

Summary of *NVIDIA: Using RecordFlux and SPARK to Implement SPDM for Secure Computing*, AdaCore Technical Paper

RecordFlux and SPARK

- The AdaCore RecordFlux technology is a Domain-Specific Language (DSL) for precisely defining the structure of binary messages, and a toolset for generating formally verifiable code for parsers, message generators, and protocol sessions.
- The produced source code is in the SPARK language.
- SPARK Pro can prove a range of program properties, ranging from valid information flow and memory safety, up to full functional correctness.

NVIDIA's challenge

- NVIDIA wanted to implement a chosen subset of SPDM functionality, with high confidence that the implementation is provably correct (for example, knowing that their application is memory safe and would never raise a runtime exception), while staying within tight device storage and runtime memory constraints for the generated code.
- Although other SPDM implementations are available (for example, OpenSPDM), NVIDIA wanted a technology with a more secure foundation, especially with respect to the programming language.
- Must be interoperable with OpenSPDM.

The open-source version of the code

- <https://github.com/AdaCore/spdm-recordflux>