Długość komunikatu – liczba całkowita z znakiem w konwencji Big Endian. Oznacza długość wiadomości w bajtach (cała wiadomość ma 4 + długość komunikatu)

Definicja komunikatów:

HELLO

Komunikat powitalny od serwera do klienta.

|  |  |
| --- | --- |
| Długość ( zawsze 1) | HELLO |

REQUEST\_PROTOCOL,

Komunikat informujący o wersji protokołu żądanej przez klienta

|  |  |  |
| --- | --- | --- |
| Długość | REQUEST\_PROTOCOL | Nazwa (string) |

NACK,

Komunikat odrzucający żądanie.

|  |  |
| --- | --- |
| Długość ( zawsze 1) | NACK |

Jeśli przesyłany po zestawieniu kryptografii to:

|  |  |
| --- | --- |
| Długość | Zaszyfrowane |

ACK,

Komunikat akceptujący żądanie.

|  |  |
| --- | --- |
| Długość ( zawsze 1) | ACK |

Jeśli przesyłany po zestawieniu kryptografii to:

|  |  |
| --- | --- |
| Długość | Zaszyfrowane |

CLIENT\_ID,

Komunikat podający identyfikator klienta.

|  |  |  |
| --- | --- | --- |
| Długość | Komunikat zaszyfrowany z użyciem klucza publicznego serwera | |
|  | CLIENT\_ID | Identyfikator(string) |

CHOOSE\_ALGORITHM,

Komunikat od serwera do klienta, potwierdający odebranie komunikatu o identyfikatorze i potwierdzający jego poprawność.

|  |  |  |
| --- | --- | --- |
| Długość | Komunikat zaszyfrowany kluczem prywatnym serwera | |
|  | CHOOSE\_ALGORITHM | Skrót Identyfikatora klienta |

CHOOSEN\_ALGORITHM,

|  |  |  |
| --- | --- | --- |
| Długość | Komunikat zaszyfrowany kluczem publicznym serwera | |
|  | CHOOSEN\_ALGORITHM | Algorytm (string) |

ESTABLISH\_ENCRYPTION,

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Długość | Komunikat zaszyfrowany kluczem publicznym serwera | | | |
|  | Długość hasha | ESTABLISH\_ENCRYPTION | Klucz symetryczny | hash |

CHOOSE\_AUTH\_MODULE,

|  |  |  |  |
| --- | --- | --- | --- |
| Długość | Komunikat zaszyfrowany kluczem symetrycznym | | |
|  | Długość hasha | CHOOSE\_AUTH\_MODULE | hash |

CHOOSEN\_AUTH\_MODULE,

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Długość | Komunikat zaszyfrowany kluczem symetrycznym | | | |
|  | Długość hasha | CHOOSEN\_AUTH\_MODULE | AuthModule(string) | hash |

AUTH\_DATA,

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Długość | Komunikat zaszyfrowany kluczem symetrycznym | | | |
|  | Długość hasha | AUTH\_DATA | Dane autoryzacyjne (cokolwiek, zależnie od modułu) | hash |

WAITING\_FOR\_LOGS,

|  |  |  |  |
| --- | --- | --- | --- |
| Długość | Komunikat zaszyfrowany kluczem symetrycznym | | |
|  | Długość hasha | WAITING\_FOR\_LOGS | hash |

LOGS\_PORTION

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Długość | Komunikat zaszyfrowany kluczem symetrycznym | | | |
|  | Długość hasha | LOGS\_PORTION | LOG\nLOG\n… | hash |

END

|  |  |  |  |
| --- | --- | --- | --- |
| Długość | Komunikat zaszyfrowany kluczem symetrycznym | | |
|  | Długość hasha | END | hash |

Skrócony opis kryptografii:

Założenia:

Klient posiada klucz publiczny serwera.

Klient posiada swoje ID (nie jest to informacja wrażliwa)

1. Klient wysyła do Serwera swoje ID zaszyfrowane kluczem publicznym
2. Serwer wyszukuje ID i sprawdza dostępne dla niego algorytmy. Następnie wylicza skrót ID klienta i wysyła do klienta zaszyfrowane swoim kluczem prywatnym.
3. Klient sprawdza poprawność skrótu i wysyła do serwera nazwe wybranego algorytmu
4. Serwer akceptuje algorytm
5. Klient wysyła do serwera zaszyfrowany kluczem publicznym klucz symetryczny

- - - - - - - - Połączenie szyfrowane kluczem symetrycznym - - - - - - - -

1. Serwer akceptuje nowy klucz i wysyła żądanie wyboru metody uwierzytelnienia klienta
2. Klient wybiera metodę i wysyła ją.
3. Serwer akceptuje metoda i uruchamia proces uwierzytelnienia i oczekuje na rezultat
4. Przy pozytywnym uwierzytelnieniu serwer wysyła żadanie podania logów, a klient je odsyła w porcjach zależnych od jego ustawień