##############################

Trusted Firmware M - ~~v1.0-beta~~ v1.0-RC1

##############################

Trusted Firmware M provides a reference implementation of secure world software for ARMv8-M.

.. Note::

  The software implementation contained in this project is designed to be a reference implementation of the ~~Arm~~ Platform Security Architecture (PSA). It currently does not implement all the features of that architecture, however we expect the code to evolve along with the specifications.

Terms ``TFM`` and ``TF-M`` are commonly used in documents and code and both refer to ``Trusted Firmware M.`` :doc:`Glossary </docs/glossary>` has the list of terms and abbreviations.

#######

License

#######

The software is provided under a BSD-3-Clause :doc:`License </license>`.
Contributions to this project are accepted under the same license with developer sign-off as described in the :doc:`Contributing Guidelines </docs/contributing>`.

This project contains code from other projects as listed below. The code from external projects is limited to ``app`` and ``platform`` folders.
The original license text is included in those source files.

- The ``platform`` folder currently contains drivers imported from external project and the files have Apache 2.0 license.

- The ``app`` folder contains files imported from CMSIS_5 project and the files
  have Apache 2.0 license.
- The ``bl2`` folder contains files imported from MCUBoot project and the files
  have Apache 2.0 license.

.. Note::
   Any code that has license other than BSD-3-Clause is kept in specific sub
   folders named ``ext`` so that it can isolated if required.

############
This Release
############
This release includes:

- A Secure FW with support for PSA Level 1 and 2 isolation on ARMv8M.
- The Interfaces exposed by the Secure FW to NS side.
- A ~~blocking~~ secure fw model with NS application example.
- Secure services running within this SPE:

  - Secure Storage Service (Protected Storage PSA API - 1.0-beta-2)
  - Attestation (PSA API 1.0-beta-0)
  - Crypto Service (PSA API 1.0-beta-1)
  - TF-M Audit Log
  - Platform Service
  ~~- Secure Storage Service~~

- PSA IPC support
- Support for ARMv8-M mainline and baseline
- Testcases running baremetal and with RTX to test the functionality.

Formatted: Italian (Italy)
Formatted: Italian (Italy)
Formatted: Italian (Italy)
Formatted: Italian (Italy)

- Basic support for higher level isolation but it is
  ``in progress with limited testing``.
- BL2 bootloader for image authentication based on SHA256 and RSA-2048
  digital signature.
- Build system based on cmake, supporting armclang and GNU Arm.

~~**********~~

~~In progress~~

~~**********~~

~~- Ongoing and incremental support for PSA features:~~

~~ - Level 2 and 3 PSA isolation~~

~~ - PSA IPC support~~

~~ - Bootloader enhancements~~

~~ - ...~~

~~- OS support and use case examples:~~

~~ - mbed OS upstream support~~

~~ - mbed cloud client examples~~

~~ - ...~~

~~- Ongoing security hardening, optimization and quality improvements.~~

****

Platforms

****

Current release has been tested on:

- Cortex M33 based SSE-200 system:

  - `FPGA image loaded on MPS2 board.

    <https://developer.arm.com/products/system-design/development-boards/cortex-m-prototyping-systems/mps2>`__

  - `Fast model FVP_MPS2_AEMv8M.

    <https://developer.arm.com/products/system-design/fixed-virtual-platforms>`__

  - `Musca-A test chip board.

    <https://developer.arm.com/products/system-design/development-boards/iot-test-chips-and-boards/musca-a-test-chip-board>`__

  - `Musca-B1 test chip board.

    <https://developer.arm.com/products/system-design/development-boards/iot-test-chips-and-boards/musca-b-test-chip-board>`__

  - `FPGA image loaded on MPS3 board.

    <https://developer.arm.com/tools-and-software/development-boards/fpga-prototyping-boards/mps3>`__

- Cortex M23 based IoT Kit system:

  - `FPGA image loaded on MPS2 board.

    <https://developer.arm.com/products/system-design/development-boards/cortex-m-prototyping-systems/mps2>`__

################

Getting Started

################

****

Prerequisite

****

Trusted Firmware M provides a reference implementation of PSA specifications.
It is assumed that the reader is familiar with PSA concepts and terms. PSA
specifications are currently not available in the public domain.

The current TF-M implementation specifically targets TrustZone for ARMv8-M so a
good understanding of the v8-M architecture is also necessary. A good place to
get started with ARMv8-M is
`developer.arm.com <https://developer.arm.com/technologies/trustzone>`__.

****
Really getting started
****
Trusted Firmware M source code is available on `git.trustedfirmware.org
<https://git.trustedfirmware.org/trusted-firmware-m.git/>`__

To build & run TF-M:

- Follow the :doc:`SW requirements guide </docs/user_guides/tfm_sw_requirement>`
  to set up your environment.
- Follow the
  :doc:`Build instructions </docs/user_guides/tfm_build_instruction>` to compile
  and build the TF-M source.
- Follow the :doc:`User guide </docs/user_guides/tfm_user_guide>` for information
  on running the example.

To port TF-M to a another system or OS, follow the
:doc:`OS Integration Guide </docs/user_guides/tfm_integration_guide>`

Please also see the :doc:`glossary </docs/glossary>` of terms used in the project.

:doc:`Contributing Guidelines </docs/contributing>` contains guidance on how to contribute to this project.

Further documents can be found in the ``docs`` folder.

####################
Feedback and support
####################
For this early access release, feedback is requested via email to `support-trustedfirmware-m@arm.com <support-trustedfirmware-m@arm.com>`__.

################
Version history
################
+-------------+--------------+--------------------+
| Version | Date | Description |
+=============+==============+====================+
| v1.0-beta | 2019-02-15 | 1.0-beta release |
| v1.0-RC1 | 2019-05-31 | 1.0-RC1 release |
+-------------+--------------+--------------------+
