PROVE & RUN

European Processor Initiative (EPI)
Embedded Security

77, avenue Niel, 75017 Paris, France

contact@provenrun.com

Prove & Run – Security Services and Solutions

A

Consulting Services

- Security analysis
- Security architecture

B

Solutions to secure-by-design critical ECUs

- Leveraging on 2 unique critical off-the-shelf software components:
- ***ProvenCore*** : ultra secure OS
- ***ProvenVisor:*** secure hypervisor

Prove & Run Team (some related references)

- Prove & Run team has a long experience in assisting major chip vendors with the their hardware and software (security) architectures,
- Prove & Run key senior security architects have assisted about half of the top ten chip vendors worldwide in designing or improving some of their major security architectures.
- Prove & Run has been associated (as a consultant) to many security projects for ARM (such as writing various Protection Profiles or security requirements for ARM, in various market segment : Smartphones, IoT, gateways, Cloud, etc.).
- In charge of defining EPI Hardware and Software Security Architecture.

Security: Certification is the final judge

Prove & Run has completed a **Common Criteria EAL7 evaluation** of ProvenCore.

This is a **world première**

There is no existing TEE or Secure OS at that level of security.

Formally verified of the complete TCB

Also a world première

EPI Security Needs and Security Architecture

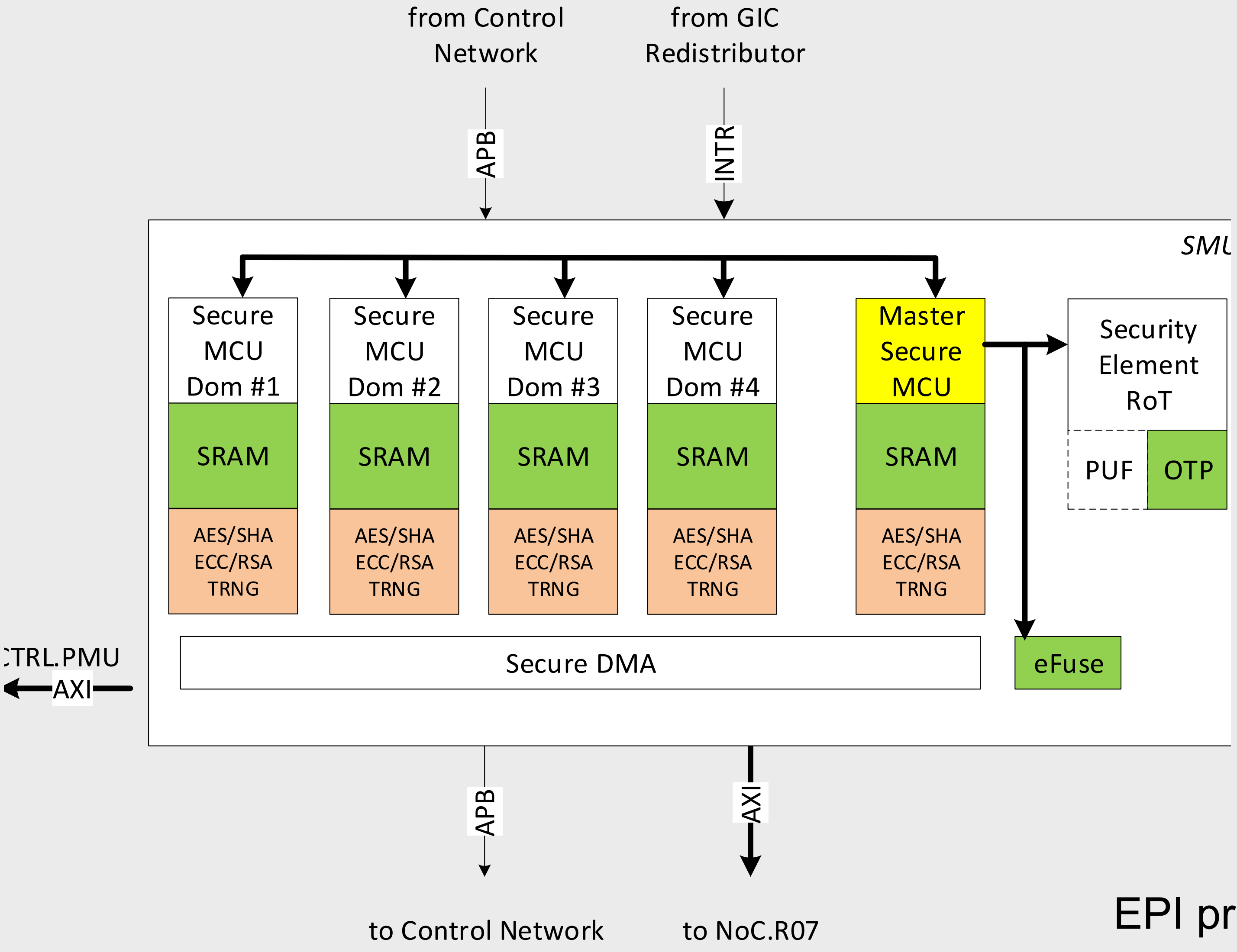
EPI (Basic) Security Needs

- Providing a strong root of trust,
- Advanced cryptographic support,
- Providing a safe deposit for keys,
- Providing key derivation services,
- Supporting full product life cycle (including the manufacturing and personalization phases),
- Providing secure debug functionality,
- Support for independent application providers (and enforcing no interdependence between them in regards of development and certification)
- Support for secure and selective firmware update
- Support for rollback,
- Etc.

EPI (More advanced) Security Needs

- High level of certification,
- High level of trust,
    - Security certification (by various bodies)
- Security domains (each one including a configurable set of application processors),
- The possibility for a security domain to execute and isolate a secure OS,
- The possibility for a security domain to control a configurable list of peripherals,

EPI High Level Security Architecture



EPI proprietary