

SSL / TLS

Położenie: (nie dotyczy)

© 3bird.net 2005, <http://3bird.net>

Wiadomości ogólne

Aby możliwe było zastosowanie SSL, serwer, na którym jest Apache, musi mieć stały numer IP (także w przypadku wykupienia usługi hostingowej ze *cPanel*, potrzebne jest wykupienie stałego numeru IP). Możliwe wtedy staje się zastosowanie tzw. *self-signed certificates* (certyfikat bezpłatny). Można także wykupić certyfikację w profesjonalnej firmie.

SSL (*Secure Socket Layer*) - powstał w 1994 w *Netscape*. Rok później wychodzi SSLv3. Protokół SSLv2 ma duże wady, gdyż można na nim wymusić stosowanie obniżonego szyfrowania (np. 40-bitowego). Należy więc wyłączyć w przeglądarce protokół SSLv2. Komunikacja SMTP poprzez SSL przebiega na porcie 465, a komunikacja HTTPS na porcie 443.

TLS (*Transport Layer Security*) - powstaje w 1999 roku (zdefiniowany w RFC 2246) i jest zaakceptowany przez *Netscape* i *Microsoft*. Jest równoważny SSL3. Można skorzystać z tego na serwerze Postfix pod warunkiem zainstalowania OpenSSL. Komunikacja SMTP za pomocą TLS przebiega po portach 25. Aby upewnić się, że komunikacja odbywa się po TLS, należy:

telnet nazwaSerweraPocztowego 25

ehlo nazwaSerweraPocztowego (powinien pojawić się napis STARTTLS).

Aby zobaczyć jakie są jeszcze inne porty otwarte na serwerze:

nmap nazwaSerwera

RSA (*Rivest-Shamir-Adleman*) - asymetryczny system kryptograficzny opracowany w 1977 chroniony patentem przez *RSA Security*.

DES (*Data Encryption Standard*) - algorytm szyfrowania opracowany przez *IBM* i uznany w 1977 za oficjalny standard w USA. W 1997 został złamany po 90 dniach starań (14000 komputerów). Zastąpiono więc ten algorytm Triple-DES (potrójny DES).

MD5 (*Message Digest Algorithm*) - opisany w RFC1321, 128-bitowy. Do tej pory niezłamany.

SHA (*Secure Hash Algorithm*) - opracowany w 1993 roku przez *National Institute of Standards and Technology*, 160-bitowy.

SASL (*Simple Authentication and Security Layer*) - znany także pod nazwą SMTP AUTH, zdefiniowany w RFC 2222, zabezpiecz tylko uwierzytelnianie, nie szyfruje przesyłanych wiadomości. Polega na tym, że przy wysyłaniu poczty podaje się hasło.

Opis sesji

<i>Klient</i>	<i>Serwer</i>
<i>Hello Serwer! Możemy porozmawiać używając:</i>	<i>Słyszę cię. Porozmawiajmy używając:</i>
<u>Wersja</u> : TLSv1; jeśli go nie znasz to SSLv3.	<u>Wersja</u> : TLSv1.
<u>Wymiana klucza</u> : RSA; jeśli go nie znasz to Diffie-Hellman.	<u>Wymiana klucza</u> : RSA.
<u>Metoda szyfrowania tajnego klucza</u> : Potrójny DES; jeśli nie to DES.	<u>Metoda szyfrowania tajnego klucza</u> : DES.
<u>Hash (skrót wiadomości)</u> : SHA-1; jeśli go nie znasz to MD5.	<u>Hash (skrót wiadomości)</u> : SHA-1.
<u>Metoda kompresji danych</u> : PKZIP; jeśli nie, to gzip.	<u>Metoda kompresji danych</u> : PKZIP.
<u>Losowy numer</u> : 196201083.	<u>Losowy numer</u> : 823455127.

Po udzieleniu odpowiedzi klientowi na *Hello*, serwer wysła swój certyfikat. Certyfikat serwera podpisany jest przez zaufany ośrodek jakim może być urząd ds. certyfikatów, czyli CA (*Certification Authority*). Klient weryfikuje certyfikat serwera za pomocą klucza publicznego udostępnionego przez CA. Następnie serwer może zarządać certyfikatu od klienta (choć nie jest to konieczne). Nawet jeśli to zrobi, klient nie musi go wysłać (po pierwsze dlatego, że nie ma komercyjnego certyfikatu; po drugie, i tak będzie weryfikowany np. za pomocą karty kredytowej). Przesyłane wiadomości i tak są szyfrowane.

Ostatnia aktualizacja: 5 czerwiec 2006.