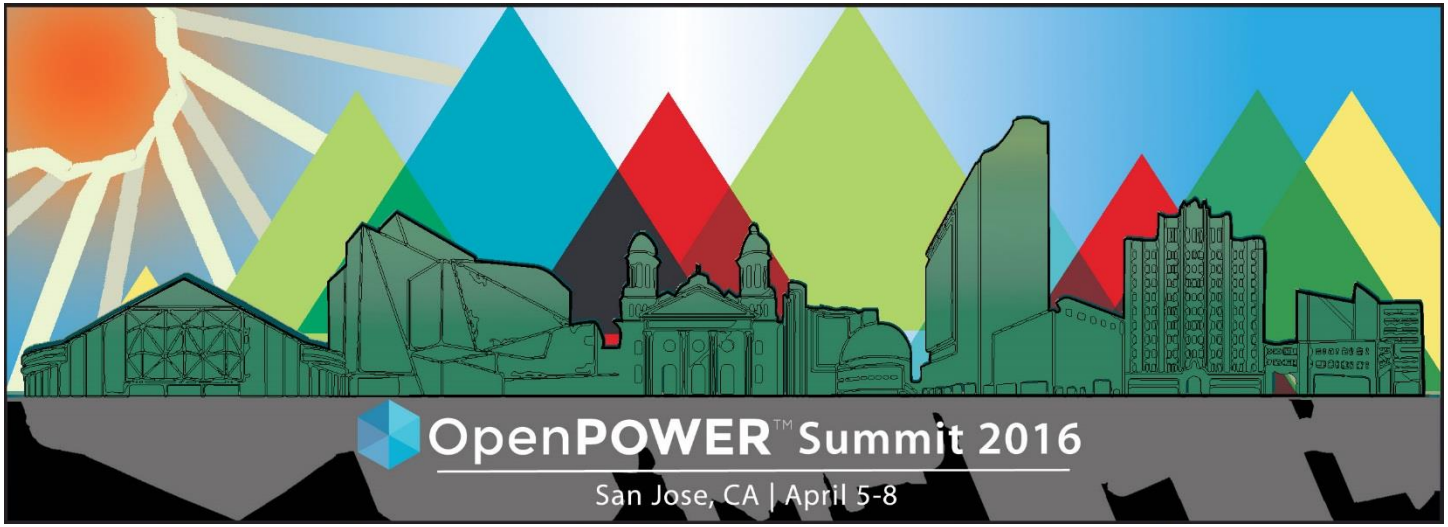
OpenPOWER™

OpenPOWER Secureboot Overview

Dean Sanner, POWER FW Architect

IBM

Revolutionizing the Datacenter



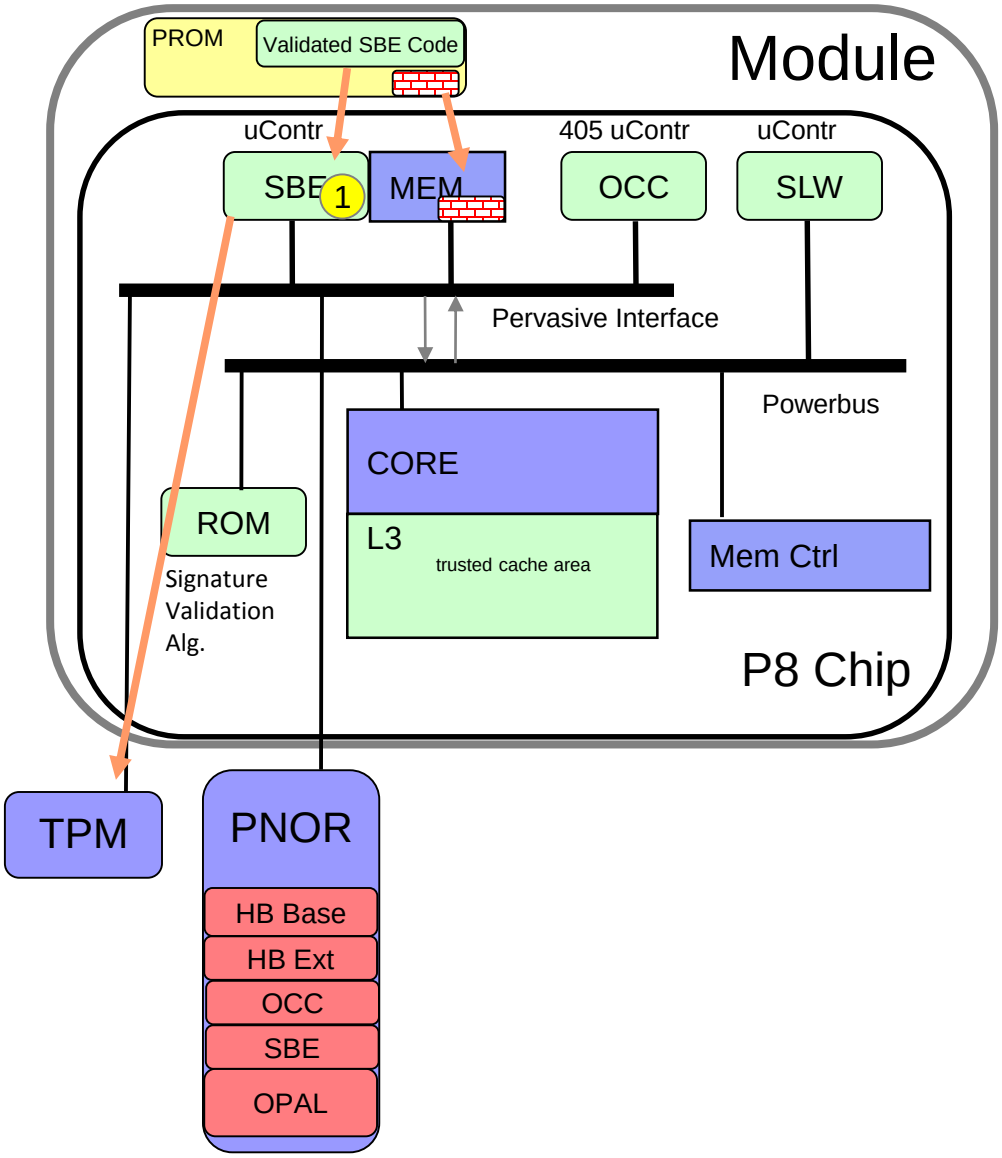
Join the Conversation #OpenPOWERSummit

OpenPOWER Secure Boot Principles

- All code in Flash is validated prior to execution
  - Never execute directly from Flash
  - Always copied into secure mem, verified, and then executed
- Design built around layers of trust:
  - Each boot starts from clean state
  - Core Root of Trust
    - Self Boot Engine(SBE) and Hostboot base
  - Lower layers verify subsequent layers
  - Processor PROM (SBE) updatable only by verified Hostboot
    - HW locked down after update
- Imprint Key
  - Well known public/private key
  - Allow partners to replace Processor PROM key with their own

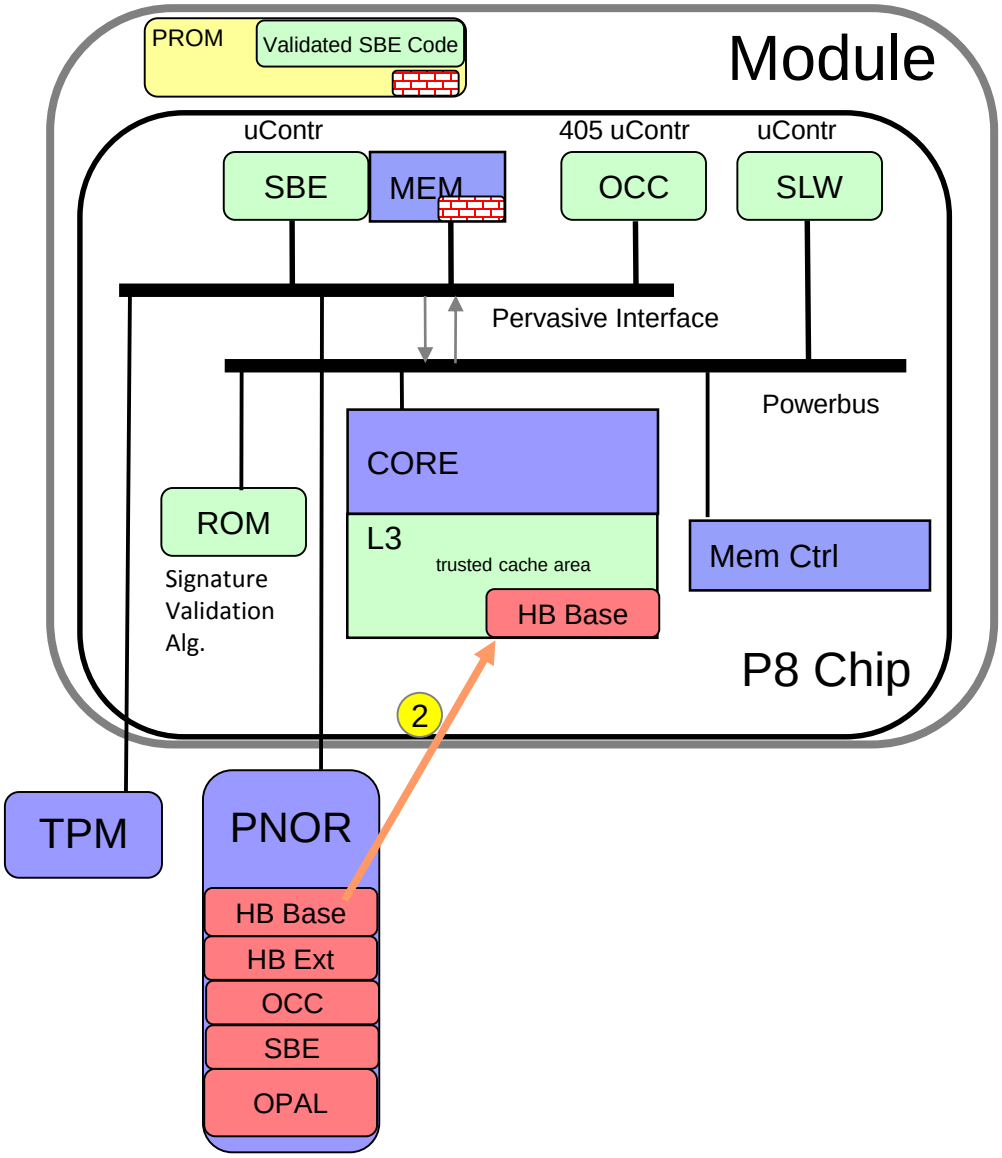
P8 Secureboot

1) SBE Execution (SEEPROM)
   - Basic Chip Init, TPM Reset
   - Move key from PROM to PIBMEM



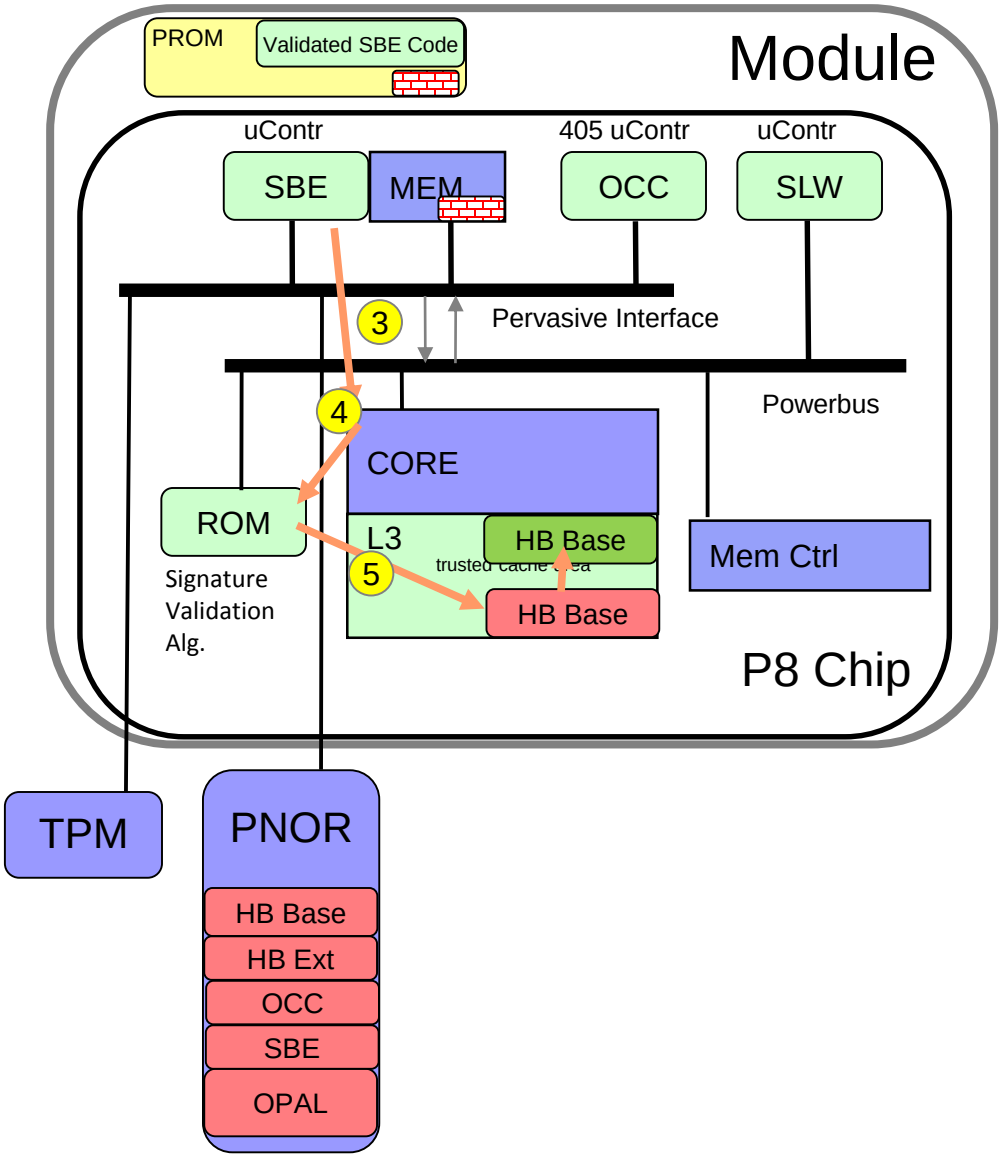
P8 Secureboot

1) SBE Execution (SEEPROM)
   - Basic Chip Init, TPM Reset
   - Move key from PROM to PIBMEM
2) **SBE loads HB Base from Flash to untrusted cache**



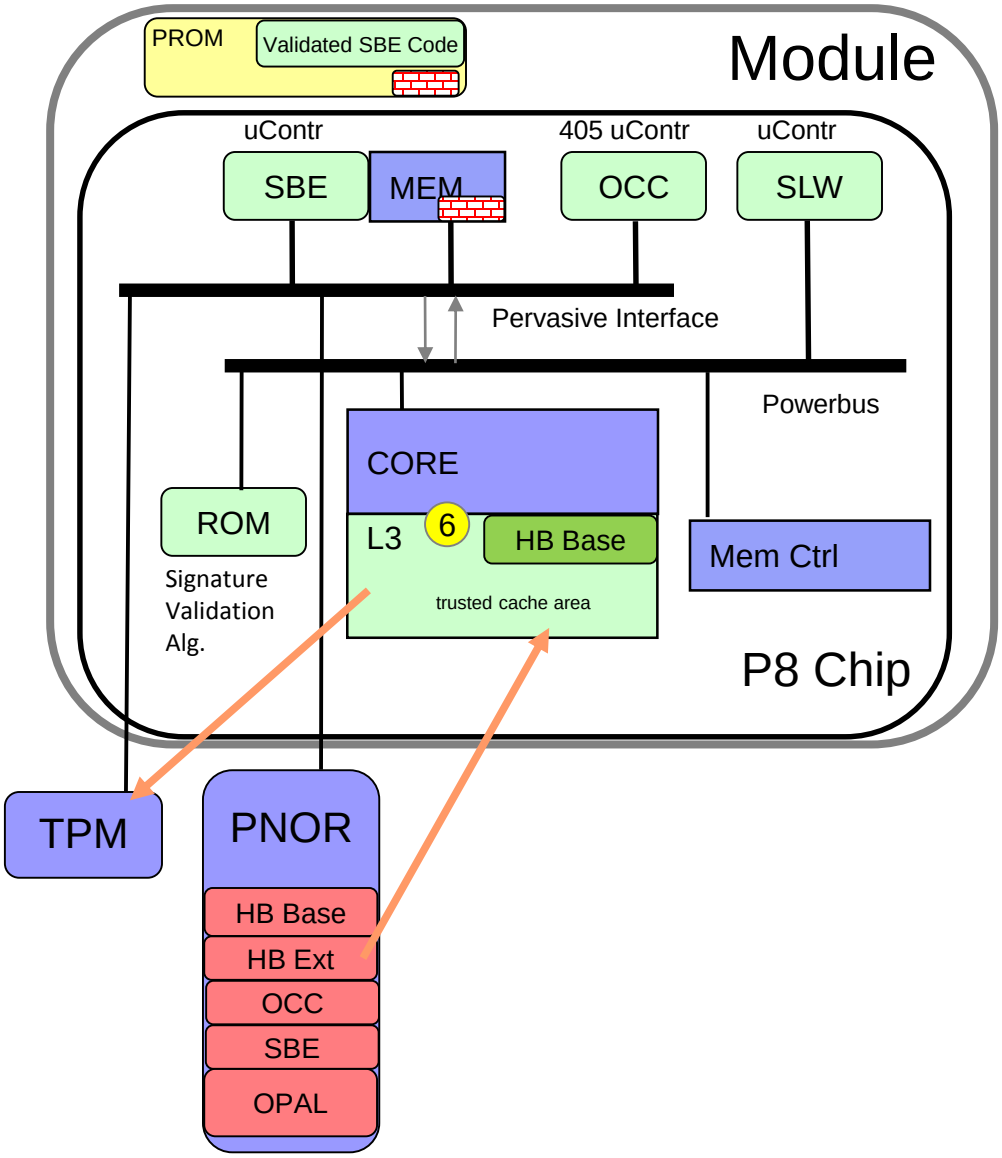
P8 Secureboot

1) SBE Execution (SEEPROM)
   - Basic Chip Init, TPM Reset
   - Move key from PROM to PIBMEM
2) SBE loads HB Base from Flash to untrusted cache
3) **Core instruction start**
4) **HW jumps to ROM**
5) **ROM verifies HB Base load based on key in PIBMEM (ECDSA521 & SHA512)**



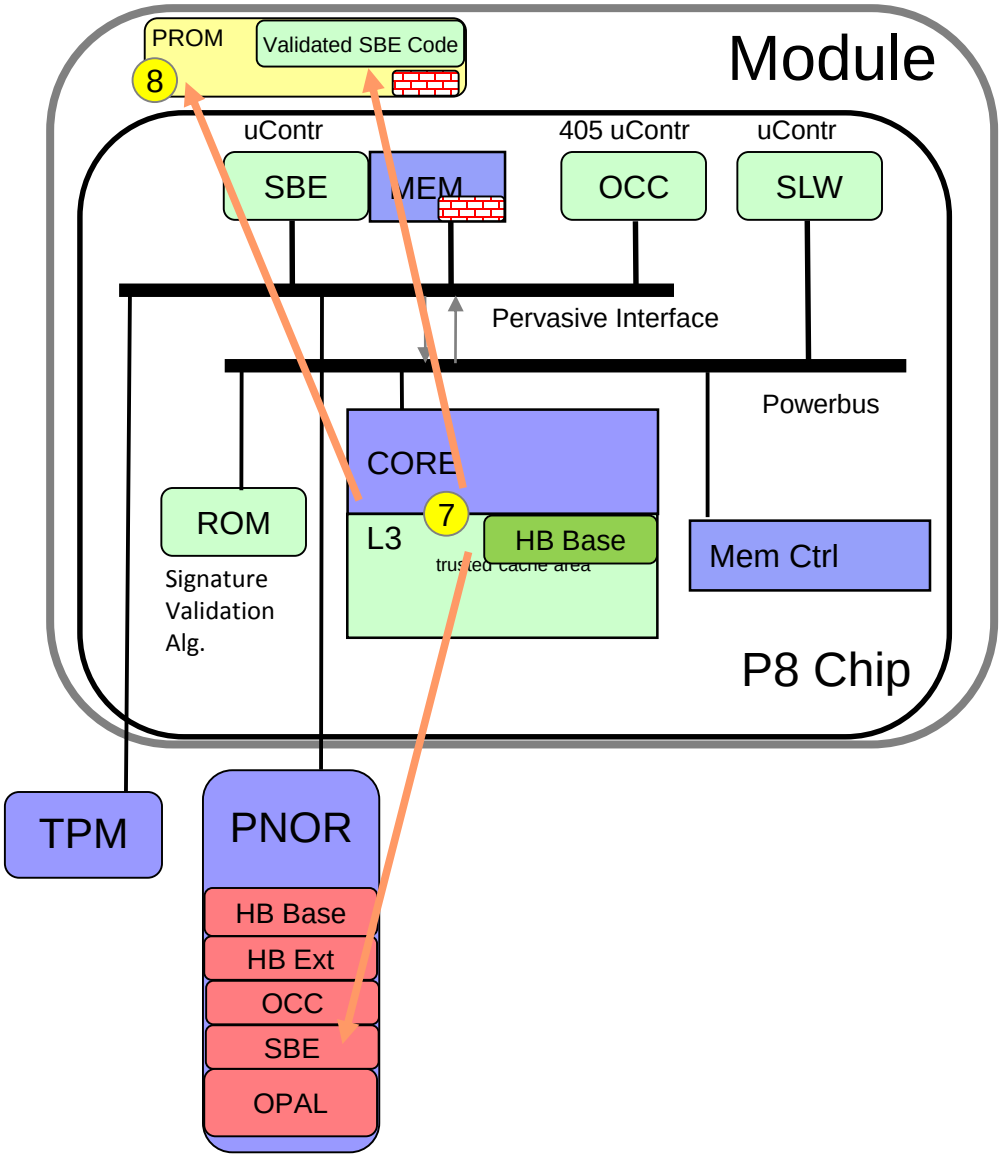
P8 Secureboot

1) SBE Execution (SEEPROM)
   - Basic Chip Init, TPM Reset
   - Move key from PROM to PIBMEM
2) SBE loads HB Base from Flash to untrusted cache
3) Core instruction start
4) HW jumps to ROM
5) ROM verifies HB Base load based on key in PIBMEM(ECDSA521 & SHA512)
6) **HB (from L3) loads HB Ext as needed**
   - **HBB contains hash of each HBI page**
   - **Verifies each page upon load**
   - **Places measurements in TPM**



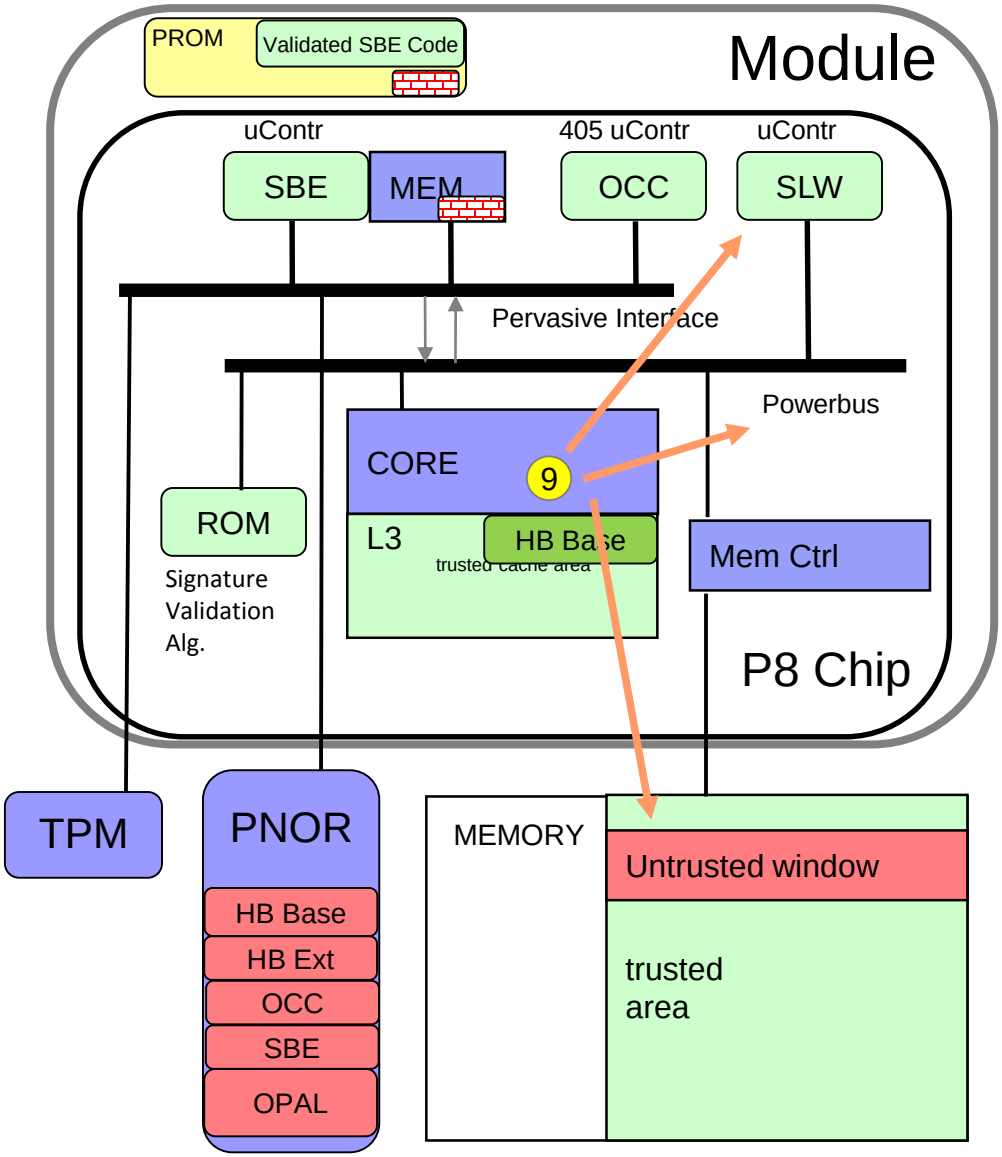
P8 Secureboot

1) SBE Execution (SEEPROM)
   - Basic Chip Init, TPM Reset
   - Move key from PROM to PIBMEM
2) SBE loads HB Base from Flash to untrusted cache
3) Core instruction start
4) HW jumps to ROM
5) ROM verifies HB Base load based on key in PIBMEM (ECDSA521 & SHA512)
6) HB (from L3) loads HB Ext as needed
   - HBB contains hash of each HBI page
   - Verifies each page upon load
   - Places measurements in TPM
7) **HB updates SEEPROM (if needed)**
   - **Validates newer version from PNOR**
8) **HB locks SEEPROM**



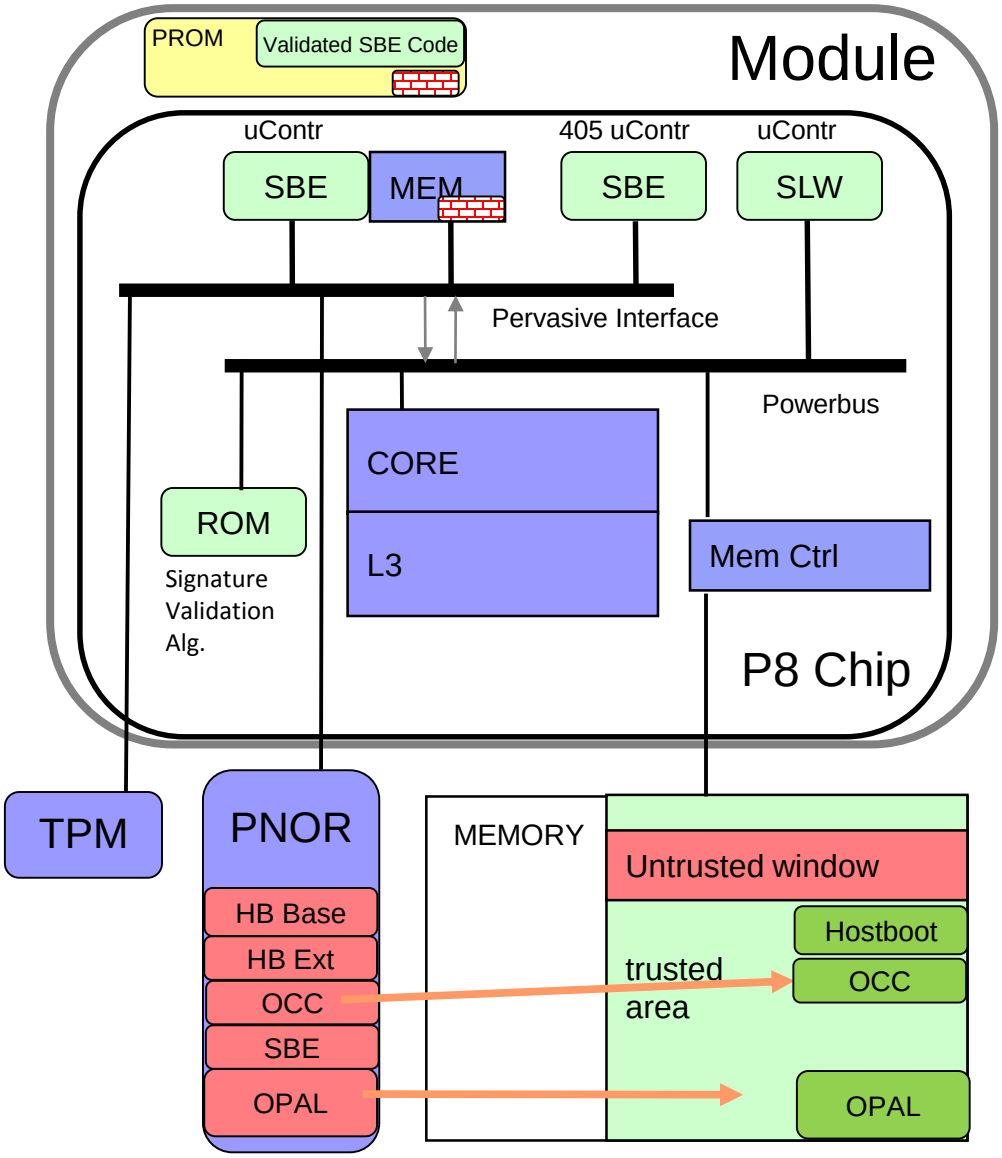
P8 Secureboot

1) SBE Execution (SEEPROM)
   - Basic Chip Init, TPM Reset
   - Move key from PROM to PIBMEM
2) SBE loads HB Base from Flash to untrusted cache
3) Core instruction start
4) HW jumps to ROM
5) ROM verifies HB Base load based on key in PIBMEM (ECDSA521 & SHA512)
6) HB (from L3) loads HB Ext as needed
   - HBB contains hash of each HBI page
   - Verifies each page upon load
   - Places measurements in TPM
7) HB updates SEEPROM (if needed)
   - Validates newer version from PNOR
8) HB locks SEEPROM
9) **HB trains memory, Powerbus, cores**
   - **Loads, verifies, starts SLW uContlr**



P8 Secureboot

1) SBE Execution (SEEPROM)
   - Basic Chip Init, TPM Reset
   - Move key from PROM to PIBMEM
2) SBE loads HB Base from Flash to untrusted cache
3) Core instruction start
4) HW jumps to ROM
5) ROM verifies HB Base load based on key in PIBMEM (ECDSA521 & SHA512)
6) HB (from L3) loads HB Ext as needed
   - HBB contains hash of each HBI page
   - Verifies each page upon load
   - Places measurements in TPM
7) HB updates SEEPROM (if needed)
   - Validates newer version from PNOR
8) HB locks SEEPROM
9) HB trains memory, Powerbus, cores
   - Loads, verifies, starts SLW uContlr
- Loads, verifies, starts STOP uContlr
10) **HB loads payload, OCC**
   - **Verifies, starts execution**



Future Secure Boot Plans

- P9 Changes
  - SBE will be open source
  - Eliminate on chip ROM Security algorithm
  - Loader and Security algorithm located on Processor PROM
    - Allows for customization of security algorithm
    - Only validated code can update PROM
    - Loader and algorithm runs on Host core
  - Firmware control over unsecure window

- Targeting limited P8 Trusted boot functionality by Year End 2016
  - P8 Modules shipped with imprint keys
  - TCG Compliant TPM 2.0 architecture – Measurement and logging
    - Specific implementation of Nuvoton TPM via I2C