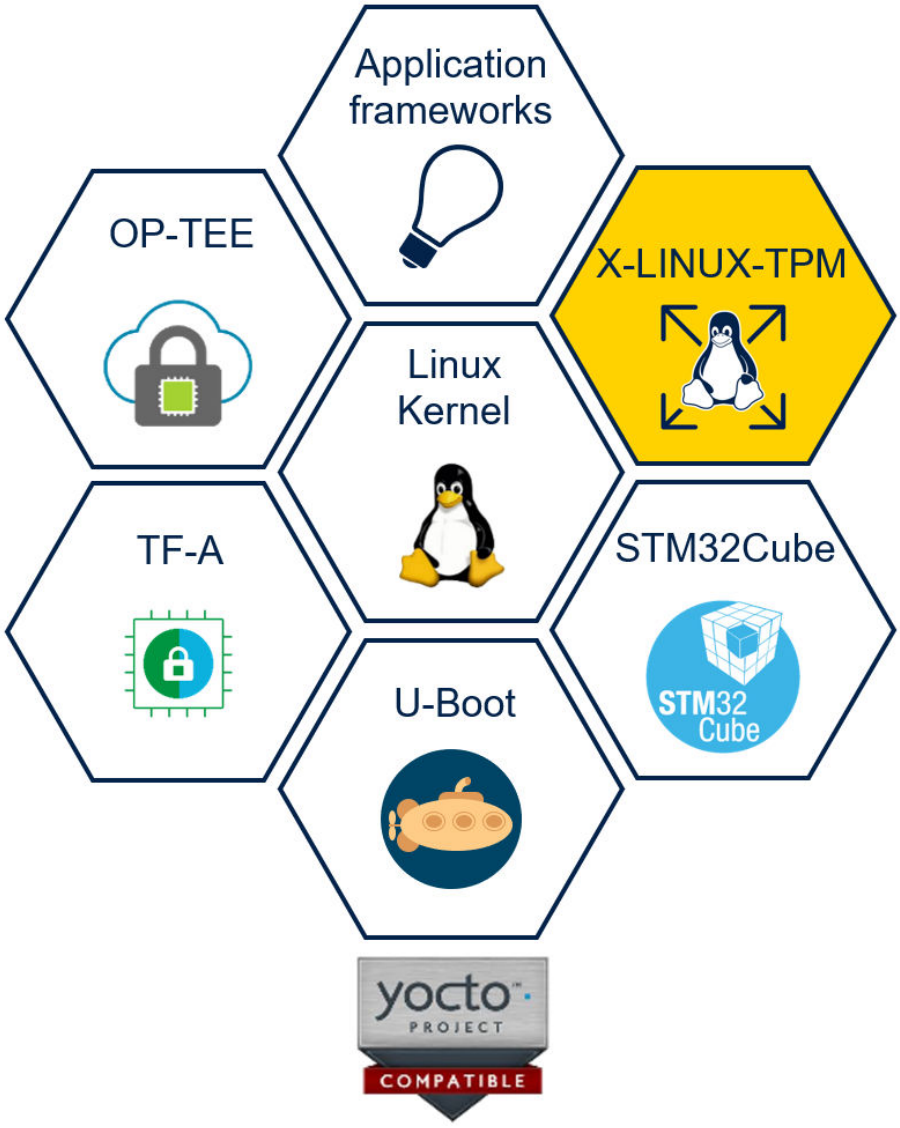
Trusted platform module Expansion Package for STM32 MPU OpenSTLinux



Product status link
X-LINUX-TPM

Features

- Integration of the STSAFE-TPM trusted platform module 2.0 based on ST33KTPM and ST33HTPH2Xxxx devices
- Support for SPI and I^2C
- Integration of the TPM software stack (`libtss`), TPM2 tools, and OpenSSL
- Validated with the STM32 MPU evaluation tools STM32MP135F-DK, STM32MP157F-DK2, and STM32MP257F-EV1
- Validated with the STSAFE evaluation boards STPM4RasPI and STPM4RasPIV21

Description

The X-LINUX-TPM OpenSTLinux Expansion Package provides the software add-ons for the integration of the STSAFE-TPM trusted platform module into the STM32 MPU OpenSTLinux Distribution. The typical services provided by TPM 2.0 are:

- Cryptographic keys generation, protection, management, and usage
- Cryptographic device identity
- Device attestation
- Measured boot
- Secure storage
- Other functions including hashing, random number generation, and secure clock

The STSAFE-TPM product benefits from Common Criteria, FIPS 140, and TCG certifications.

1 General information

The X-LINUX-TPM Expansion Package runs on STM32 microprocessors based on Arm® Cortex® processors.

Note: Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

1.1 Ordering information

X-LINUX-TPM is available for free download from the *www.st.com* website.

1.2 Versioning

The major and minor versions of the X-LINUX-TPM OpenSTLinux Expansion Package are aligned on the major and minor versions of the OpenSTLinux Distribution. This prevents painful backward compatibility attempts and makes dependencies straightforward.

The X-LINUX-TPM generic versioning vx.y.z is built as follows:

- **x**: major version matching the OpenSTLinux Distribution major version. Each new major version is incompatible with previous OpenSTLinux Distribution versions.
- **y**: minor version matching the OpenSTLinux Distribution minor version. Each new minor version might be incompatible with previous OpenSTLinux Distribution versions.
- **z**: patch version to introduce bug fixes. A patch version is implemented in a backward-compatible manner.

1.3 License

X-LINUX-TPM is delivered under the *Mix Ultimate Liberty+OSS+3rd-party V1* software license agreement (SLA0048).

Software component license agreements

The software components provided in this package come with different license schemes. Refer to wiki.st.com/stm32mpu/wiki/X-LINUX-TPM_licenses for details.

Revision history

Table 1. **Document revision history**

Date	Revision	Changes
28-Oct-2024	1	Initial release.