Mbed TLS, Mbed Crypto, Mbed OS

What have we been up to and where are we going?

Jaeden Amero

2019-10-30

What we work on

Mbed TLS

Mbed TLS is a TLS stack that can use the PSA Crypto API.

- TLS library
- X.509 library
- No implementation of cryptography

Mbed Crypto

Mbed Crypto is Arm's reference implementation of PSA Crypto.

- Cryptography library with a PSA Crypto API
- Split from Mbed TLS in 2018
  - Provides the Mbed TLS Crypto API as well (for backwards compatibility)

Mbed OS

Mbed OS is a connectivity-rich IoT OS.

- Provides a pre-integrated, ready to go platform for IoT

What we've been up to

Secure element driver interface

The PSA secure element driver interface is for hardware with keys you can't read.

- Hardware examples
  - Secure element
  - Smart card
  - HSM
- Example Mbed OS driver for ATECC508A

Providing a TLS stack built on PSA

We've been making Mbed TLS use PSA in more and more places.

We've been optimizing the whole stack.

- Reduced code size
- Reduced RAM usage

We've been improving our examples.

- Mutually authenticated TLS, with keys in secure element

Where we are going

Mbed OS

We are working on integrating Mbed OS with TF-M.

- Using TF-M as-is, rather than copy-pasting bits

Secure element driver interface

We are working to standardize the interface in PSA.

- Keep working with it, refining in preparation for standardization
- Standardize in PSA Crypto API 1.x

Entropy source driver interface

The entropy source driver interface is used to seed the software random number generator.

- Implement for at least one device
- Standardize in PSA Crypto API 1.x

Accelerator driver interface

The PSA accelerator driver interface is used to write drivers for devices that work with keys in cleartext.

- Hardware examples
  - MCU-specific crypto accelerators
  - CryptoCell 312
  - Sometimes also secure elements (e.g. hashing)
- Implement for at least one device
- Standardize in PSA Crypto 1.x

How to work with us

How to work with us

Work with us on GitHub or via email.

- GitHub
  - Good for public communication
  - Good for code contributions
  - https://github.com/ARMmbed/mbedtls
  - https://github.com/ARMmbed/mbed-crypto
  - https://github.com/ARMmbed/mbed-os
- Email
  - Good for confidential communication
  - support@mbed.com
  - mbed-crypto@arm.com

Thank You!

Danke!

Merci!

谢谢!

ありがとう!

Gracias!

Kiitos!

תודה

arm