$$
\begin{aligned}
P \quad &\triangleq \quad \nu\, sk_{\mathcal{S}}.\nu\, sk_{\mathcal{C}}.\nu\, s. \\
&\quad \text{let } pk_S = \mathsf{pk}(sk_{\mathcal{S}}) \text{ in let } pk_C = \mathsf{pk}(sk_{\mathcal{C}}) \text{ in} \\
&\quad (\overline{c}\langle pk_S\rangle \mid \overline{c}\langle pk_C\rangle \mid !P_{\mathcal{S}} \mid !P_{\mathcal{C}})
\end{aligned}
$$

$$
\begin{aligned}
P_{\mathcal{S}} \quad &\triangleq \quad c(x\_pk).\nu\, k.\overline{c}\langle \mathsf{aenc}(x\_pk, \mathsf{sign}(sk_{\mathcal{S}}, k))\rangle. \\
&\quad c(z).\text{if } \mathsf{fst}(\mathsf{sdec}(k, z)) = tag \text{ then } Q
\end{aligned}
$$

$$
\begin{aligned}
P_{\mathcal{C}} \quad &\triangleq \quad c(y).\text{let } y' = \mathsf{adec}(sk_{\mathcal{C}}, y) \text{ in let } y\_k = \mathsf{getmsg}(y') \text{ in} \\
&\quad \text{if } \mathsf{checksign}(pk_S, y') = \mathsf{true} \text{ then} \\
&\quad \overline{c}\langle \mathsf{senc}(y\_k, \mathsf{pair}(tag, s))\rangle
\end{aligned}
$$