

## BEZPIECZEŃSTWO NOBLE FUNDS ONLINE

### Szyfrowanie

Dla zapewnienia jak najwyższego poziomu bezpieczeństwa w trakcie korzystania z serwisu transakcyjnego Noble Funds Online, do zabezpieczenia połączenia Klienta z Serwisem wykorzystuje protokół szyfrujący Transport Layer Security (TLS). Protokół TLS zapewnia poufność informacji i gwarantuje, że nikt postronny nie może odczytać lub zmienić danych przesyłanych między Klientem a Serwisem.

W trakcie połączenia z serwisem transakcyjnym wykorzystywane są następujące techniki kryptograficzne:

1. algorytm asymetryczny (z kluczem prywatnym i publicznym serwera Towarzystwa), używany w trakcie inicjowania połączenia, do zabezpieczenia transmisji (przekazania) losowo wygenerowanego klucza sesyjnego (wykorzystywanego następnie w algorytmie symetrycznym);
2. algorytm symetryczny, używany do zabezpieczenia całej sesji komunikacyjnej między przeglądarką klienta a serwerem WWW Towarzystwa;
3. funkcja skrótu używana do generowania podpisów cyfrowych dla przesyłanej informacji, które zapewniają integralność przesyłanej informacji - każda próba zmiany danych w czasie transmisji zostanie natychmiast wykryta.

Zastosowane przez serwis internetowy Towarzystwa metody kryptograficzne uznane są przez specjalistów za bezpieczne i zapewniające pełną poufność operacji finansowych.

### Certyfikaty

Pierwszym krokiem przy nawiązywaniu połączenia przez przeglądarkę klienta z serwerem serwisu internetowego jest pobranie tzw. certyfikatu.

Certyfikat to rodzaj dokumentu tożsamości dla serwera WWW, wydany przez niezależną firmę tzw. Certification Authority (CA).

Certyfikat zawiera m.in.:

- 1) nazwę właściciela certyfikatu,
- 2) nazwę wydawcy certyfikatu,

- 3) publiczny klucz właściciela,
- 4) okres ważności,
- 5) nazwę serwera, dla którego certyfikat jest wystawiany.

Certyfikat dla Noble Funds Online wystawiła znana amerykańska firma certyfikująca - Comodo Secure. Wydanie certyfikatu zostało poprzedzone drobiazgowym sprawdzeniem autentyczności serwisu internetowego oraz weryfikacją praw do domeny internetowej, w której działają serwery Towarzystwa.