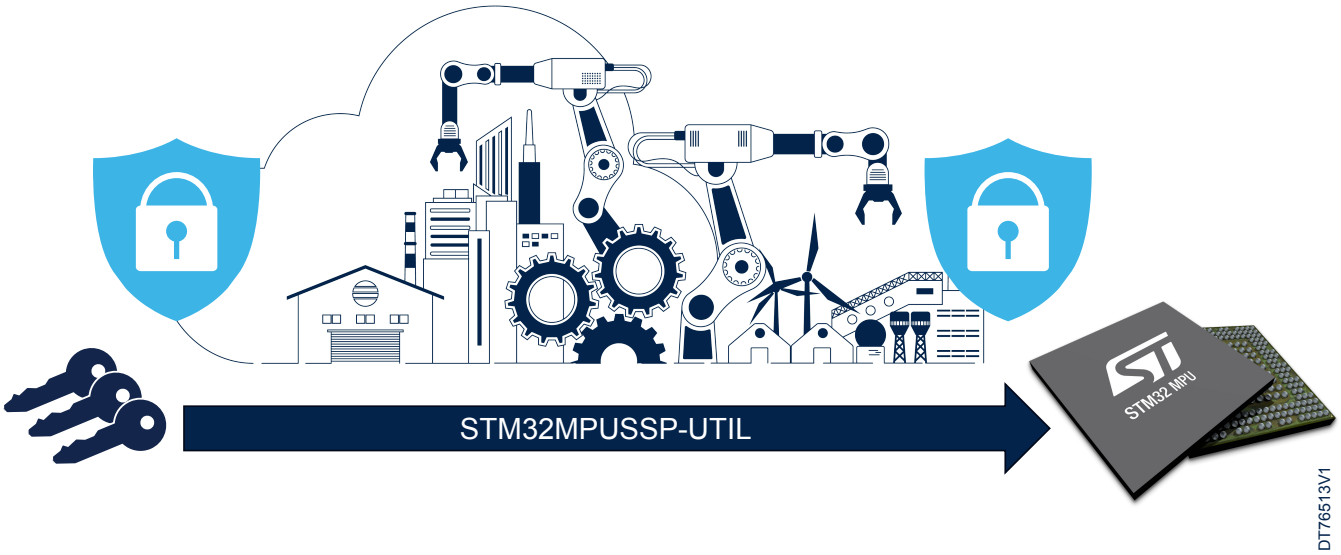
# STM32MPUSSP-UTIL

Data brief

## Secure secret provisioning (SSP) solution for STM32 microprocessors




| Product status link |
| --- |
| STM32MPUSSP-UTIL |

## Features

- Support for various services and API functions to integrate in the user's secure programming tool:
  - STM32HSM-V2 personalization data files
  - OEM secrets and keys programming into the OTP memory of STM32 MPUs
  - OEM RMA password programming into the OTP memory of STM32 MPUs
- Compatibility with STM32CubeProgrammer and STM32 Trusted Package Creator (STM32CubeProg) v2.18.0 and above
- Secure secret provisioning

## Description

STM32MPUSSP-UTIL is a solution for secure secret provisioning, protecting the transport of the original equipment manufacturer (OEM) keys from their generation to their storage in the STM32 microprocessor's internal memory during device manufacturing.

In the case of a device failure (return material authorization), STM32 MPUs feature a mechanism to reopen the device while maintaining protection on other secrets and keys. This mechanism is secured by a password that the OEM can program using STM32MPUSSP-UTIL.

Regulations, standards, or applications mandate the storage of keys in devices. These keys are sensitive assets that require protection during their generation, injection into the devices, and storage and use within the devices. The transport of these keys from their generation (such as in an HSM) to their injection into the MPUs (on the manufacturing line) represents a sensitive operation.

Outsourcing product manufacturing allows original equipment manufacturers to reduce direct costs and focus on high-value activities. However, contract manufacturing puts the OEM secrets at risk. Since the contract manufacturer (CM) handles the OEM's intellectual property (IP), it might be disclosed to other customers or appropriated.

To meet these security requirements and protect OEMs against any leakage of their IP, STMicroelectronics introduces a new security concept: Secure secret provisioning (SSP), represented by STM32MPUSSP-UTIL for STM32 MPUs. STM32MPUSSP-UTIL enables the secure programming of OEM secrets into the STM32 MPUs' OTP area, ensuring confidentiality, authentication, and integrity.

The STM32 MPUs support protection mechanisms that safeguard critical operations (such as cryptographic algorithms) and critical data (such as secret keys) against unauthorized access. SSP is a secure mechanism implemented in STM32 MPUs that enables the secure and controlled installation of OEM secrets in untrusted production environments.

SSP prevents:

- Access to OEM secrets by the contract manufacturer
- Extraction or disclosure of OEM secrets
- Over-manufacturing of OEM devices

SSP initiates device security processes, including the secure boot chain and authentication.

Information about SSP is available from various sources:

- The AN5510 application note about secure secret provisioning (SSP) on STM32 microprocessors
- The *Secure Secret Provisioning (SSP) overview* wiki page on wiki.st.com/stm32mpu
- The *How to deploy SSP using a step-by-step approach* wiki page on wiki.st.com/stm32mpu
- The STM32MPUSSP-UTIL product page on the *www.st.com* website

**Table 1. Applicable products**

| Type | Products |
|---|---|
| Microprocessors | • STM32MP1 series<br>• STM32MP2 series |
| Software development tool | STM32CubeProgrammer and STM32 Trusted Package Creator (STM32CubeProg) |
| Hardware tool | STM32HSM-V2 secure application module |

# 1 General information

STM32MPUSSP-UTIL is an SSP solution that applies to STM32 microprocessors based on the Arm® Cortex® processor.

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

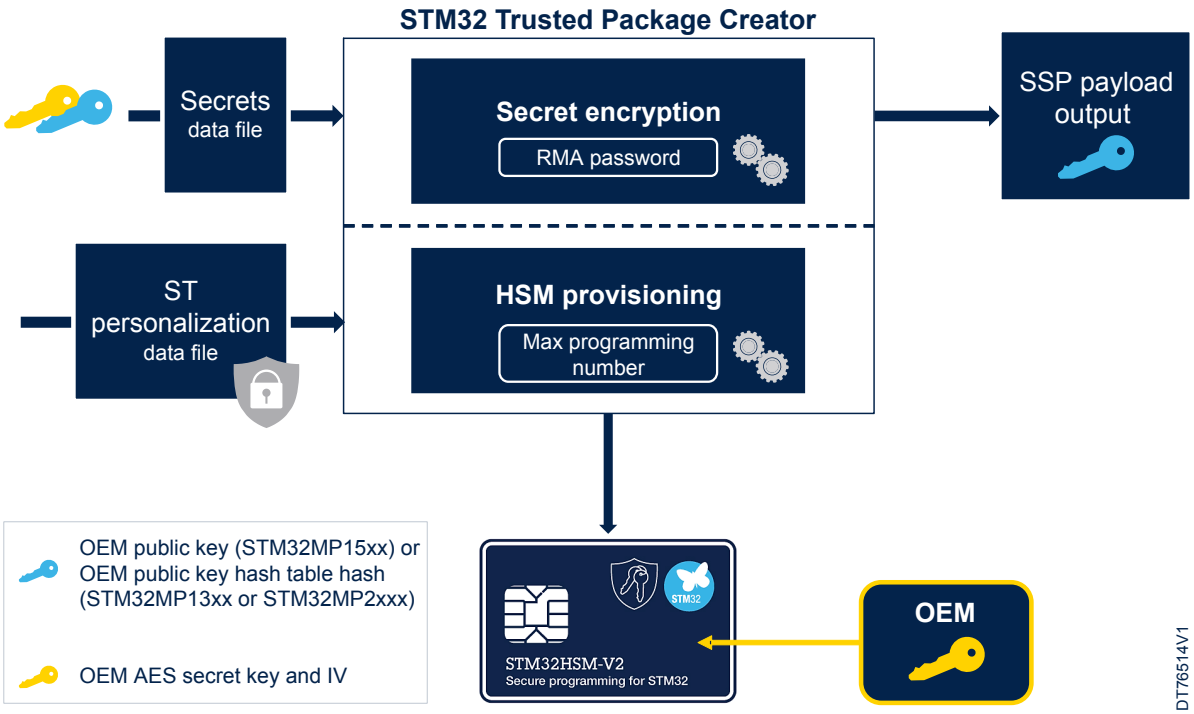
## 1.1 Ordering information

STM32MPUSSP-UTIL is available for free download from the *www.st.com* website.

## 1.2 Secure secret provisioning with STM32 Trusted Package Creator

Figure 1 illustrates the SSP setup using the STM32 Trusted Package Creator.

**Figure 1. SSP with STM32 TPC**



# 2 License

STM32MPUSSP-UTIL is delivered under the *ULTIMATE LIBERTY* software license agreement (SLA0044).

# Revision history

Table 2. **Document revision history**

| Date | Revision | Changes |
|---|---|---|
| 04-Dec-2024 | 1 | Initial release. |