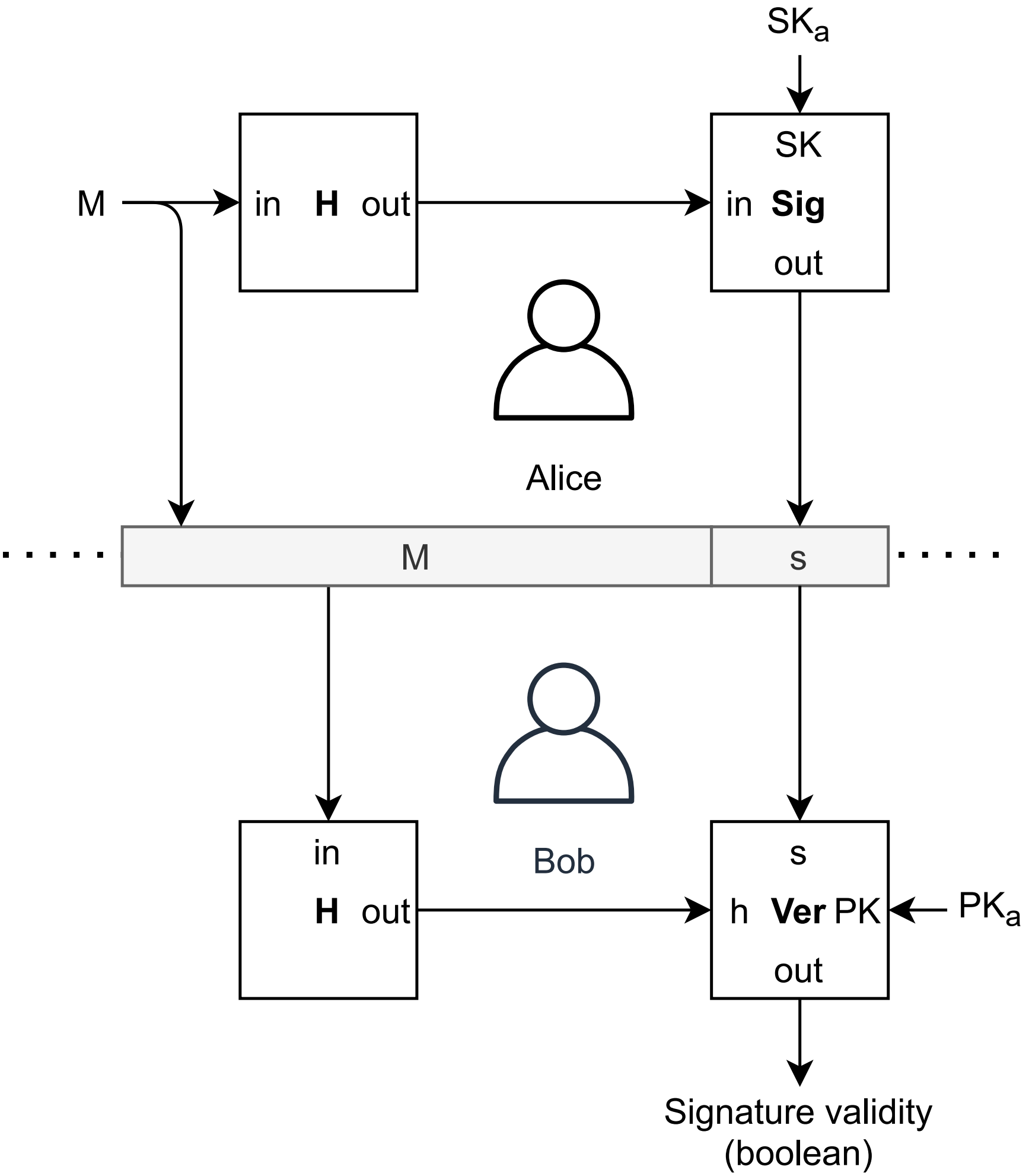
SK$_a$
M
in
H
out
SK
in
Sig
out
Alice
M
s
Bob
in
H
out
s
h
Ver
PK
out
PK$_a$
Signature validity
(boolean)