saving credentials

$[\text{credentials}]_{\text{eff.org} \wedge \text{box.com}}$

❶

fb.us

alice

missing priv

❷

eff.org   box.com

KEY:

$[E_{KEY}(\text{credentials})]_{\text{box.com}}$
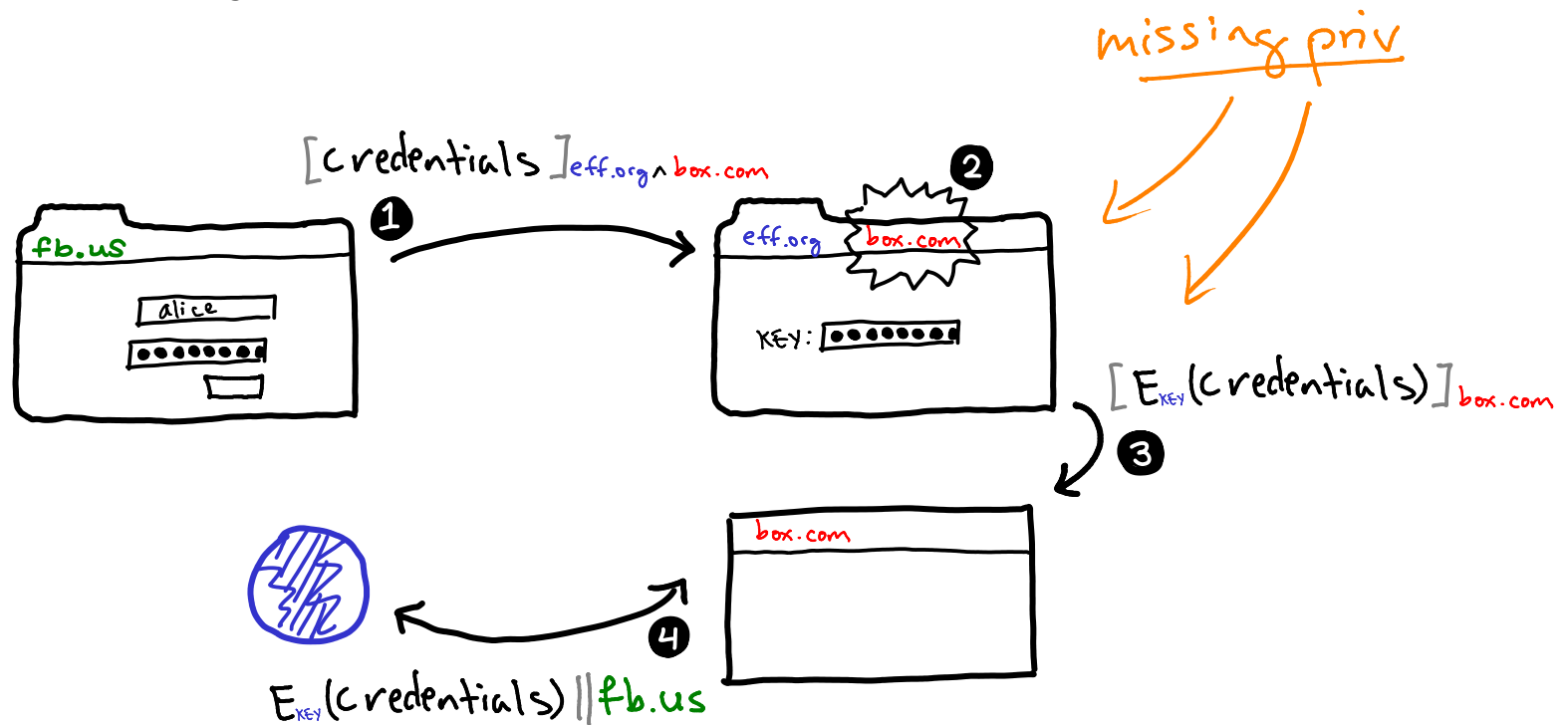
❸

box.com

❹

$E_{KEY}(\text{credentials}) \| \text{fb.us}$

fb.us creates the two compartments, and (1) sends the manager code the credentials labeled with "eff.org ∧ box.com", as to ensure that the data must be declassified by "box.com" before being stored (server-side). The manager reads the credentials (2) and encrypts; importantly after reading the credentials it cannot arbitrarily communicate over the network. The encrypted credentials are sent to the storage layer (3) which simply saves them alongside ownership meta-data ("fb.us") on the server-side (4).