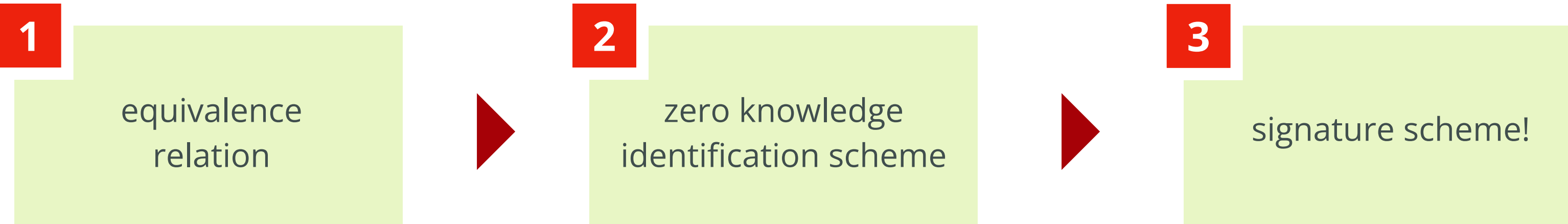




**From MCE
to MEDS**





**From MCE
to MEDS**

1

equivalence
relation



2

zero knowledge
identification scheme



3

signature scheme!

Fiat-Shamir