

Sprzętowe zabezpieczenia obejmują techniki takie jak fizyczna izolacja, zabezpieczenia przeciwfałszywkowe i bezpieczne magazynowanie kluczy kryptograficznych. Ważne jest również zabezpieczenie interfejsów komunikacyjnych i wbudowanych modułów, aby zapobiec nieautoryzowanemu dostępowi i manipulacjom. Implementowanie sprzętowych mechanizmów bezpieczeństwa stanowi pierwszą linię obrony przed zagrożeniami.