

FIDO UAF

Registration

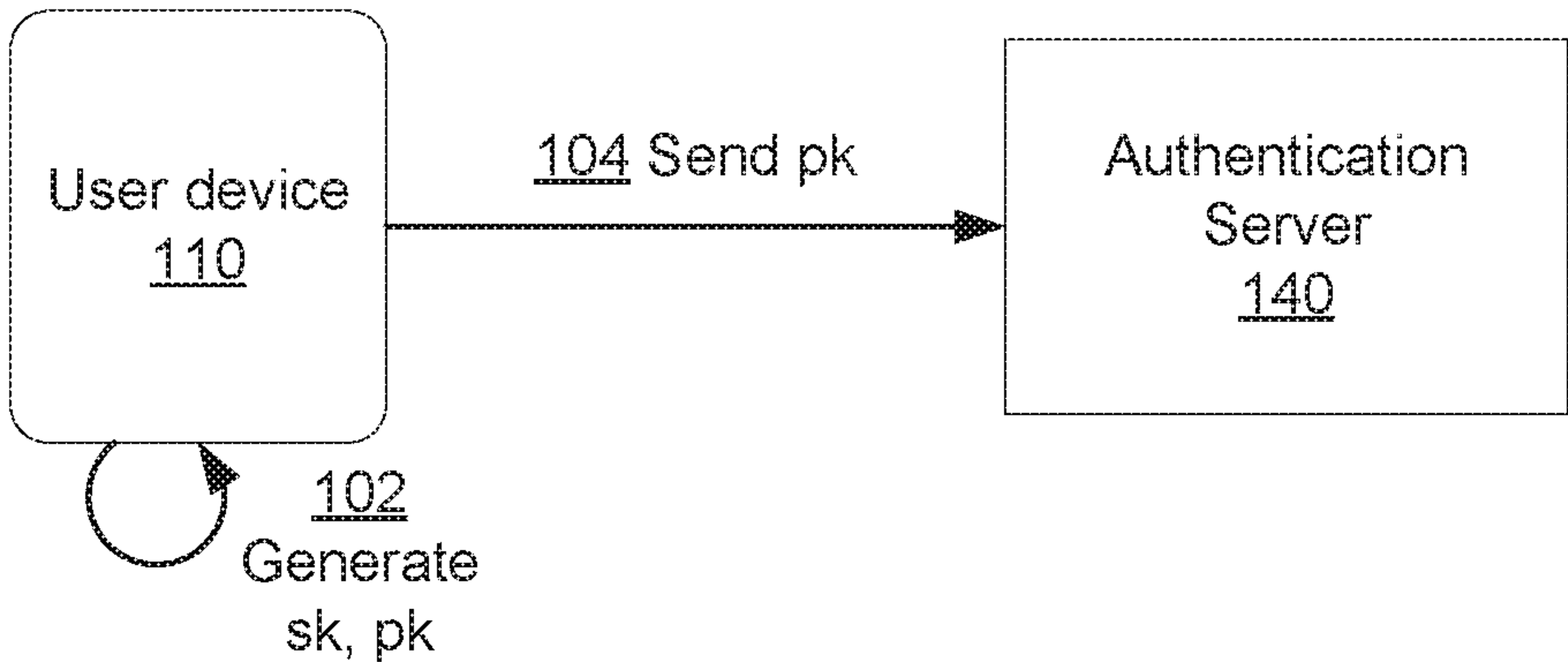


FIG. 1A

Authentication

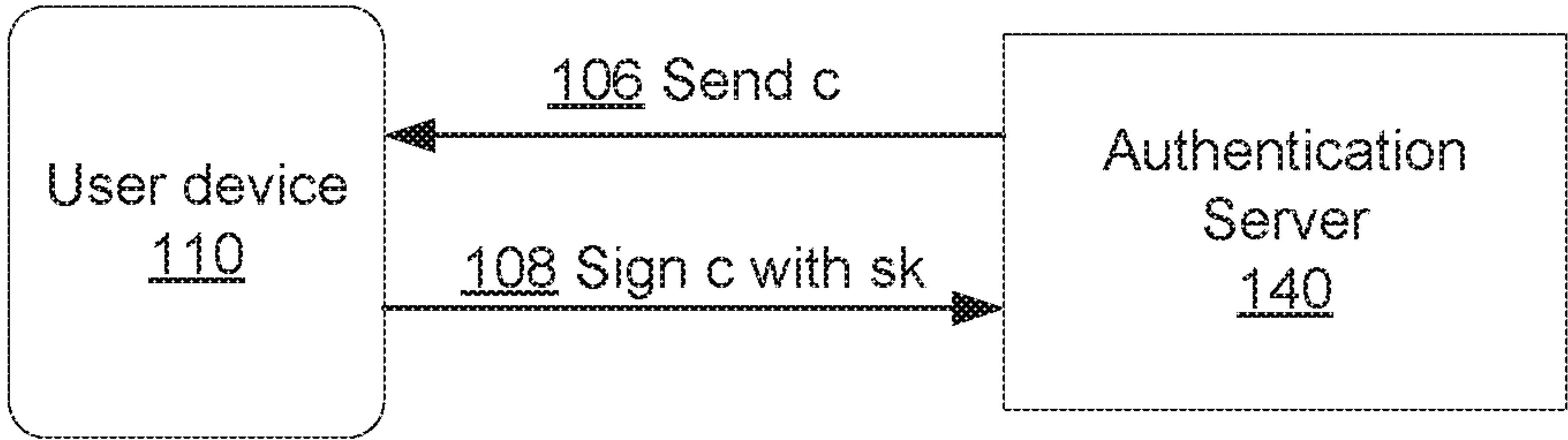


FIG. 1B

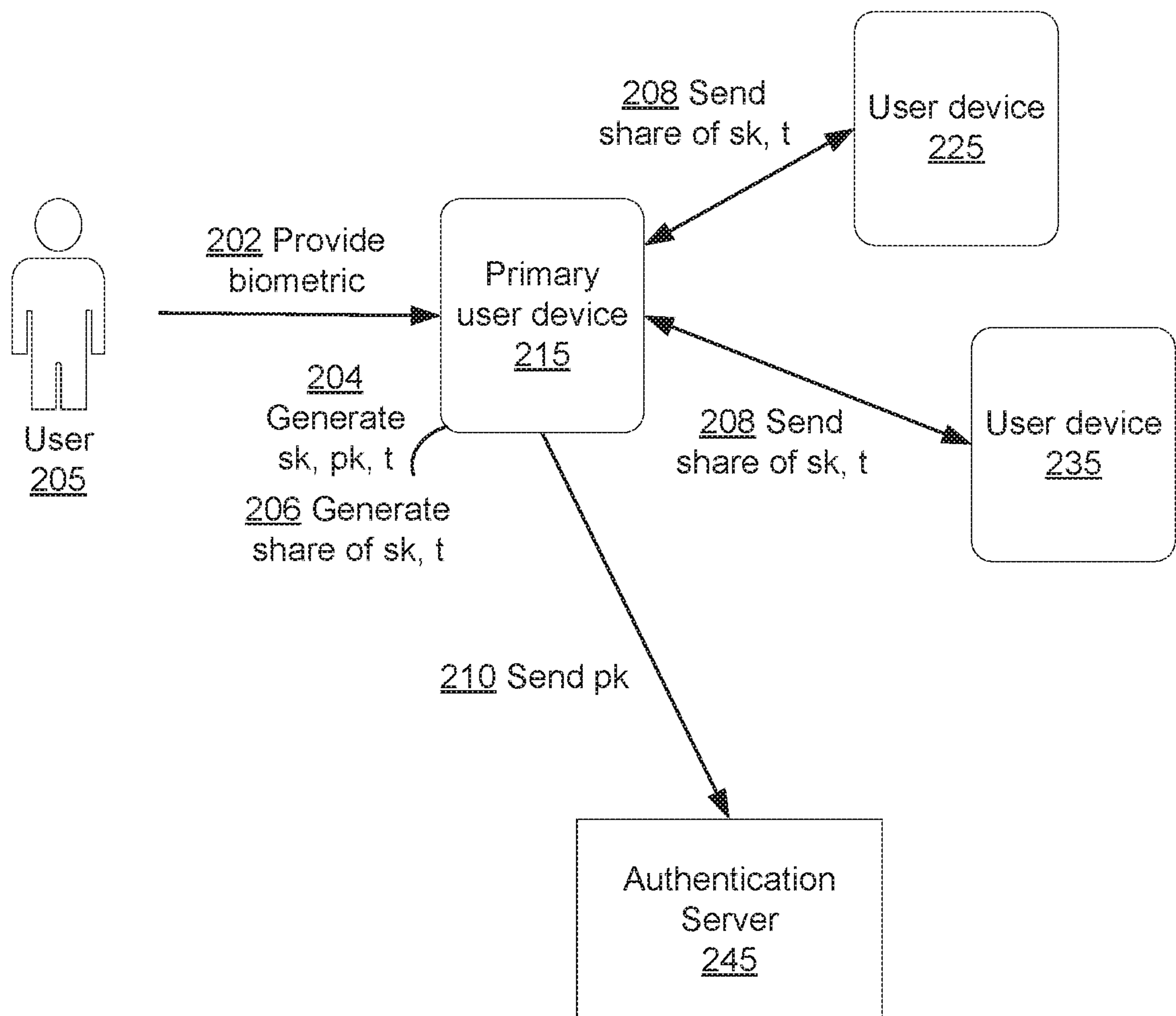


FIG. 2

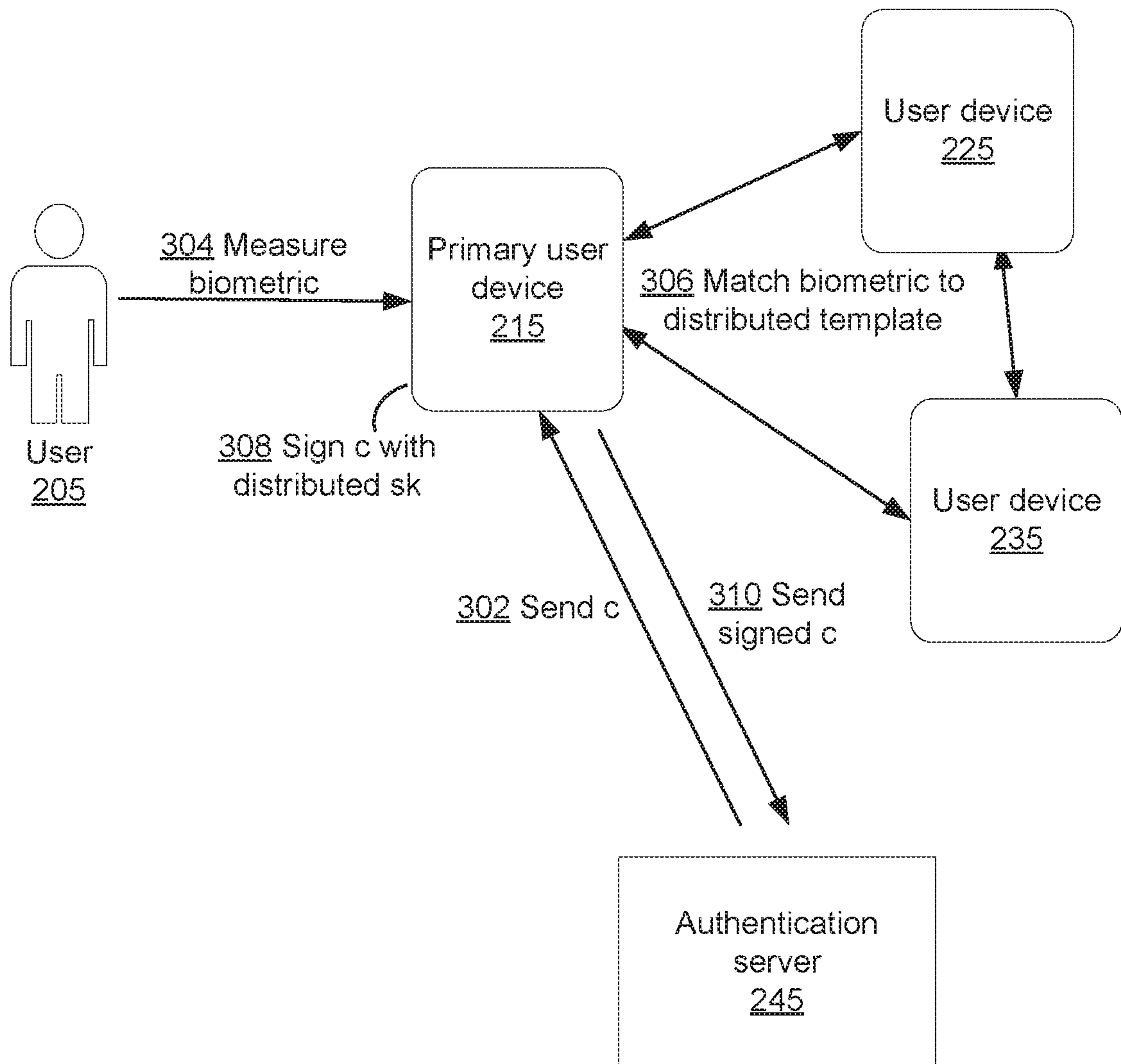


FIG. 3

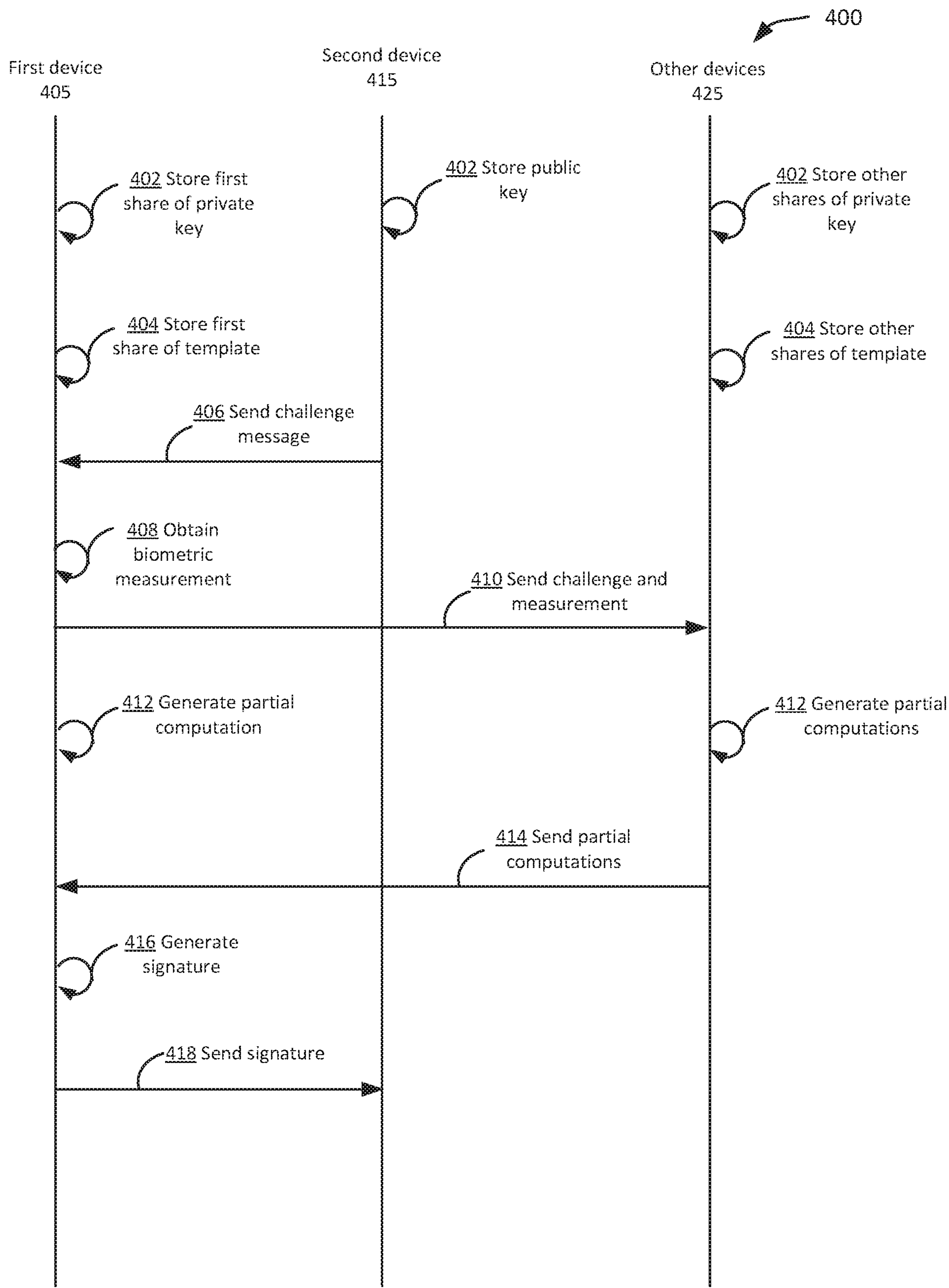


FIG. 4

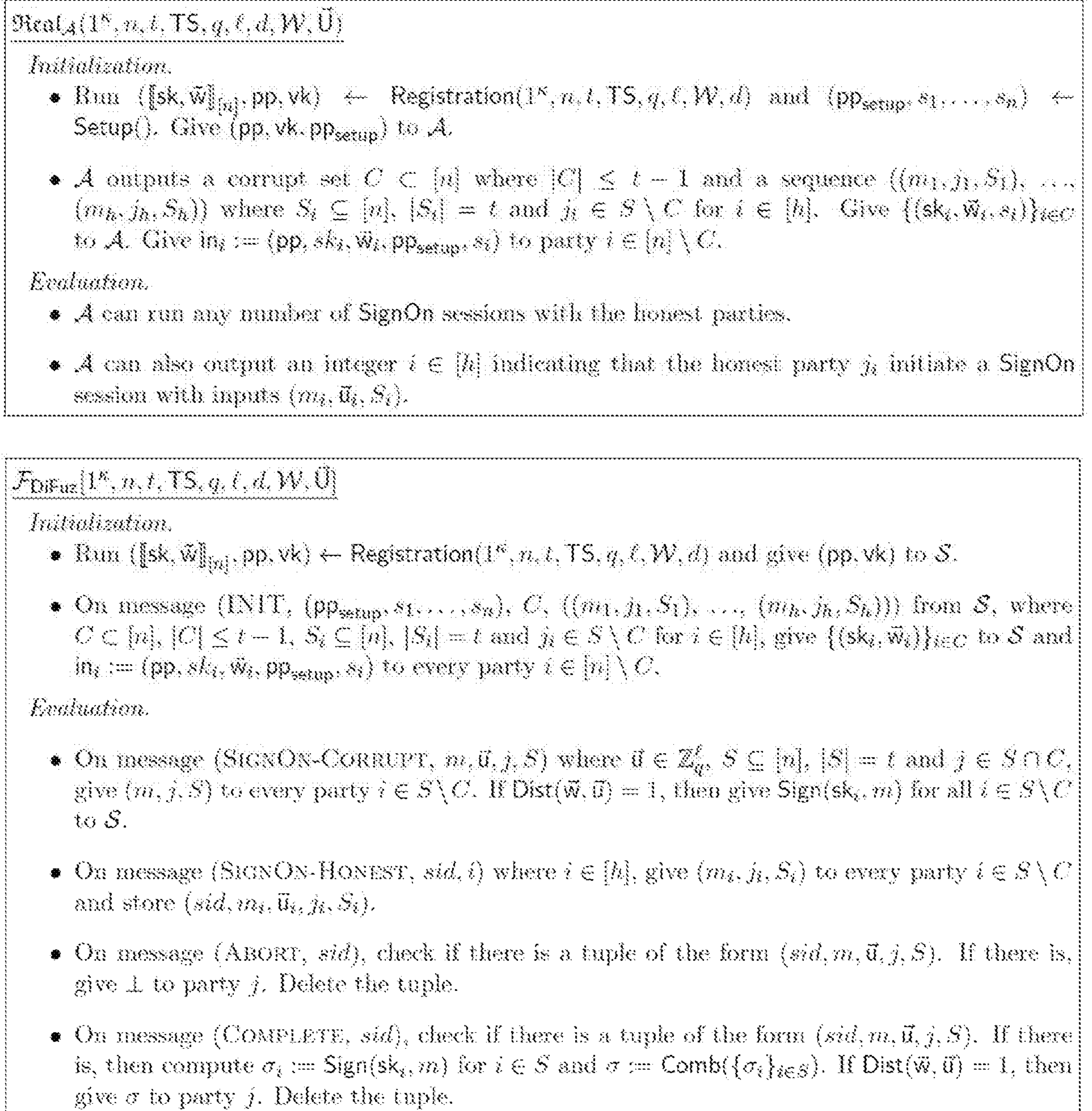


FIG. 5

Inputs:

- Party $P_i \in \mathcal{S}$ has input $(\tilde{w}_i, sk_i^{TS})$.
- Party $P^* \in \mathcal{S}$ additionally also has input $(\tilde{u}, m)$.

Computation:

- Compute $\tilde{w} = \text{Recon}(\{\tilde{w}_i\}_{i \in \mathcal{S}})$. Output $\perp$ to P^* if the reconstruction fails.
- If $\text{Dist}(\tilde{u}, \tilde{w}) < d$, output $\perp$ to P^* .
- Compute $\text{Token}_i = \text{TS.Sign}(sk_i^{TS}, m)$ using some randomness.
- Output $\{\text{Token}_i\}_{i \in \mathcal{S}}$ to party P^* .

FIG. 6

Hardwired values: $(a, b, c, d, p, q, r_2, \text{Pad}, d^2)$.^a

Inputs: $(x_1, x_2, y_1, y_2, z_1, z_2)$.

Computation:

- Abort if any of the following occur:
 - * $x_2 \neq (a \cdot x_1 + b)$ (or)
 - * $y_2 \neq (c \cdot y_1 + d)$ (or)
 - * $z_2 \neq (p \cdot z_1 + q)$
- Compute $\text{IP} = (z_1 - r_2) + x_1$
- If $\text{IP}^2 > (d^2 \cdot y_1)$, output Pad. Else, output $\perp$.

^aRecall that d is the threshold value for Cosine Similarity.

FIG. 7

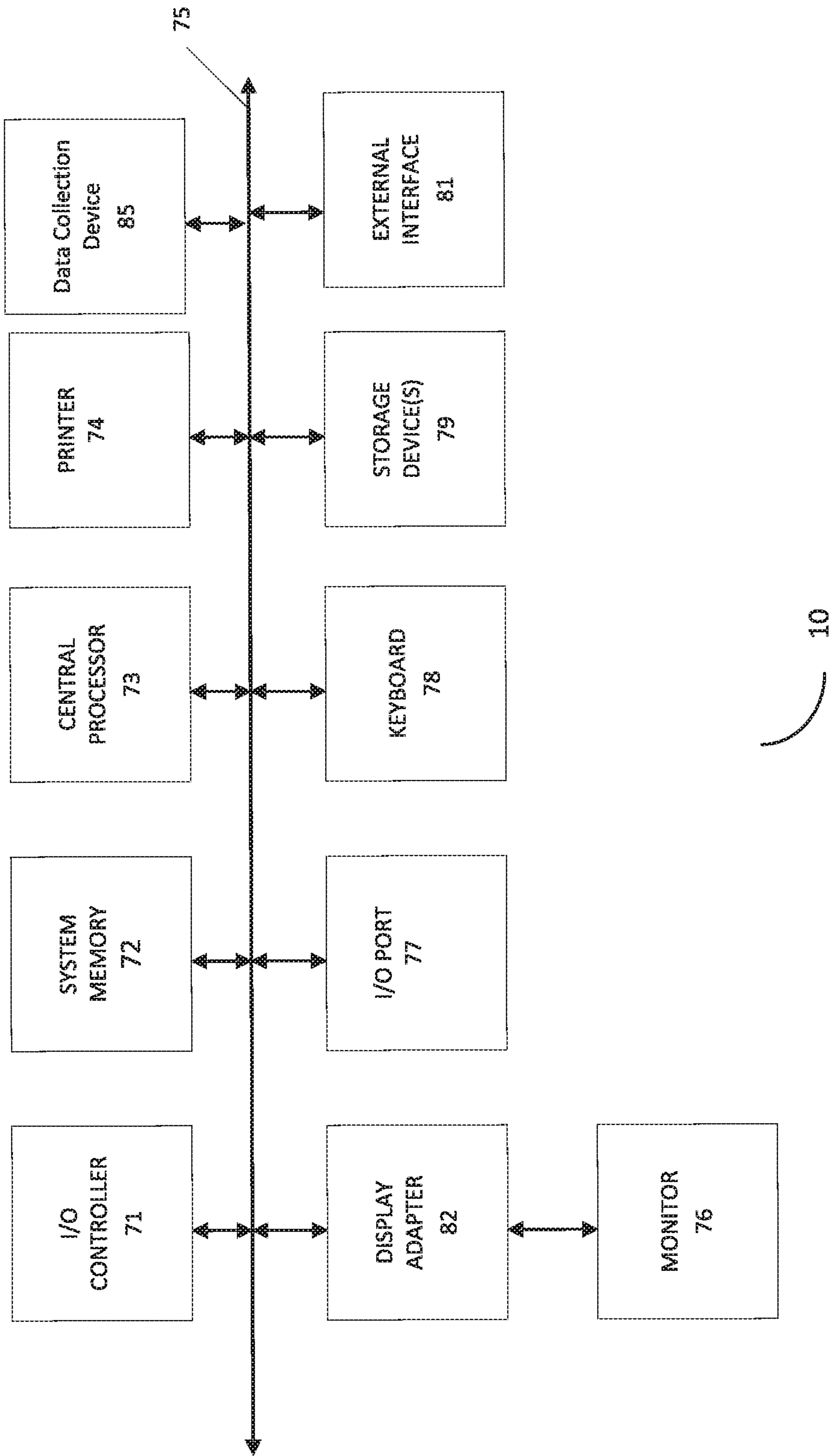


FIG. 8