

Come generare le chiavi VAPID con Python

Le chiavi VAPID (Voluntary Application Server Identification) sono utilizzate per autenticare i server che inviano notifiche push ai browser tramite il protocollo Web Push. Queste chiavi sono essenziali per garantire la sicurezza e l'affidabilità delle notifiche push. In questa guida, vedremo come generare chiavi VAPID utilizzando Python.

Prima di iniziare, assicurati di avere Python installato sul tuo sistema. Puoi scaricare Python dal sito ufficiale. Inoltre, avrai bisogno del pacchetto `py-vapid`, che fornisce gli strumenti necessari per generare e gestire le chiavi VAPID.

Per installare `py-vapid`, puoi utilizzare `pip`, il gestore di pacchetti di Python. Apri un terminale e esegui il seguente comando:

```
pip install py-vapid
```

Una volta installato il pacchetto, puoi utilizzare il seguente script Python per generare una coppia di chiavi VAPID (chiave pubblica e chiave privata).

```
from vapid import Vapid

# Genera una nuova coppia di chiavi VAPID
vapid_keys = Vapid().generate_keys()

# Estrai la chiave pubblica e privata
```

```
public_key = vapid_keys["public_key"]
private_key = vapid_keys["private_key"]

# Stampa le chiavi generate
print("Public Key: ", public_key)
print("Private Key: ", private_key)
```

Questo script genera una nuova coppia di chiavi VAPID e le stampa nel terminale. La chiave pubblica sarà utilizzata per identificare il server che invia le notifiche push, mentre la chiave privata sarà utilizzata per firmare i messaggi.

Una volta generate le chiavi, puoi utilizzarle per inviare notifiche push. Di seguito è riportato un esempio di come utilizzare le chiavi VAPID con la libreria pywebpush per inviare una notifica push.

Per installare pywebpush, esegui il seguente comando:

```
pip install pywebpush
```

Ecco un esempio di come inviare una notifica push utilizzando le chiavi VAPID generate:

```
from pywebpush import webpush, WebPushException

# Dati dell'abbonamento del client
subscription_info = {
    "endpoint":
    "https://fcm.googleapis.com/fcm/send/...",
    "keys": {
```

```

        "p256dh": "base64-encoded-key",
        "auth": "base64-encoded-auth-secret"
    }
}

# Carica le chiavi VAPID generate
vapid_private_key = "la_tua_chiave_privata"
vapid_claims = {
    "sub": "mailto:tuo_indirizzo_email@example.com"
}

# Contenuto del messaggio
message = {
    "title": "Titolo della Notifica",
    "body": "Corpo della notifica",
    "icon": "url_dell_icon"
}

# Invio della notifica push
try:
    response = webpush(
        subscription_info,
        message,
        vapid_private_key=vapid_private_key,
        vapid_claims=vapid_claims
    )
    print("Notifica inviata con successo!")
except WebPushException as ex:
    print("Errore durante l'invio della notifica: ",
    repr(ex))

```

In questo esempio, `subscription_info` contiene le informazioni di abbonamento del client, che dovrebbero essere ottenute durante la

registrazione del servizio di notifiche push nel browser. `vapid_private_key` e `vapid_claims` sono utilizzati per firmare il messaggio, garantendo che provenga da una fonte autenticata.

Conclusione

Generare chiavi VAPID con Python è un processo semplice grazie alla libreria `py-vapid`. Queste chiavi sono fondamentali per garantire la sicurezza delle notifiche push inviate ai browser. Con le chiavi generate, puoi utilizzare `pywebpush` per inviare notifiche push sicure e affidabili ai tuoi utenti.