Client
$$C$$

Server S
 $(sk_S, pk_S, cert_S)$

$$\begin{array}{c}
r_C \stackrel{\$}{\leftarrow} \{0, 1\}^{256} \\
CH \leftarrow \\
(r_C, enc, hash, certreq, keyex)
\end{array}$$
 CH

$$\begin{array}{c}
r_S \stackrel{\$}{\leftarrow} \{0, 1\}^{256} \\
SH \leftarrow \\
(r_S, enc, hash, cert_S, keyex)
\end{array}$$

$$\begin{array}{c}
sh \leftarrow \\
r_S \stackrel{\$}{\leftarrow} \{0, 1\}^{256} \\
SH \leftarrow \\
(r_S, enc, hash, cert_S, keyex)
\end{array}$$

$$\begin{array}{c}
c \leftarrow \mathsf{PK}.\mathsf{Enc}_{pk_S}(mk) \\
(k_{enc}^C, k_{end}^S, k_{mac}^C, k_{mac}^S) \leftarrow \\
\mathsf{KDF}(label, mk, r_C, r_S, cert_S) \\
mac_C \leftarrow \\
\mathsf{H}(k_{mac}^C | \mathsf{H}(\mathsf{cvp}|CH|SH) \\
CMK \leftarrow (c, mac_C)
\end{array}$$

$$\begin{array}{c}
CMK
\end{array}$$

$$\begin{array}{c}
mk \leftarrow \mathsf{PK}.\mathsf{Dec}_{sk_S}(c) \\
(k_{enc}^C, k_{end}^S, k_{mac}^C, k_{mac}^S) \leftarrow \\
\mathsf{KDF}(label, mk, r_C, r_S, cert_S) \\
\mathsf{SID} \stackrel{\$}{\leftarrow} \{0, 1\}^{256} \\
\mathsf{SH} \leftarrow \\
\mathsf{KDF}(label, mk, r_C, r_S, cert_S)
\end{array}$$

$$\begin{array}{c}
sh \leftarrow \mathsf{PK}.\mathsf{Dec}_{sk_S}(c) \\
(k_{enc}^C, k_{end}^S, k_{mac}^C, k_{mac}^S) \leftarrow \\
\mathsf{KDF}(label, mk, r_C, r_S, cert_S)
\end{array}$$

$$\begin{array}{c}
\mathsf{SID} \stackrel{\$}{\leftarrow} \{0, 1\}^{256} \\
\mathsf{SH} \leftarrow \\
\mathsf{KDF}(label, mk, r_C, r_S, cert_S)
\end{array}$$

$$\begin{array}{c}
\mathsf{SID} \stackrel{\$}{\leftarrow} \{0, 1\}^{8\cdot32} \\
\mathsf{Mac}_S \leftarrow \\
\mathsf{H}(k_{mac}^S | \mathsf{H}(\mathsf{Sr}|r_C|r_S|SID) \\
\mathsf{SV} \leftarrow (SID, mac_S)
\end{array}$$