Come generare le chiavi VAPID con C++

Le chiavi VAPID (Voluntary Application Server Identification for Web Push) sono utilizzate per autenticare i server che inviano notifiche push attraverso il protocollo Web Push. Generare queste chiavi può essere fatto in vari linguaggi di programmazione, incluso il C++. In questo articolo, vedremo come creare chiavi VAPID utilizzando C++ e la libreria OpenSSL.

Prima di iniziare, assicurati di avere:

- Un ambiente di sviluppo C++ (ad esempio, GCC o Clang)
- La libreria OpenSSL

Crea un nuovo progetto C++ e un file sorgente, ad esempio `vapid_keys.cpp`. Nel tuo file `vapid_keys.cpp`, includi le intestazioni necessarie di OpenSSL:

```
#include <openssl/ec.h>
#include <openssl/evp.h>
#include <openssl/pem.h>
#include <openssl/bio.h>
#include <openssl/buffer.h>
#include <iostream>
#include <memory>
```

Scrivi una funzione per generare le chiavi VAPID:

```
void generateVapidKeys() {
```

```
    // Creare una curva EC
    EC_KEY *eckey =
EC_KEY_new_by_curve_name(NID_X9_62_prime256v1);
    if (eckey == nullptr) {
        std::cerr << "Errore nella creazione della
chiave EC\n";
        return;
    }

    // Generare la chiave privata
    if (EC_KEY_generate_key(eckey) == 0) {
        std::cerr << "Errore nella generazione della
chiave EC\n";
        EC_KEY_free(eckey);
        return;
    }

    // Estrarre la chiave pubblica in formato PEM
    BIO *pub = BIO_new(BIO_s_mem());
    PEM_write_bio_EC_PUBKEY(pub, eckey);

    BUF_MEM *pubKeyMem;
    BIO_get_mem_ptr(pub, &pubKeyMem);

    std::string publicKey(pubKeyMem->data, pubKeyMem-
>length);
    BIO_free(pub);

    // Estrarre la chiave privata in formato PEM
    BIO *priv = BIO_new(BIO_s_mem());
    PEM_write_bio_ECPrivateKey(priv, eckey, nullptr,
nullptr, 0, nullptr, nullptr);

    BUF_MEM *privKeyMem;
```

```
    BIO_get_mem_ptr(priv, &privKeyMem);

    std::string privateKey(privKeyMem->data,
privKeyMem->length);
    BIO_free(priv);

    // Liberare la chiave EC
    EC_KEY_free(eckey);

    // Stampare le chiavi
    std::cout << "Chiave pubblica (PEM):\n" <<
publicKey << "\n";
    std::cout << "Chiave privata (PEM):\n" <<
privateKey << "\n";
}
```

Infine, aggiungi una funzione `main` per chiamare la funzione di generazione delle chiavi:

```
int main() {
    generateVapidKeys();
    return 0;
}
```

Compila il programma utilizzando il tuo compilatore C++ preferito. Ad esempio, con `g++`:

```
g++ -o vapid_keys vapid_keys.cpp -lssl -lcrypto
./vapid_keys
```

Dopo aver eseguito il programma, dovresti vedere le chiavi pubbliche e private stampate sullo schermo.

Conclusione

In questo articolo, abbiamo visto come generare chiavi VAPID utilizzando C++ e la libreria OpenSSL. Questo è un passaggio fondamentale per chiunque desideri implementare il supporto per le notifiche push nel proprio server web. Con le chiavi VAPID, il server può autenticarsi e inviare notifiche push in modo sicuro e affidabile.