



Meeeeeeeeeeeeeeeeeh

Протоколы SSL и TLS

Версия	Дата публикации	Актуальность
SSL 1.0	не публиковался	не публиковался
SSL 2.0	1995	Признан устаревшим в 2011 году
SSL 3.0	1996	Признан устаревшим в 2015 году
TLS 1.0	1999	Признан устаревшим в 2020 году
TLS 1.1	2006	Признан устаревшим в 2020 году
TLS 1.2	2008	
TLS 1.3	2018	

Handshake TLS 1.2

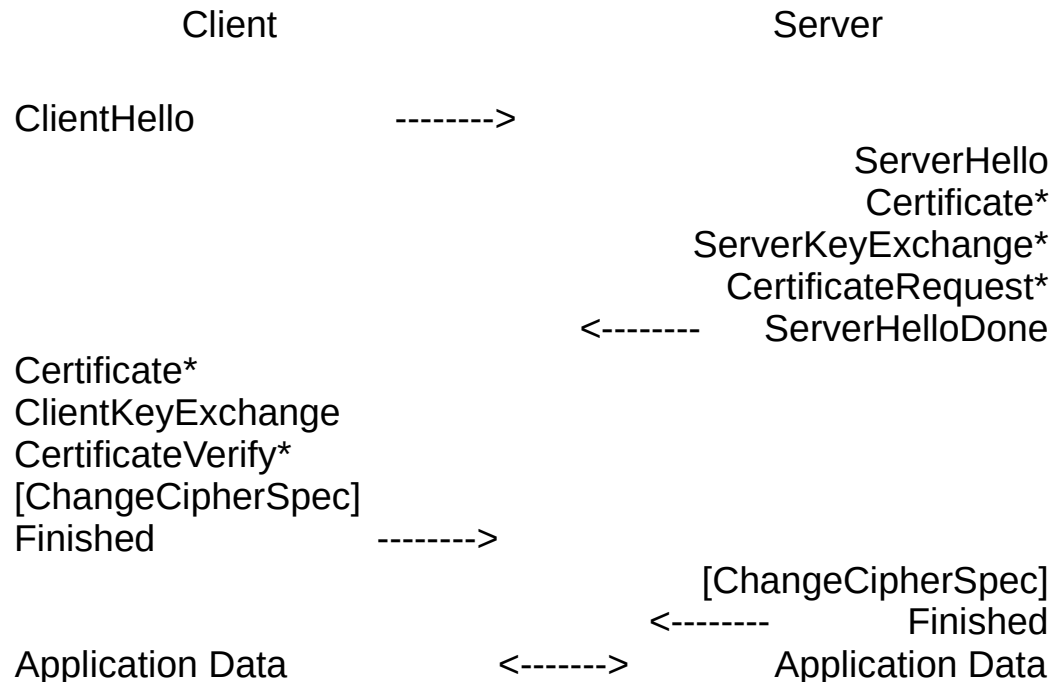
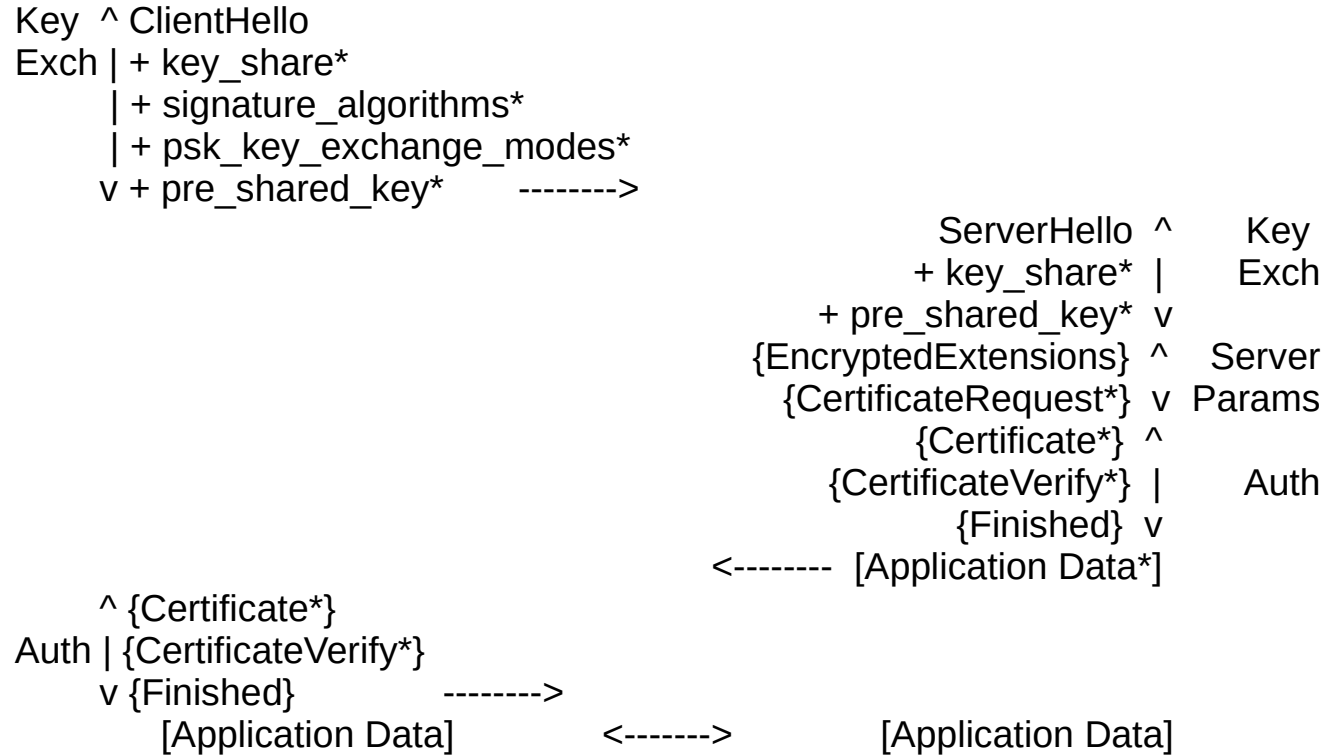


Схема обмена Handshake-сообщениями TLS 1.2
(ChangeCipherSpec - не является сообщением Handshake).
Источник: RFC 5246

Handshake TLS 1.3

Client

Server



Установление соединения по полной схеме TLS 1.3

Источник: RFC 8446

