life.augmented

Everything you need to know to implement security on STM32H5 MCUs

Security FAQ

STM32 Trust

Frequently Asked Questions around STM32H5 and security

1. STM32H5 security
2. STM32H5 hardware security
3. Security ecosystem
4. Secure Manager

life.augmented

1

STM32H5 security

1 Where can I find information about the STM32H5 and security?

Visit the STM32Trust webpage for information on the STM32 generic security framework.

More details are available on STM32 security solutions on our wiki site – Security.

Find all the information available, including security & ecosystem on the STM32H5 product page

2 Is the STM32H5 certified and where can I find latest certificates?

STM32H573 MCU targets SESIP3 and PSA level 3 certifications.

Certificates are only available from certification schemes: PSA & SESIP.

The random generator is compliant with NIST FIPS SP 800-90B – check for certificates here.

3 Does the STM32H5 implement security based on a standard?

The STM32H5 follows the Arm® Platform Security Assurance (PSA) standard associated with ST proprietary security IP.

4 Where can I report security issues on STM32?

A procedure for reporting issues around security is available in our PSIRT page

life.augmented

2

STM32H5 hardware security (1/3)

1 Where can I find information about STM32H5 hardware security?

More details are available on STM32 security solutions on our wiki site – Security.

Find all the information available, including security & ecosystem on the STM32H5 product page.

2 Are STM32H5 cryptographic algorithms protected against side channel attacks?

Yes, the STM32H5 embeds SCA protected hardware cryptographic accelerators. You can check the algorithm details providing these properties in the RM0481 resource.

3 Where can I find implementation examples and references of hardware security IP?

All implementation examples are available inside the STM32CubeH5 package.

4 What is ST-iRoT?

ST-iRoT is the immutable root of trust embedded inside the STM32H573 MCU.

5 Is it mandatory to use the ST-iRoT?

ST-iRoT is optional and can be bypassed. In this case, you require an OEM-iRoT.

life.augmented

2

STM32H5 Hardware security (2/3)

6 Which product lifecycle is available on the STM32H5?

STM32H5 uses product states as defined by Arm® Platform Security Assurance (PSA).

RDP legacy mechanism is no more supported on the STM32H5. Please refer to the RM0481 for details.

7 What is the debug authentication mechanism for?

It allows you to reopen the debug using a certificate authentication mechanism.

8 What is the password regression mechanism for?

It enables a full part regression to its original state, removing all the device's programmed information.

9 What is an HUK on the STM32H5?

An HUK is a hardware unique key, derived from product state and other secrets. It is used to protect keys and secrets.

10 Is there a device certificate on the STM32H5 to attest that the device is unique?

Yes, several certificates are programmed in the ST production facilities.
They can only be used with the Secure Manager attestations services.

life.augmented

3

Security Ecosystem

1	**Where can I find information about the STM32H5 security ecosystem?**
Information is available on our wiki Security for STM32H5.	
The STM32H5 product page lists all available material including security & ecosystem.	
STM32Cube gathers most of our ecosystem tools & implementations.	
2	**Do you have implementations or references for cloud solutions?**
Azure middleware and cloud solutions are available at X-CUBE-AZURE-H5.	
AWS middleware and cloud solutions are available at X-CUBE-AWS-H5.	
3	**Do you have a TF-M implementation on STM32H5?**
Not yet, the TF-M implementation drivers will be available on the TrustedFirmware Github at a later stage. Check for updates on www.st.com.	

life.augmented

4

STM32Trust TEE Secure Manager (1/3)

1 What security challenges does the STM32H5 solve for developers?

It reduces cost of security by reducing the level of expertise required for security implementations, easing certifications and maintenance. It lets developers speed up their time to market, while reducing the cost of securing manufacturing flows.

2 What is the difference between SMAK and SMDK?

SMAK supports the development of applications using Secure Manager services.

SMDK supports the development of secure modules or trusted apps.

3 What STM32Trust security functions does the Secure Manager meet?

The Secure Manager linked to the STM32H5 covers all 12 STM32Trust security functions.

4 How can users develop an application using SMAK?

Download the STM32CubeH5 package and the Secure Manager binary and follow our wiki page on Getting started with STM32H5 security.

life.augmented

4

STM32Trust TEE Secure Manager (2/3)

5 Is it mandatory to use the Secure Manager on the STM32H573 MCU?

No, it is only optional. The Secure Manager can be installed at a later stage on the STM32H573 MCU.

6 How much does Secure Manager cost on the STM32H573?

There is no additional cost for using the Secure Manager on STM32H573.

7 What is the footprint associated with the use of the Secure Manager?

They depend on user configurations. You can read more on the Flash/RAM footprints here.

8 Is there a real-time impact of using secured modules inside the SPE?

Yes, there is. Check the SMDK documentation to understand the impacts in further details.

9 Is the Secure Manager subject to export control?

Export control classifications are the following: EU : 5D002.c.1 / USA : 5D002.c.1

4

STM32Trust TEE Secure Manager (3/3)

10 What does multitenant IP protection mean on the Secure Manager?

Multitenant IP protection refers to software IP coming from various sources or ownerships, cohabiting inside the same environment.

11 How is multitenant IP protection achieved on the STM32H5 with the Secure Manager?

IP confidentiality is protected during development, debugging, production, and in the field, thanks to secure update capabilities.

11 Where can I find performance information on the Secure Manager?

You can read performance details here.

life.augmented

Our technology starts with You

© STMicroelectronics - All rights reserved.
ST logo is a trademark or a registered trademark of STMicroelectronics International NV or its affiliates in the EU and/or other countries.
For additional information about ST trademarks, please refer to www.st.com/trademarks.
All other product or service names are the property of their respective owners.

life.augmented