PROEKSPERT

Software, design and data services

Secure Firmware Updaters on STM32 MCUs

A standalone **Secure Firmware Updater** provides secure offline, on-premise firmware (FW) updates for industrial devices. The product is designed to make secure FW updates, providing a security layer in front of a target device and using encrypted firmware, TrustZone® technology, and a secure element chip in the process to ensure only authentic tamper-free FW can be updated and taken into use.

Key features of Secure Firmware Updater

- Secure and tamper-proof FW update process
- Authentic FW verification
- USB / offline FW updating

Custom features:

- Custom integration with target device
- Custom FW updater logic
- Custom MCU flashing of the target device

Supported microcontrollers and hardware

Security features of Secure Firmware Updater

Family	MCU device	Secure element	TrustZone®	Secure Boot	PCROP	Data signing	Data encryption
STM32F4	STM32F446RE	STSAFE-A110	N/A	Custom feature	Yes	Yes	Yes
STM32U5	STM32U575ZI	STSAFE-A110	Yes	Yes	N/A	Yes	Yes
STM32L5	STM32L552ZE	STSAFE-A110	Yes	Yes	N/A	Yes	Yes

Get in touch

Our experienced engineers can help assess and mitigate cyber risks concerning your product. Let's see if we are the right partner for you.

Read more on our website:

proekspert.com/blog/connected-products/secure-firmware-updaters-on-stm32-mcus

Terry London
Partner & Product Manager

terry.london@proekspert.ee

Terry London

Phone: +372 651 8700