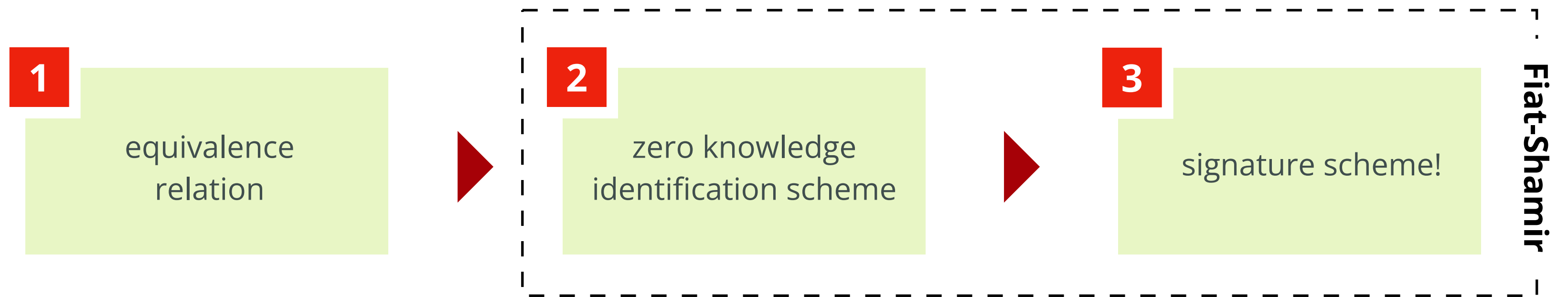




From MCE
to MEDS



1 → 2

SETUP

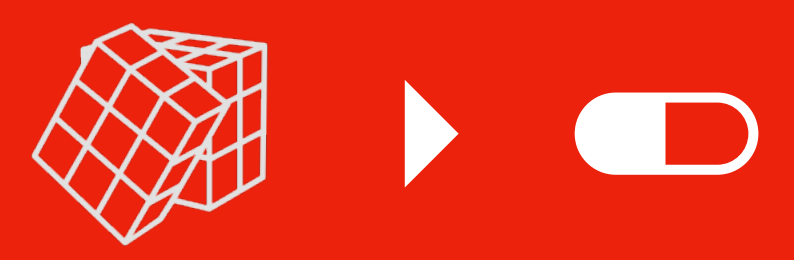
- Assume parameter set q, n, m, k . and "starting" code \mathcal{C}_0
- Generate **secret key** $A \in \text{GL}_m(q), B \in \text{GL}_n(q)$
- Generate **public key** $\mathcal{C}_1 = A\mathcal{C}_0B$

COMMIT

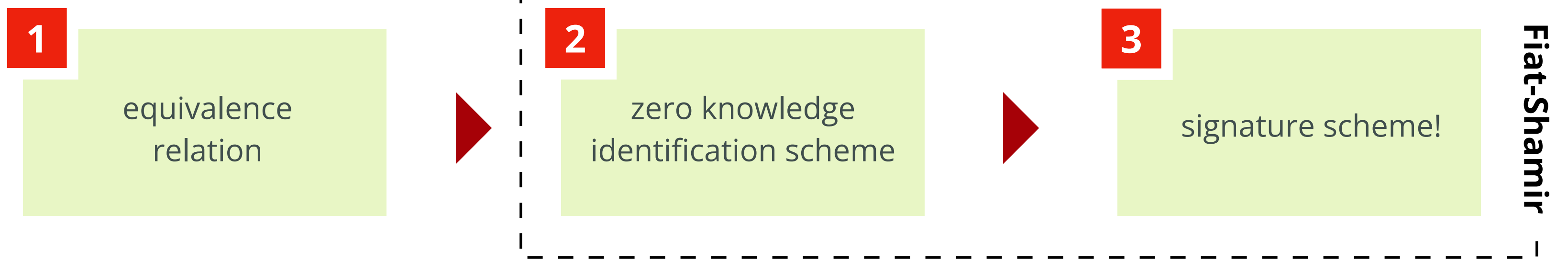
- Generate **ephemeral** $\tilde{A} \in \text{GL}_m(q), \tilde{B} \in \text{GL}_n(q)$
- Generate **ephemeral code** $\tilde{\mathcal{C}} = \tilde{A}\mathcal{C}_0\tilde{B}$

$$\begin{array}{ccc}
 \mathcal{C}_0 & \xrightarrow{(\tilde{A}, \tilde{B})} & \tilde{\mathcal{C}} \\
 (A, B) \downarrow & & \\
 \mathcal{C}_1 & &
 \end{array}$$

2



From MCE to MEDS



1 → 2

SETUP

COMMIT

- Assume parameter set q, n, m, k . and "starting" code \mathcal{C}_0
- Generate **secret key** $A \in GL_m(q), B \in GL_n(q)$
- Generate **public key** $\mathcal{C}_1 = A\mathcal{C}_0B$

- Generate **ephemeral** $\tilde{A} \in GL_m(q), \tilde{B} \in GL_n(q)$
- Generate **ephemeral code** $\tilde{\mathcal{C}} = \tilde{A}\mathcal{C}_0\tilde{B}$

