

**Instrukcja korzystania
z usługi znakowania czasem
w programie OpenSSL z Time Stamp Patch**

Spis treści

Wstęp	1
Przykłady tworzenia żądań znacznika czasu	1
Przykłady wykorzystania klienta tsget	2
Przykłady weryfikacji znacznika czasu	2
Instalacja Time Stamp Patch	3
Korzystanie z OpenSSL pod MS Windows	3
Tworzenie pliku żądania znacznika czasu (funkcja skrótu md5)	3
Tworzenie pliku żądania znacznika czasu (funkcja skrótu sha1)	3
Tworzenie pliku żądania znacznika czasu (funkcja skrótu ripemd160)	4
Tworzenie żądań znacznika czasu za pomocą komendy ts	4
Korzystanie z klienta znacznika czasu tsget	5
Weryfikacja znaczników czasu za pomocą komendy ts	5

Wstęp

Time Stamp Patch dla OpenSSL umożliwia tworzenie żądań znakowania czasem, generowanie odpowiedzi i ich późniejszą weryfikację. Zainstalowanie łąty (patcha) dodaje do zestawu poleceń OpenSSL nową komendę - **ts**, która umożliwia wykonywanie operacji związanych ze znakowaniem czasem.

Program zyskuje ponadto funkcję prostego klienta, obsługiwanego z linii poleceń, służącego do tworzenia i wysyłania żądań znakowania czasem do Urzędu Znakowania Czasem. Klient ten korzysta z protokołów HTTP i HTTPS oraz pozwala otrzymywać i weryfikować odpowiedzi.

Źródła OpenSSL są dostępne na stronie www.openssl.org

Źródła Time Stamp Patch dla OpenSSL są do pobrania ze strony www.opentsa.org

Skompilowana wersja OpenSSL 0.9.6g dla MS Windows wraz z curl 7.10.3 (ssl) i Tee32 - pobierz opnssl.zip.

OpenSSL dostarczany jest w postaci źródeł umożliwiających kompilacje na platformach Unix, OpenVMS, Windows oraz MacOS. Time Stamp Patch for OpenSSL umożliwia korzystanie z usługi znakowania czasem na tych platformach.

Przykłady tworzenia żądań znacznika czasu

Stworzenie żądania dla pliku **test.txt** z wykorzystaniem funkcji skrótu **SHA-1** bez **nonce** oraz bez **certyfikatu urzędu TSA** dołączonego do odpowiedzi. Żądanie zostanie zapisane w pliku o nazwie **test.tsq**:

```
$openssl ts -query -data test.txt -no_nonce -out test.tsq
```

Stworzenie żądania na podstawie skrótu bez **nonce** oraz bez **certyfikatu urzędu TSA** dołączonego do odpowiedzi. Żądanie zostanie zapisane w pliku o nazwie **test.tsq**:

```
$openssl ts -query -digest ac0fd3f4e6c8b3837985aa09c5a4e6904dff712e -  
no_nonce -out test.tsq
```

Stworzenie żądania dla pliku **test.txt** z wykorzystaniem funkcji skrótu **MD5** bez **nonce** oraz z **certyfikatem urzędu TSA** dołączonym do odpowiedzi. Żądanie zostanie zapisane w pliku o nazwie **test.tsq**:

```
$openssl ts -query -data test.txt -no_nonce -cert -md5 -out test.tsq
```

Wyświetlenie żądania zapisanego w pliku **test.tsq**:

```
$openssl ts -query -in test.tsq -text
```

Przykłady wykorzystania klienta tsget

Uwaga: korzystanie z klienta tsget za pomocą protokołów HTTP i HTTPS wymaga obecności w systemie pakietów Perl, curl i curl-easy!

Wysłanie żądania znacznika czasu zapisanego w pliku test.tsq do TSA za pomocą protokołu HTTP i zapisanie znacznika czasu w pliku test.tsr:

```
$tsget -h http://time.sigmet.pl/tsa test.tsq
```

Wysłanie żądania znacznika czasu zapisanego w plikach test1.tsq i test2.tsq do TSA za pomocą protokołu HTTP i zapisanie znacznika czasu w plikach test1.tsr i test2.tsr:

```
$tsget -h http://time.sigmet.pl/tsa test1.tsq test2.tsq
```

Wysłanie żądania znacznika czasu zapisanego w pliku test.tsq do TSA za pomocą protokołu HTTPS i zapisanie znacznika czasu w pliku test.tsr. W katalogu cert znajdują się skróty certyfikatów urzędów CA:

```
$tsget -h https://time.sigmet.pl/tsa -P cert test.tsq
```

Przykłady weryfikacji znacznika czasu

Weryfikacja znacznika czasu z żądaniem znacznika czasu:

```
$openssl ts -verify -queryfile test.tsq -in test.tsr -CAfile cacert.pem -  
untrusted tsacert.pem
```

Weryfikacja znacznika czasu zawierającego certyfikat TSA z żądaniem znacznika czasu:

```
$openssl ts -verify -queryfile test.tsq -in test.tsr -CAfile cacert.pem
```

Weryfikacja znacznika czasu zawierającego certyfikat TSA z wykorzystaniem pliku użytego do stworzenia żądania:

```
$openssl ts -verify -data test.txt -in test.tsr -CAfile cacert.pem
```

Instalacja Time Stamp Patch

1. Pobierz źródła OpenSSL oraz odpowiadającą mu wersję Time Stamp Patch (adresy stron znajdziesz wyżej).

2. Rozpakuj źródła OpenSSL

```
#gzip -cd openssl-VERSION.tar.gz | tar xf -
```

3. Nałóż łatę (patch) na źródła OpenSSL

```
#cd openssl-wersja_openssl
```

```
#gzip -cd ../ts-wersja_openssl.patch.gz | patch -p1
```

4. Skonfiguruj i zbuduj OpenSSL

```
#!/config
```

```
#make
```

```
#make test
```

```
#make install
```

5. Sprawdź, czy w systemie jest nowa komenda ts

```
#!/openssl ts
```

Korzystanie z OpenSSL pod MS Windows

Ze względu na wykorzystywanie przez tsget pakietów Perl, curl i curl-easy w systemie Windows, można zastosować alternatywne rozwiązanie do wysyłania żądań czasu i odbioru znaczników czasu.

Rozwiązanie to wykorzystuje curl i tee, które zostały dołączone do archiwum openssl.zip.

Tworzenie pliku żądania znacznika czasu (funkcja skrótu md5)

Żądanie znacznika czasu zawiera: skrót obliczony za pomocą funkcji skrótu md5 oraz żądanie dołączenia certyfikatu urzędu do znacznika.

Żądanie zostaje stworzone na podstawie pliku test.txt i zapisane w pliku test.tsq.

Żądanie zostaje wysłane za pomocą protokołu HTTP do TSA. Otrzymana odpowiedź zostanie zapisana w pliku test.tsr.

```
C:\openssl\bin>openssl ts -query -data test.txt -md5 -cert|tee test.tsq /A  
|curl -s -S -H Content-Type:application/timestamp-query --data-binary @-  
http://time.signet.pl/tsa -o test.tsr
```

Tworzenie pliku żądania znacznika czasu (funkcja skrótu sha1)

Żądanie znacznika czasu zawiera: skrót obliczony za pomocą funkcji skrótu sha1 oraz żądanie dołączenia certyfikatu urzędu do znacznika.

Żądanie zostaje stworzone na podstawie pliku test.txt i zapisane w pliku test.tsq.

Żądanie zostaje wysłane za pomocą protokołu HTTPS do TSA a otrzymana odpowiedź zostanie zapisana w pliku test.tsr. Dodatkowo dokonywana jest weryfikacja certyfikatu SSL dla HTTPS

```
C:\openssl\bin>openssl ts -query -data test.txt -sha1 -cert|tee test.tsq /A  
|curl -s -S --capath hash -H Content-Type:application/timestamp-query --  
data-binary @- https://time.signet.pl/tsa -o test.tsr
```

Tworzenie pliku żądania znacznika czasu (funkcja skrótu ripemd160)

Żądanie znacznika czasu zawiera: skrót obliczony za pomocą funkcji skrótu ripemd160 oraz żądanie dołączenia certyfikatu urzędu do znacznika.

Żądanie zostaje stworzone na podstawie pliku test.txt i zapisane w pliku test.tsq.

Żądanie zostaje wysłane za pomocą protokołu HTTPS do TSA. Otrzymana odpowiedź zostanie zapisana w pliku test.tsr, bez weryfikacji certyfikatu SSL dla HTTPS.

```
C:\openssl\bin>openssl ts -query -data test.txt -ripemd160 -cert|tee  
test.tsq /A |curl -s -S -k -H Content-Type:application/timestamp-query --  
data-binary @- https://time.signet.pl/tsa -o test.tsr
```

Tworzenie żądań znacznika czasu za pomocą komendy ts

Składnia ts -query

```
openssl ts -query [-rand file:file...] [-config configfile] [-data  
file_to_hash] [-digest digest_bytes] [-md2|-md4|-md5|-sha|-sha1|-mdc2|-  
ripemd160] [-policy object_id] [-no_nonce] [-cert] [-in request.tsq] [-out  
request.tsq] [-text]
```

[-rand file:file]

wskazanie na plik zawierający losowe dane będące podstawą dla generatora liczb losowych

[-config configfile]

plik konfiguracyjny dla środowiska OpenSSL

[-data file_to_hash]

plik, którego skrót zostanie wykorzystany do stworzenia żądania o znacznik czasu

[-digest digest_bytes]

skrót, który zostanie wykorzystany do stworzenia żądania o znacznik czasu

-md2|-md4|-md5|-sha|-sha1|-mdc2|-ripemd160

dostępne funkcje skrótu służące do wyliczenia wartości skrótu (domyślnie SHA-1)

[-policy object_id]

wskazanie na identyfikator polityki, na podstawie której TSA wystawi znacznik czasu

[-no_nonce]

rezygnacja z losowej 64 bitowej liczby losowej dołączanej do wniosku o znacznik czasu

[-cert]

żądanie dołączenia do stempla czasu certyfikatu urzędu TSA

[-in request.tsq]

wskazanie pliku zawierającego żądanie znacznika czasu, stosowane w celu wyświetlenia zawartości żądania

[-out request.tsq]

wskazanie pliku, w którym zostanie zapisane żądanie znacznika czasu

[-text]

wyświetlenie żądania o znacznik czasu w czytelnej formie

Korzystanie z klienta znacznika czasu tsget

Składnia tsget

```
tsget -h server_url [-e extension] [-o output] [-v] [-d] [-k  
private_key.pem] [-p key_password] [-c client_cert.pem] [-C CA_certs.pem]  
[-P CA_path] [-r file:file...] [-g EGD_socket] [request]
```

[-h server_url]

adres serwera **HTTP** lub **HTTPS** oczekującego na żądania znacznika czasu

[-e extension]

rozszerzenie nadawane plikom zawierającym znaczniki czasu, domyślnie jest to .tsr

[-o output]

nazwa pliku, pod którą zostanie zapisany pojedynczy znacznik czasu

[-P CA_path]

wskazanie na katalog zawierający skróty certyfikatów urzędów CA - opcja wykorzystywana jedynie przy wykorzystaniu protokołu **HTTPS**

[request]

wskazanie na plik zawierający żądanie znacznika czasu zgodne z **RFC 3161**

Weryfikacja znaczników czasu za pomocą komendy ts

Składnia ts -verify

```
openssl ts -verify [-data file_to_hash] [-digest digest_bytes] [-queryfile  
request.tsq] [-in response.tsr] [-token_in] [-CApath trusted_cert_path] [-  
CAfile trusted_certs.pem] [-untrusted cert_file.pem]
```

[-data file_to_hash]

wskazanie na plik na podstawie, którego został obliczony skrót umieszczony w żądaniu znacznika czasem

[-digest digest_bytes]

skrót wykorzystany do stworzenia żądania znacznika czasu

[-queryfile request.tsq]

wskazanie na plik zawierający żądanie o znacznik czasu (stosowane gdy nie podajemy pliku lub skrótu)

[-in response.tsr]

wskazanie na plik zawierający znacznik czasu zapisany jako TimeStampResp

[-token_in]

opcja używana jeżeli plik zawierający znacznik czasu zapisany jako TimeStamp Token

[-CApath trusted_cert_path]

wskazanie na katalog zawierający skróty certyfikatów urzędów CA