(1) HW key embedded in chip

(2) HW key signed by manufacturer