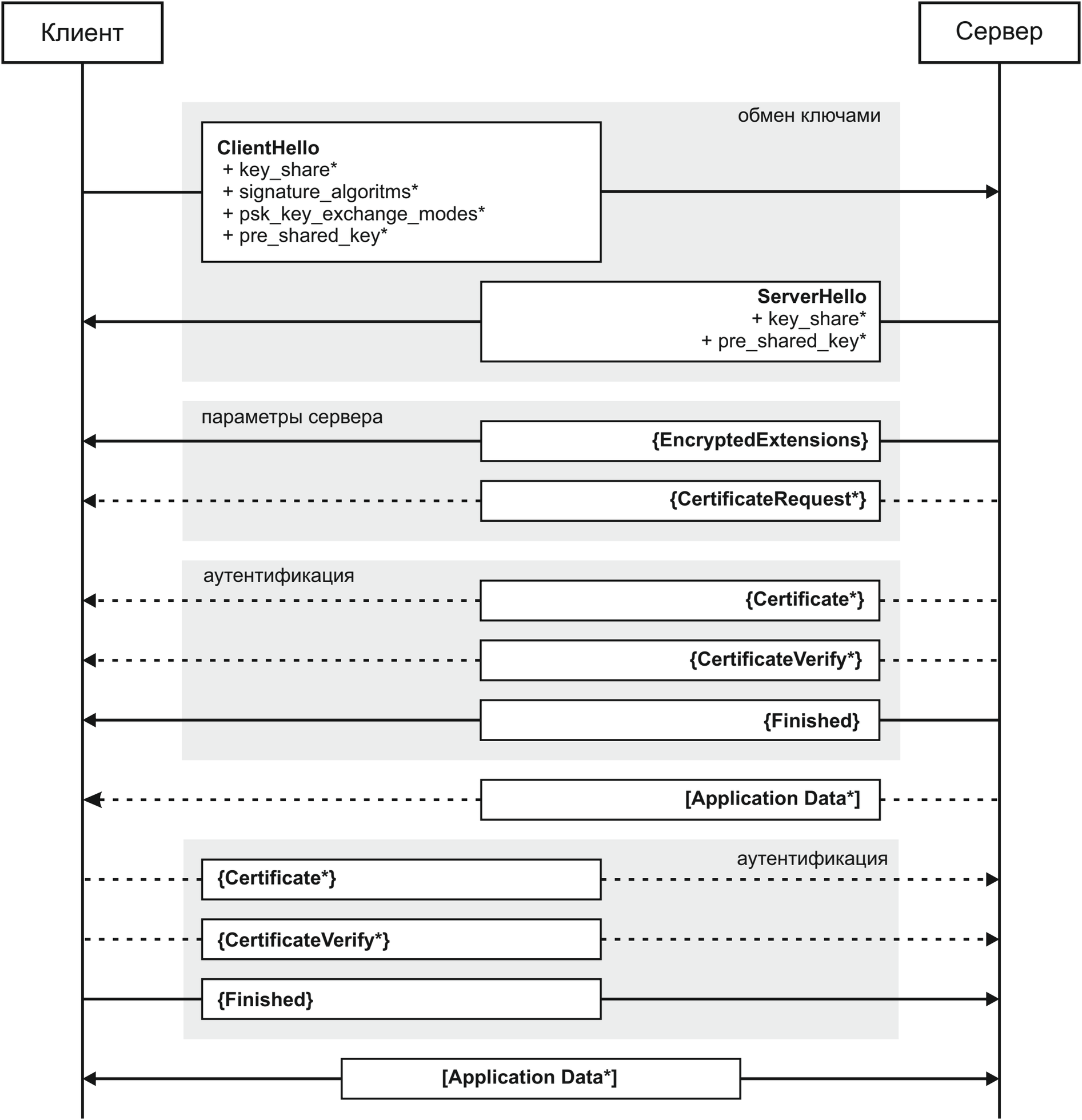
Клиент
Сервер
обмен ключами
ClientHello
+ key_share*
+ signature_algoritms*
+ psk_key_exchange_modes*
+ pre_shared_key*
ServerHello
+ key_share*
+ pre_shared_key*
параметры сервера
{EncryptedExtensions}
{CertificateRequest*}
аутентификация
{Certificate*}
{CertificateVerify*}
{Finished}
[Application Data*]
аутентификация
{Certificate*}
{CertificateVerify*}
{Finished}
[Application Data*]