MACHINE
VARIABLES
p_out, p_in
INVARIANTS
inv7: $phase \in \{res, est\} \Rightarrow comp\_mac(p\_in(front) \mapsto p\_in(int) \mapsto p\_in(len)) = p\_in(mac)$
EVENTS
Event Report ⟨ordinary⟩ ≙
refines Report
where
grd10: $m = comp\_mac(fr \mapsto i \mapsto le)$
then
act2: $p\_out := \{front \mapsto fr, int \mapsto i, len \mapsto le, mac \mapsto m\}$
end

Event Integrity ⟨ordinary⟩ ≙
refines Integrity
where
grd7: $comp\_mac(rec2(front) \mapsto rec2(int) \mapsto rec2(len)) = rec2(mac) \Rightarrow acc = TRUE$
grd8: $comp\_mac(rec2(front) \mapsto rec2(int) \mapsto rec2(len)) \neq rec2(mac) \Rightarrow acc = FALSE$
then
act1: $phase :| (acc = TRUE \Rightarrow phase' = res) \wedge (acc = FALSE \Rightarrow phase' = detection)$
end
END

2