Rambus

SECURITY • CRYPTOGRAPHY
Debug Access Control
Use Case

Debug Access Control

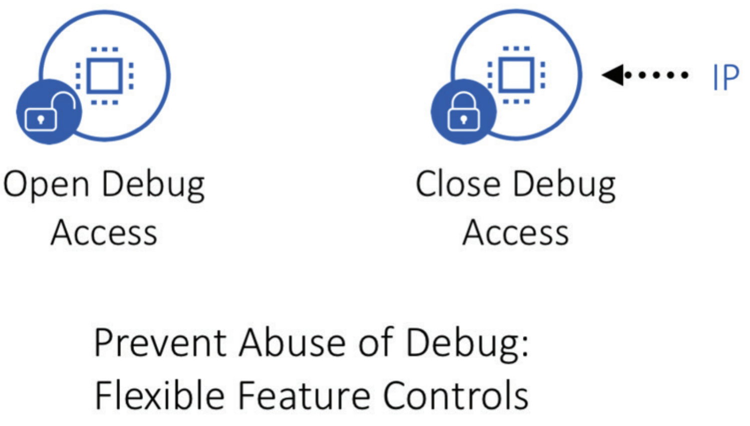
When chips are shipped into the field, it is required that test features, needed to test the chip during manufacturing, must be securely disabled (see Figure 1 below). If left enabled in the field, these test and debug ports could provide a back door into the device that could be used maliciously to read sensitive keys and other sensitive data from the device. These test features must be disabled when the part ships into the field, but must also be securely enabled later when defective parts are returned through the RMA (Return Merchandise Authorization) channel for failure analysis.

To prevent misuse of debug modes (e.g. BIST, scan, JTAG), the CryptoManager Root of Trust can be connected to the debug mode enable, which defaults to an off (safe) setting. The Root of Trust can selectively enable debug features as needed, for example:

- At specified manufacturing stages (wafer test, package test), necessary debug capabilities can be temporarily enabled
- In the case of a defective chip or device, debug capability can be re-enabled for Return Merchandise Authorization (RMA) and Failure Analysis (FA)

Once the debug is completed, the Root of Trust will disable the debug mode.
The CryptoManager solution provides a method for chip and device companies to authenticate the device and authorize the provisioning of the debug enable/disable operation for each device.

Figure 1: Secure Debug Access Control


IP
Open Debug Access
Close Debug Access
Prevent Abuse of Debug:
Flexible Feature Controls