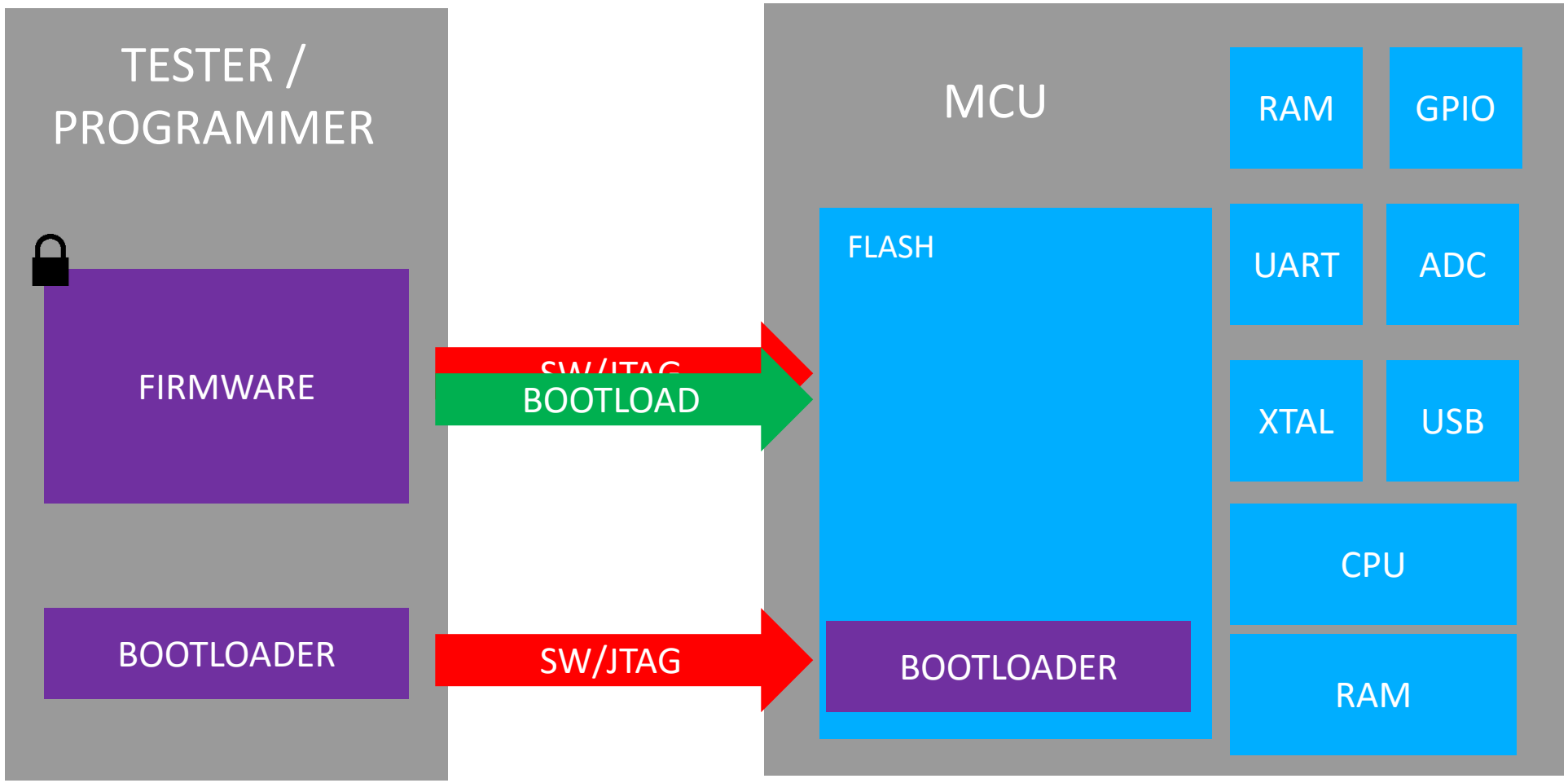
SILICON LABS

Security in Manufacturing: Closing the Backdoor in IoT

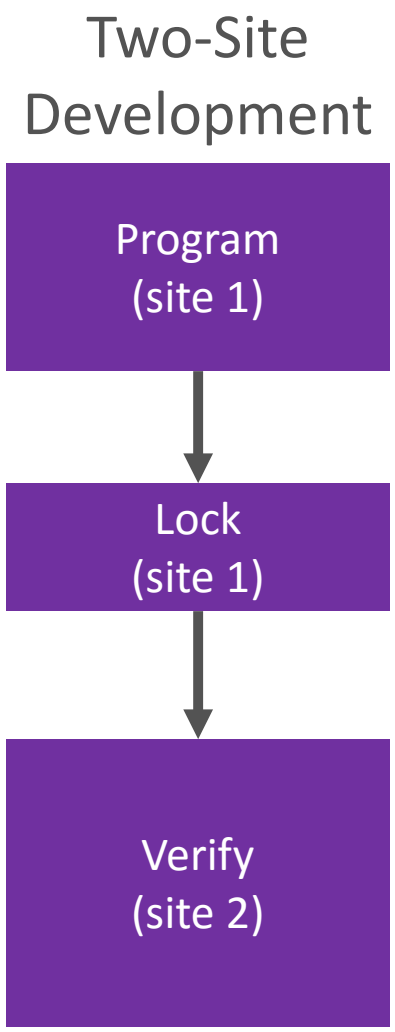
JOSH NOREM

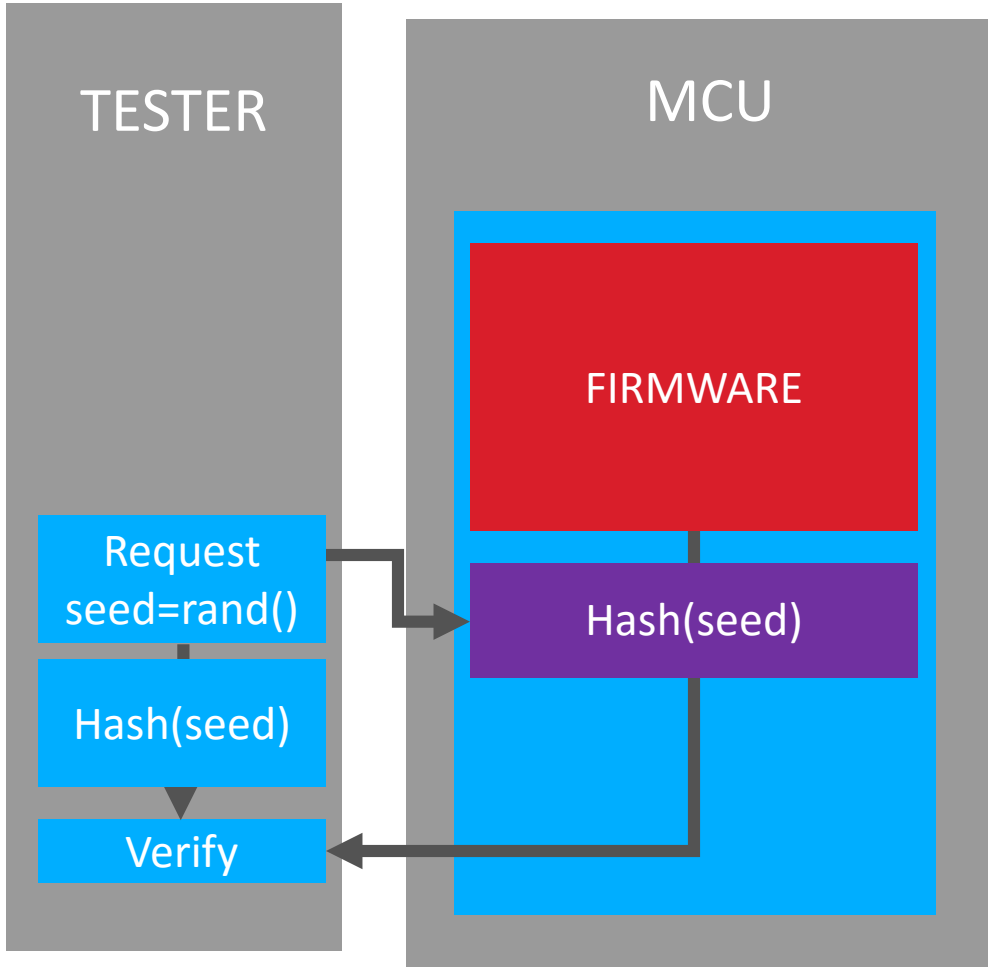
Introduction

Firmware Integrity: Challenge

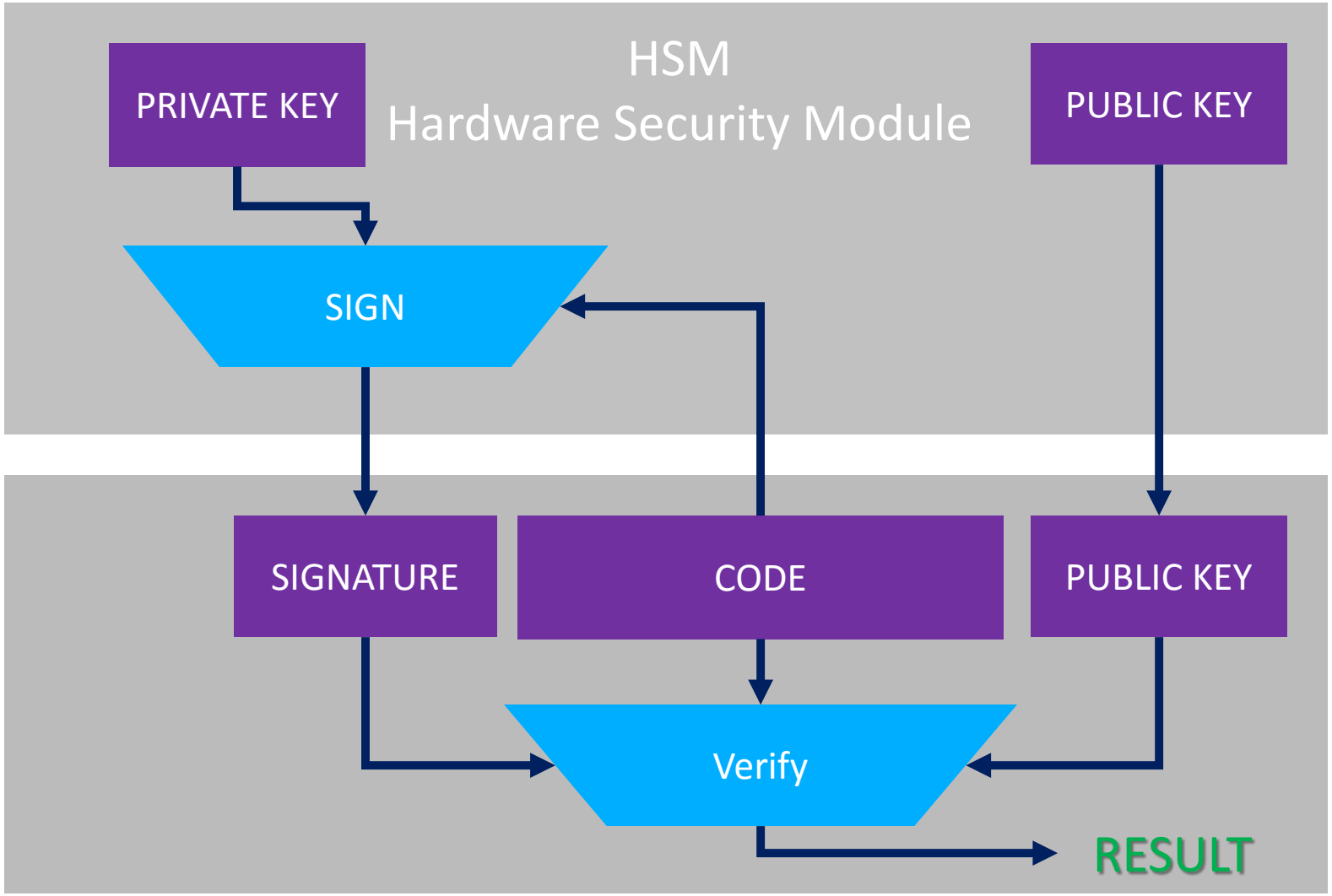


Firmware Integrity: Current Solutions

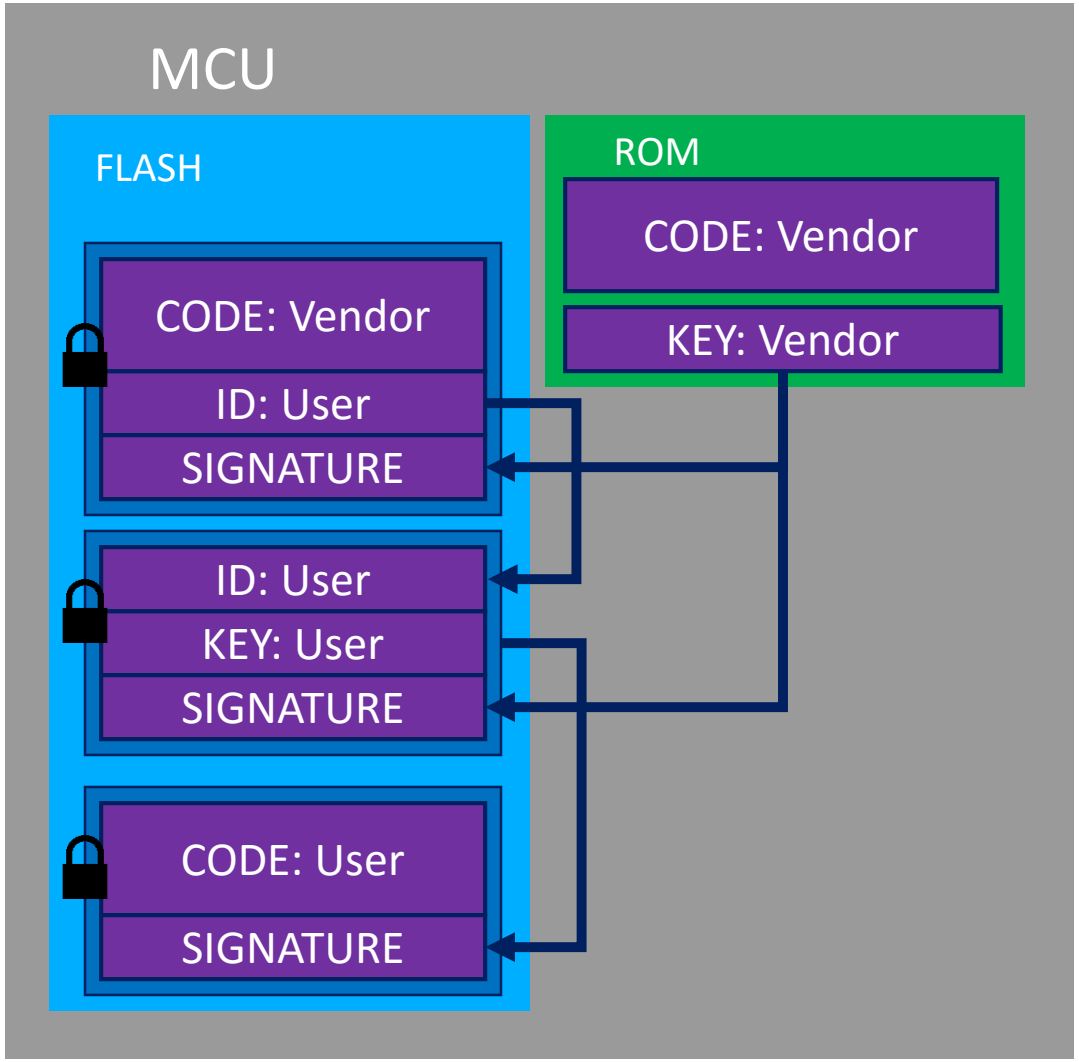




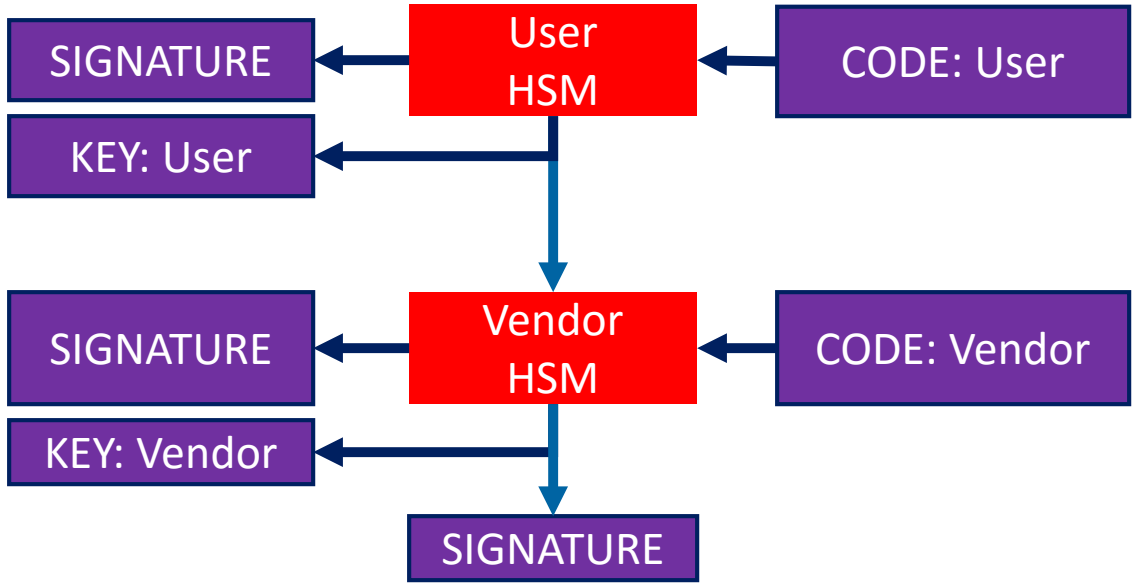
Signing Refresher



Firmware Integrity: Secure Boot

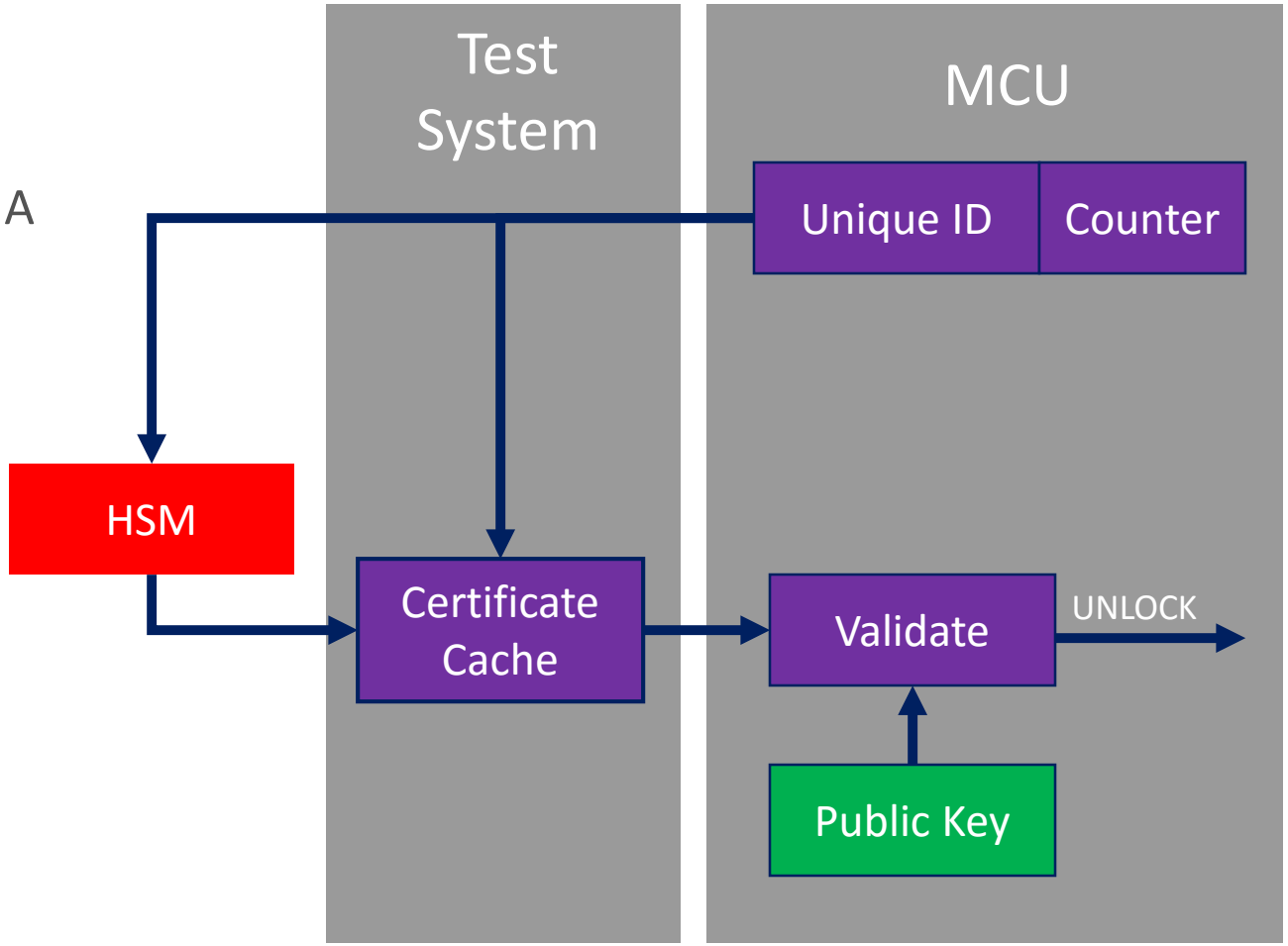


1. Add tamper proof Root of Trust (RoT)
2. Protect vendor code with RoT
3. User also signs code
4. User KEY protected by Vendor
5. Part can be tied to specific user



Secure Debug

- Today's solutions
  - Don't lock the device
  - Permanently lock device preventing RMA
  - Provide unlock + erase
  - Provide a secret backdoor to unlock
- Secure debug provides access without risk
  - System queries device unique ID
  - HSM generates unlock certificate
  - System sends certificate to unlock
  - Revoke certificate with counter



Securing Development

- Secure access to systems
  - Physical security
  - Auto-lock screens
- Secure source
  - Code reviews
  - Managed releases
- Secure delivery systems
  - FTP
  - Database

Conclusion

- Development and manufacturing are essential parts of product security
- Innovative hardware solutions are being developed and implemented today
- We can take many critical steps today to limit risk

www.silabs.com/EW2018