	Device	**Server**

$$\mathbf{s} \leftarrow \text{POK} \quad \xrightarrow{\quad \mathbf{s} \quad} \quad \mathbf{h} \leftarrow \text{FE.Gen}(\mathbf{s})$$

$$\mathbf{e} \leftarrow \bar{\Psi}_{\alpha}$$

$$\text{DB} \leftarrow (\mathbf{s}, \mathbf{h}, \mathbf{e})$$

$$\mathbf{r} \leftarrow \text{TRNG}()$$

$$\text{seed}_{\mathbf{a}'} \leftarrow \text{TRNG}()$$

$$\mathbf{X} \leftarrow \text{TRNG}()$$

$$\mathbf{b}' \leftarrow \text{LFSR}(\text{seed}_{\mathbf{a}'})^T \mathbf{s} + \mathbf{X}^T \mathbf{e} + \mathbf{r} \lfloor q/2 \rfloor$$

$$\mathbf{c}' \leftarrow (\text{seed}_{\mathbf{a}'}, \mathbf{b}')$$

$$\text{DB} \leftarrow (\mathbf{c}', \mathbf{r})$$

$$\tilde{\mathbf{s}} \leftarrow \text{POK} \quad \xleftarrow{\quad \mathbf{h}, \mathbf{c}' \quad} \quad \mathbf{h}, \mathbf{c}', \mathbf{r} \leftarrow \text{DB}$$

$$\mathbf{s} \leftarrow \text{FE.Rec}(\tilde{\mathbf{s}}, \mathbf{h})$$

$$\tilde{\mathbf{r}} \leftarrow \text{PUF}(\mathbf{c}', \mathbf{s}) \quad \xrightarrow{\quad \tilde{\mathbf{r}} \quad} \quad \text{accept if } \text{HD}(\tilde{\mathbf{r}}, \mathbf{r}) < th$$

Enroll.$(1\times)$

CRP Genarate.$(d\times)$

Authenticate.$(d\times)$