PROVE & RUN

www.provenrun.com

PROVENCORE-CC7

ProvenCore-CC7 is a trusted operating system (OS) designed to help secure embedded devices based on application processors such as automotive gateways or telematic units, IoT gateways, communication and mobile devices, etc. ProvenCore-CC7 provides security architects with an off-the-shelf certifiable foundation to build or reinforce the security architecture of their solution, whether for new or existing devices.

Why Use ProvenCore-CC7

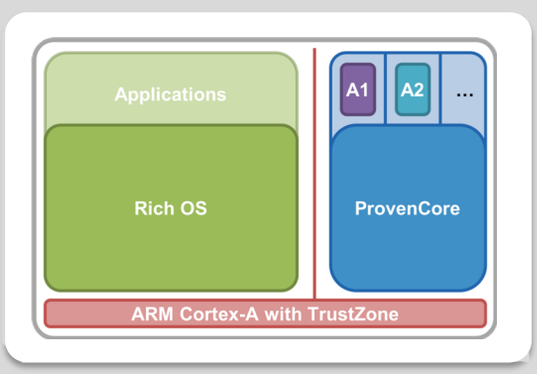
ProvenCore-CC7 is primarily designed to run alongside a conventional OS (or Rich OS) in embedded systems. Many processors are designed with this dual OS architecture in mind – a technology called TrustZone by ARM© and SGX© by Intel. The privileged situation of trusted OSs in what is called a trusted execution environment (TEE) allows them to execute security functions and exert control over the conventional OS.

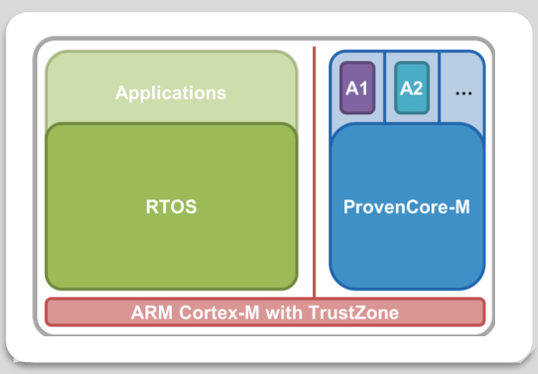
A dual-OS architecture is a valuable design for security and has been widely adopted in the mobile phone industry. However, the trusted OSs that have been developed so far for the mobile industry do not offer the necessary protection against remote attacks targeting connected devices. Moreover, most trusted OSs do not possess the features that would make them capable of executing all the functions that should be performed in a TEE for security reasons. ProvenCore-CC7 offers a solution to the two issues identified.

- Developed using formal methods and backed by a Common Criteria EAL7 certification, ProvenCore-CC7 can claim superior code quality (as close as possible to zero-defects) leaving almost no attack surface to hackers. Use of formal proofs also promotes much easier maintainability of the ProvenCore code base, a critical factor for a software component as complex as an OS, and consequently a much-reduced Total Cost of Ownership (TCO).
- ProvenCore-CC7 offers a high level of abstraction for developing security services. ProvenCore-CC7 checks all the interactions between the security services, as well as all the interactions between the security services and the outside world. With ProvenCore-CC7 , the development of security services becomes simpler and cheaper, leading to more security at a lower cost.

For those industrial sectors that are subject to certification – or may be subject to certification in the coming years – ProvenCore-CC7 brings certainty that certification will be met with no pain – whatever the requirement level – for the lowest possible cost.

Typical Configurations





Examples of Security Functions That Can Run on ProvenCore

- Fully autonomous firmware update over-the-air (FOTA)
- Secure VPN
- Secure storage and use of keys and certificates
- Intrusion detection and protection systems (IDPS)
- Filters, firewalls
- Remote maintenance
- Trusted user interface (TUI)
- Recovery OS (implementing the most necessary features of the Rich OS when it fails)

Supported Processors

ProvenCore runs on:

- ARM Cortex-A microprocessors compliant with the ARMv7-A and ARMv8-A architectures,
- ARM Cortex-M microcontrollers compliant with the ARMv7-M and ARMv8-M architectures,
- RISC-V processors.

77 avenue Niel, 75017 Paris, France - +33 1 75 77 55 55 - contact@provenrun.com