	Device		**Server**
Enroll.($1\times$)	$\mathbf{s} \leftarrow \text{POK}$	$\xrightarrow{\mathbf{s}}$	$\mathbf{h} \leftarrow \text{FE.Gen}(\mathbf{s})$ $\mathbf{e} \leftarrow \bar{\Psi}_\alpha$ $\text{DB} \leftarrow (\mathbf{s}, \mathbf{h}, \mathbf{e})$
CRP Generate.($N\times$)			$\mathbf{r} \leftarrow \text{TRNG}()$ $\text{seed}_{\mathbf{a}'} \leftarrow \text{TRNG}()$ $\mathbf{X} \leftarrow \text{TRNG}()$ $\mathbf{b}' \leftarrow \text{LFSR}(\text{seed}_{\mathbf{a}'})^T\mathbf{s} + \mathbf{X}^T\mathbf{e} + \mathbf{r}\lfloor q/2 \rfloor$ $ch \leftarrow (\text{seed}_{\mathbf{a}'}, \mathbf{b}')$ $\text{DB} \leftarrow (ch, \mathbf{r})$
Authenticate.(∞)	$\mathbf{s}_R \leftarrow \text{POK}$	$\xleftarrow{\mathbf{h}, ch}$	$\mathbf{h}, ch, \mathbf{r} \leftarrow \text{DB}$
	$\mathbf{s} \leftarrow \text{FE.Rec}(\mathbf{s_R}, \mathbf{h})$		
	$\mathbf{r}_R \leftarrow \text{PUF}(ch, \mathbf{s})$	$\xrightarrow{\mathbf{r}_R}$	accept if $\text{HD}(\mathbf{r}_R, \mathbf{r}) < th$