Passkey

Le passkey sono una soluzione di sicurezza alternativa alle password basata sulla crittografia avanzata e la biometria. Questa nuova tecnologia offre un modo semplice e sicuro per accedere agli account online. Questo articolo ne descrive il funzionamento, i vantaggi e gli svantaggi, nonché le implicazioni per la sicurezza digitale.

I sistemi per crittografare e proteggere gli account utente si sono evoluti nel tempo, dalle password semplici a quelle complesse e fino all'autenticazione a due fattori. La tendenza osservata è stata quella di aumentare continuamente la sicurezza dell'utente nelle procedure di login, a costo però di maggiori complicazioni e passaggi richiesti. L'approccio più recente, quello delle passkey, mira a semplificare notevolmente il login e a incrementare ulteriormente i livelli di sicurezza. Le passkey vengono viste come una soluzione innovativa, tanto sicura quanto facile da usare.

Punti importanti:

- Se si usano le passkey non bisogna più ricordare e salvare le password.
- Il sistema non è attaccabile con il phishing (https://www.ebas.ch/it/phishing/) , perché ogni singola passkey è abbinata crittograficamente a un sito Internet o a un'app. Per quanto sofisticato possa essere un sito di phishing, non riceverà mai le informazioni necessarie per effettuare il login.
- La passkey è protetta attraverso un PIN o dati biometrici come l'impronta digitale o il riconoscimento facciale.
- Un elemento imprescindibile affinché anche le passkey salvate localmente siano sicure è la protezione di base del dispositivo con le nostre «5 operazioni per la vostra sicurezza digitale» (http://www.ebas.ch/5steps) .
- Una fuga di dati che comprende le credenziali salvate da un fornitore di servizi online non si ripercuote in alcun modo sull'accesso protetto tramite passkey.

Che cosa sono le passkey?

La passkey è un metodo per effettuare il login agli account utente che elimina la necessità di ricordare e inserire una password.

Una passkey è una chiave digitale composta da due elementi: una chiave pubblica e una segreta. La chiave segreta è memorizzata sul vostro dispositivo e protetta da PIN o dati biometrici come l'impronta digitale o il riconoscimento facciale.

Le passkey sono considerate sicure. Usano una crittografia robusta e dati biometrici difficili da falsificare. Anche se il vostro dispositivo viene rubato, nessuno può accedere alle vostre passkey senza disporre dei vostri dati biometrici o del PIN.

Le passkey non sono attaccabili con il phishing (https://www.ebas.ch/it/phishing/) , perché ogni singola passkey è abbinata crittograficamente a un sito Internet o a un'app. Inoltre, la chiave segreta rimane sempre sul dispositivo locale, p. es. uno smartphone o una chiavetta USB, senza uscirne mai.

Quando si effettua un login, la chiave pubblica rimane inutilizzabile senza l'autorizzazione fornita sul dispositivo locale. Questo procedimento rappresenta anche un vantaggio per quanto riguarda le eventuali fughe di dati (nel qual caso persone non autorizzate potrebbero impadronirsi delle credenziali valide per un sito Internet). Anche se una terza persona entrasse in possesso della chiave pubblica per l'accesso all'account utente, non potrebbe accedere a quell'account senza l'autorizzazione conferita sul dispositivo locale.

La tecnologia alla base del procedimento è stata sviluppata dalla FIDO Alliance, un'organizzazione di sicurezza IT non commerciale che si prefigge lo scopo di sviluppare sistemi di «identità rapida online» (**F**ast **ID**entity **O**nline).

Come funziona?

Quando effettuate l'accesso a un fornitore di servizi che offre l'identificazione tramite passkey, il sistema comunica con il vostro dispositivo locale inviandogli una richiesta (challenge). Voi dovete quindi identificarvi tramite PIN o biometria (riconoscimento facciale o impronta digitale). Il dispositivo risponde allora al sito Internet tramettendogli una firma digitale e confermando che siete proprio voi a voler effettuare l'accesso.

Il funzionamento delle passkey è relativamente semplice, anche se la tecnologia su cui si basa è avanzata. Ecco, in poche parole, la procedura per creare una passkey:

1. **Registrazione:** quando create un account su un sito Internet o un'app, sul dispositivo viene generata una passkey composta da una chiave pubblica e una segreta. La passkey è univoca ed è legata al sito o all'app in questione.
2. **Salvataggio:** la chiave segreta della passkey viene protetta in modo sicuro sul vostro dispositivo o nel sistema operativo con lo stesso metodo di autenticazione utilizzato per sbloccare il dispositivo, cioè p. es. tramite biometria (riconoscimento facciale o impronta digitale) o codice PIN. Su macOS e iOS le passkey vengono memorizzate nel portachiavi, su Windows si utilizza Windows Hello e su Android il gestore delle password di Google.
3. **Login:** la prossima volta che vorrete accedere a quel sito o a quell'app, il dispositivo utilizzerà la chiave segreta della passkey memorizzata localmente. Il sito Internet possiede soltanto la chiave pubblica. Basta confermare al sito la vostra identità tramite i vostri dati biometrici o il PIN, e il login sarà completo.

Vantaggi

- Non dovete più ricordare password complicate e nemmeno inserirle al momento del login. I vostri dati biometrici o un PIN sono sufficienti per effettuare l'accesso.
- Effettuare l'accesso con una passkey è molto più semplice e veloce che digitare una password o consultare un password manager.
- La passkey (chiave segreta) non viene mai inviata al sito, e ciò previene gli attacchi di phishing (https://www.ebas.ch/it/phishing/) .
- Poiché i siti Internet memorizzano solo la chiave pubblica e mai quella privata della passkey, l'accesso è protetto anche qualora il fornitore di servizi subisse una fuga di dati. La chiave pubblica della passkey può essere rinnovata con un impegno minimo.

Svantaggi

- L'abbinamento al dispositivo complica la condivisione della passkey. Se un servizio deve essere utilizzato contemporaneamente da due persone, resta utilizzabile solo da quella che può accedere al dispositivo con la passkey memorizzata.

- Le passkey vengono salvate sul dispositivo. Senza questo dispositivo non si può accedere alla passkey e quindi nemmeno al sito Internet o all'app.
- La gestione delle passkey è specifica per il sistema operativo, quindi le si possono impiegare facilmente su più dispositivi solo rimanendo all'interno dello stesso sistema (p.es. Microsoft, Apple) o della stessa famiglia di sistemi.
- In Linux l'uso delle passkey è molto limitato. Tuttavia, l'accesso funziona con soluzioni trasversali ai sistemi, come il codice QR.

Come si impostano e utilizzano le passkey?

Windows

Qui (https://learn.microsoft.com/it-it/windows/security/identity-protection/passkeys/?tabs=windows) trovate le istruzioni per creare e utilizzare le passkey su Windows.

macOS, iPhone/iPad

Apple sincronizza le passkey su tutti i dispositivi dell'utente tramite il portachiavi iCloud.

- Istruzioni per macOS (https://support.apple.com/it-it/guide/mac-help/mchl4af65d1a/mac)
- Istruzioni per iPhone/iPad (https://support.apple.com/it-it/guide/iphone/iphf538ea8d0/ios)

Android

Per utilizzare una passkey in Google è necessario attivare il blocco del display ed eventualmente il Bluetooth.

Qui (https://support.google.com/accounts/answer/13548313?sjid=10008299915686849826-EU&hl=it) trovate le istruzioni per creare e utilizzare le passkey con Google.

Utilizzo su sistemi differenti

Attualmente l'uso delle passkey su più sistemi diversi è possibile tramite codice QR o Bluetooth, attraverso i quali vengono trasmesse le autenticazioni effettuate.

Alcuni gestori di password supportano le passkey, rendendo in linea di principio possibile lo scambio tra diversi dispositivi. Tuttavia, il punto critico rimane il fatto che i fornitori gestiscono le passkey con i propri strumenti e le salvano nel proprio cloud.

In conclusione

Le passkey rendono l'accesso agli account utente più semplice e sicuro. Essendo supportate da sempre più fornitori di servizi, le passkey potrebbero rappresentare il futuro dell'autenticazione digitale. In termini di sicurezza tecnica, le passkey offrono un vantaggio riguardo alle fughe di dati e al phishing. Tuttavia, gli hacker potrebbero essere sempre più tentati di attaccare i dispositivi e le soluzioni cloud degli utenti per acquisire le chiavi segrete. Quindi dispositivi e account cloud devono essere sempre ben protetti e all'avanguardia in termini di sicurezza.

Una passkey permette di effettuare un login senza password. Il funzionamento si basa su una coppia di chiavi, una segreta e una pubblica. La chiave segreta rimane sempre su un dispositivo locale, p. es. uno smartphone o una chiavetta USB, senza uscirne mai. È il dispositivo a fungere da strumento di autenticazione. Quindi le passkey sono legate al dispositivo, non alla persona come le password.