PSA Crypto Headers for v8-M Systems

TF-M Technical Forum

Antonio de Angelis, Arm OSS group

June’23

PSA Crypto Headers for v8-M Systems

- PSA Crypto API Specification leaves certain portions as IMPDEF
  - Implementation details of structures, platform-dependent behaviour
  - Different implementations end up with different implementation-specific header files
  - Increased flexibility for a wide set of scenarios
    - degrees of freedom between implementations

- Looking at reducing barriers for using PSA Certified APIs on v8-M systems
  - Provide a unique reference for what the PSA Crypto spec leaves undefined
  - Not an appendix to the PSA specifications, but a reference implementation

- Define the implementation for a transport layer based on SPM for v8-M TrustZone
  - Implementation reflects what is needed for a remote call across the SPM based transport layer on a v8M system
  - v8-M PSA API Secure firmware interface (S and NS) uses these PSA Crypto headers file implementation.
  - Uniquely identify a recommended solution when deploying PSA Crypto along TrustZone enabled v8-M Systems
  - If having a unified header:
    - Mbed TLS + TF-M Crypto have a simpler integration in SDKs where they coexist

arm

Thank You
Danke
Gracias
Grazie
谢谢
ありがとう
Asante
Merci
감사합니다
धन्यवाद
Kiitos
شكرًا
ধন্যবাদ
תודה