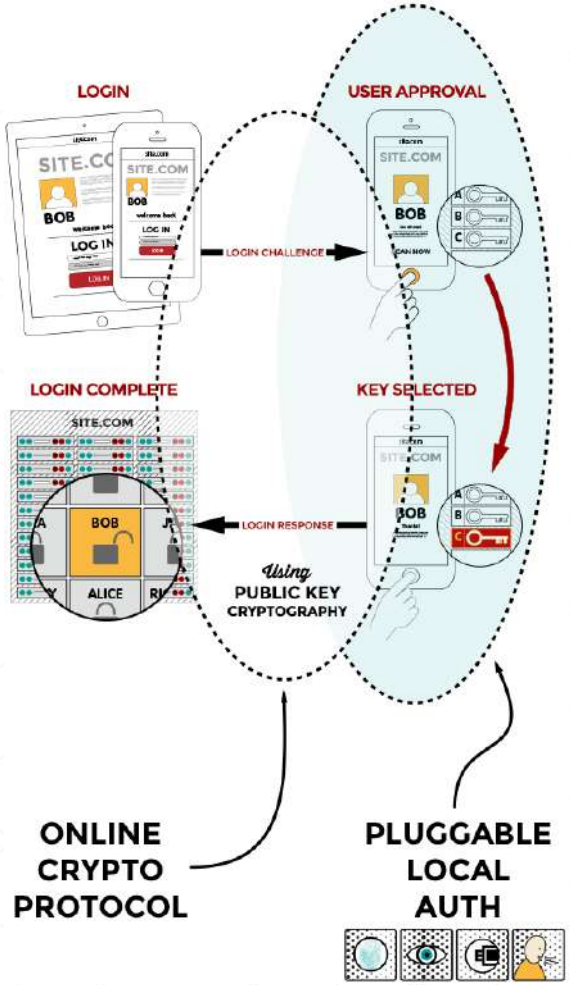


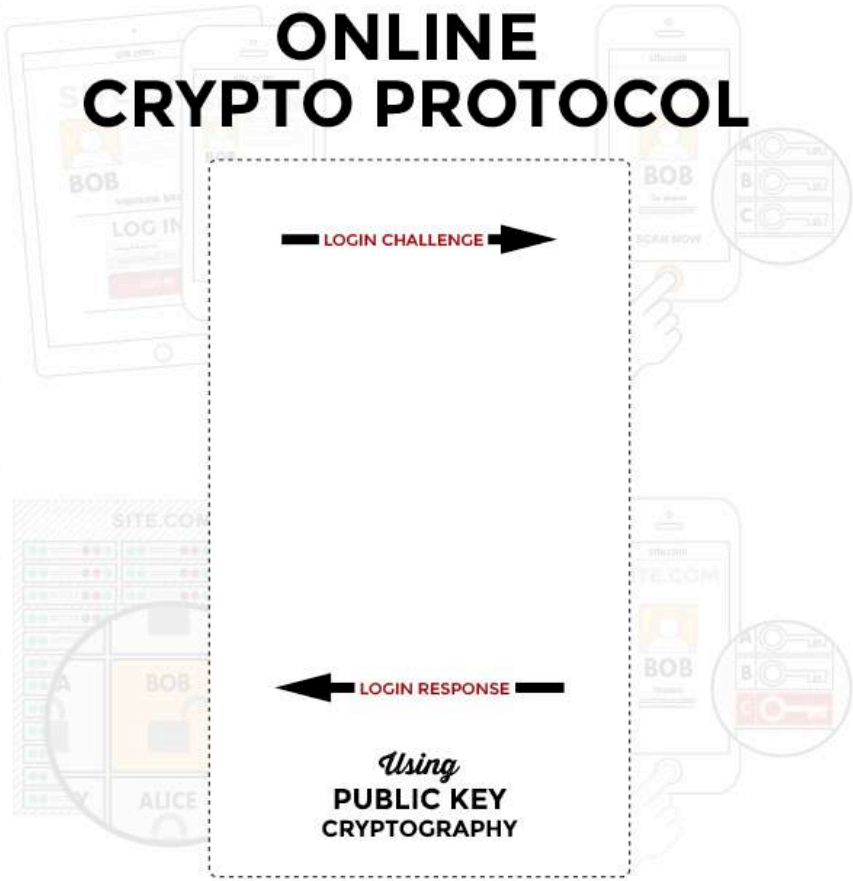
CAMBIO DI PARADIGMA

I concetti di base del protocollo FIDO sono la facilità di utilizzo, la privacy e la sicurezza, e la standardizzazione.

Negli anni molte aziende si sono impegnate per implementare con soluzioni proprietarie questo intero stack di clients e protocolli.

FIDO ha cambiato il paradigma standardizzando sia i clients che i protocolli ed utilizzando la crittografia attraverso le chiavi pubbliche e private che servono alle parti per abilitare il processo di autenticazione.





CAMBIO DI PARADIGMA

FIDO2 è il naming dato dalla FIDO Alliance a questo nuovo stack tecnologico.

Le specifiche FIDO2 sono le specifiche del W3C "WebAuthn" e il corrispondente protocollo "Client-to-Authenticator" (CTAP) della FIDO Alliance.

WEB AUTHENTICATION (WEBAUTHN)

WebAuthn abilita i servizi digitali nell'utilizzo dell'autenticazione FIDO attraverso una web API standard che può essere costruita all'interno dei browser Web.

WebAuthn è stato designato come uno **standard ufficiale a Marzo 2019** ed è attualmente supportato da Windows 10, Android, Google Chrome, Mozilla Firefox, Microsoft Edge ed Apple Safari.

CLIENT TO AUTHENTICATOR PROTOCOL (CTAP)

CTAP abilita casi d'uso estesi attraverso l'utilizzo dello standard FIDO e **dà la possibilità a device esterni di interagire con i browser che supportano WebAuthn**.

MYNTECH
DRIVING TECHNOLOGY

myntech.it
hello@myntech.it

MILANO
Via Montenapoleone, 8 – 20121