	Signature	**PKE**	**Revised PKE**	**Pre-Shared Key**
$data_I$	n_I, ID_I	$\mathsf{Enc}(pk_R, n_I)$, $\mathsf{Enc}(pk_R, ID_I)$	$\mathsf{Enc}(pk_R, n_I)$, $ke_I := \mathsf{PRF}_{n_I}(\mathsf{cky_I})$, $\mathsf{Enc}(ke_I; ID_I)$	n_I, ID_I
$data_R$	n_R, ID_R	$\mathsf{Enc}(pk_I, n_R)$, $\mathsf{Enc}(pk_I, ID_R)$	$\mathsf{Enc}(pk_R, n_I)$, $ke_R := \mathsf{PRF}_{n_R}(\mathsf{cky_R})$ $\mathsf{Enc}(ke_R; ID_R)$	n_R, ID_R
sig_I	$cert_R, \sigma_I$	prf_I	prf_I	prf_I
sig_R	$cert_R, \sigma_R$	prf_R	prf_R	prf_R