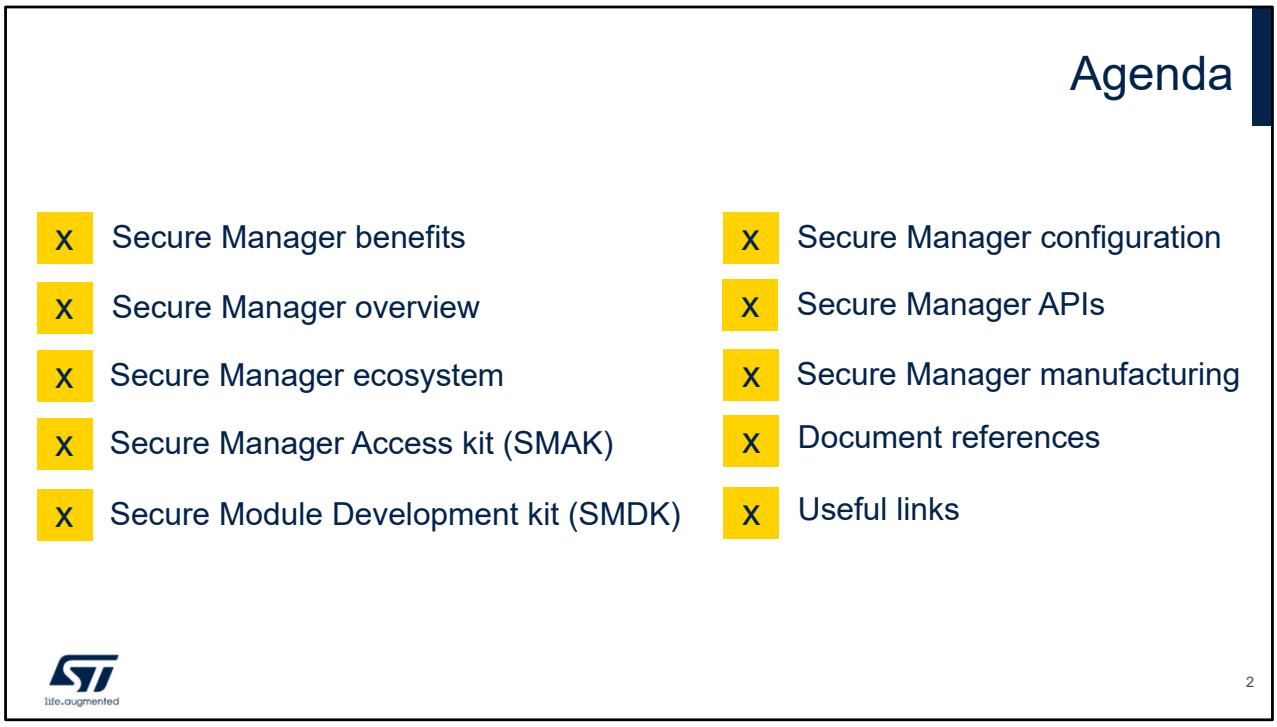
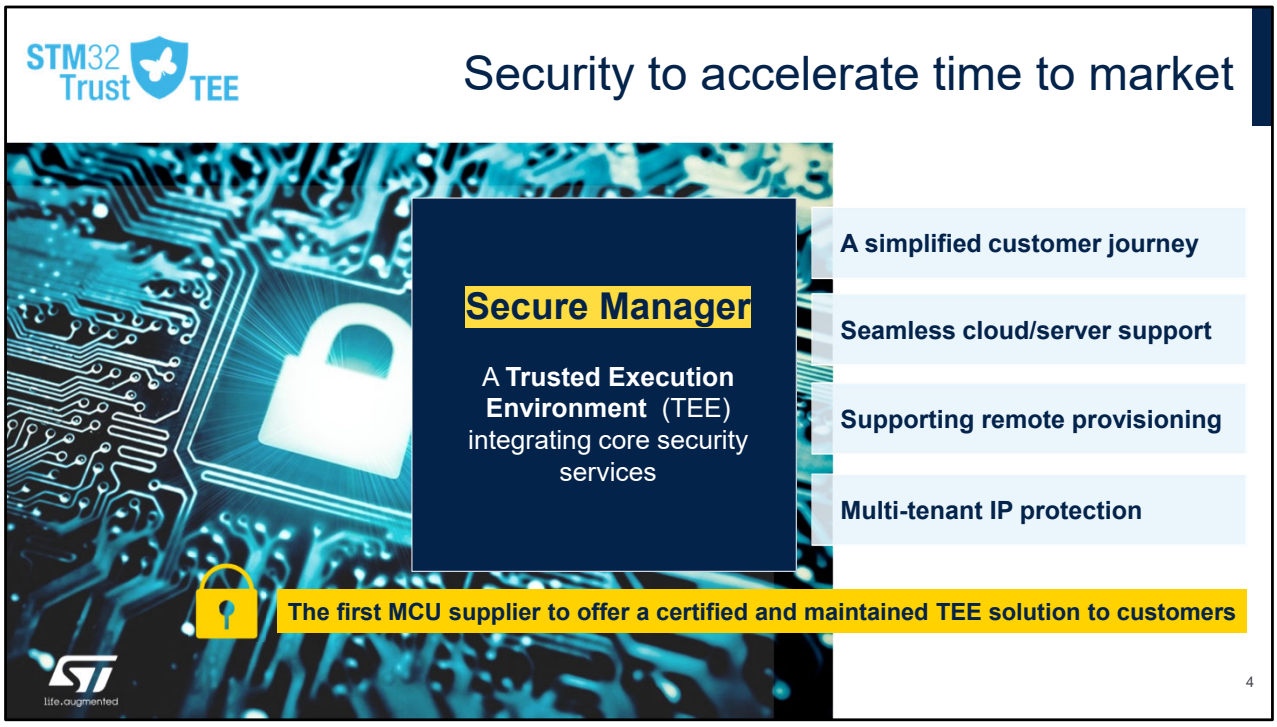
Hello and welcome to this presentation describing the STM32H5's security software component called Secure Manager.
The STM32 Trusted Execution Environment Secure Manager (STM32TRUSTEE-SM) is a suite of system-on-chip security solutions that simplifies the development of embedded applications to ensure ready to use security services.



This presentation looks at the following Secure Manager Topics:

- the benefits
- an overview
- the ecosystem
- the Access Kit or S.M.A.K
- the Development Kit or S.M.D.K
- the configuration
- A.P.is
- manufacturing
- related document references
- useful links

So, let’s start by reviewing our security strategy to increase the level and the accessibility of security solutions embedded into our newest STM32 products.



ST has identified an opportunity to offer a game-changing solution for our customer working on adding security to their applications.
ST will be the first MCU supplier to develop, certify and maintain a Trusted Execution Environment turnkey solution: the Secure Manager.
This is where ST fills these gaps and brings a security offer, for fast time to market, which is scalable, covering from pure Hardware security IP to full Security Services.
This solution reduces the security costs for the OEM.

Secure Manager simplifies the costumer journey by:
- Supplying turnkey TEE security solution including services
- Targeting security certified solution
- Abstracting TrustZone complexity

Secure Manager offers seamless cloud/server support by supplying:

- PSA compliancy
- Pre-provisioned keys and certificates
- Seamless cloud/server registration

Secure Manager offers remote provisioning by:

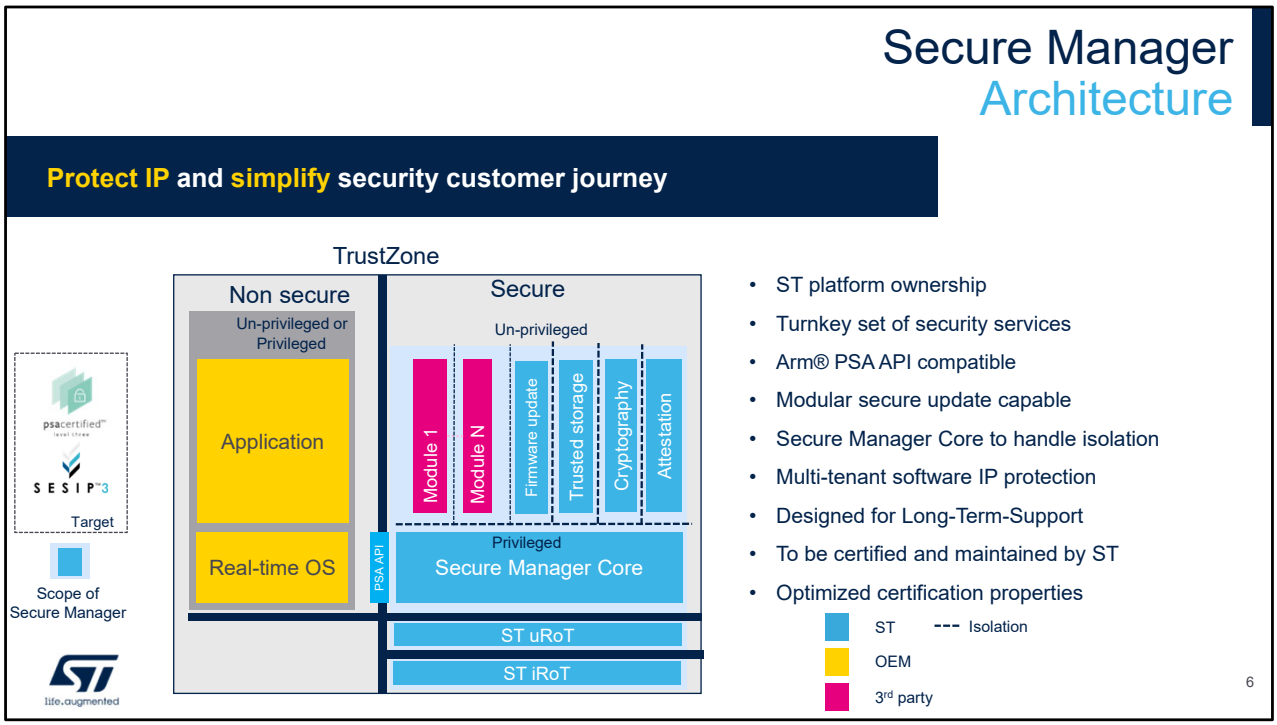
- Enabling remote PKI lifecycle management
- Enabling certificate installation, rotation, revocation

Secure Manager offers multiple-tenant IP protection by supplying:

- Isolation for confidentiality at installation and runtime
- Protected development flow for image creation and installation

Secure Manager overview

Let us now describe the Secure Manager.



What is the Secure Manager ?
The Secure Manager is an STMicroelectronics trusted execution environment security framework that is compliant with Arm® Platform Security Architecture (PSA) specifications for Cortex®-M (Armv8-M).
The Secure Manager is aiming at simplifying the security development cycle of embedded applications by providing ready to use security services developed according to best practices.
It is supported by our STM32.Cube ecosystem and can be installed easily installed on a selection of our STM32 devices.
The Secure Manager targets PSA level 3 and SESIP3 certification.

Secure Manager is executed in a Secure Processing

Environment (SPE).
It is responsible for Secure Boot and Secure Firmware Update, and it provides secure services to non-secure applications at runtime.
Secure Manager is composed of:
- A 2-stage Root of Trust
    - An immutable Root of Trust (STiRoT)
    - An updatable Root of Trust (STuRoT)
- The Secure Manager Core
- Secure Services such as
    - Cryptography
    - Initial attestation
    - Trusted storage
    - Firmware update

Additionally, trusted applications, also called secure modules, can be added by the user, but are not part of the Secure Manager.

Some important features:
- Secure Manager is owned and delivered by ST
- Secure Manager Core is used to isolate secure services
- Secure Manager supports multi-tenant IP protection
- Is ready to support multiple profiles
- And is PSA API compliant
- Secure Manager is designed for Long-Term Support, which means that ST insures Secure Manager maintenance and support
- Secure Manager is supplied with full secure update capabilities
- Secure Manager binary is ready for certification.

Secure Manager
Main features

	STM32H5
Profiles	**Large** (exhaustive set of features, crypto algo…)
PSA	ARM PSA standard and API compliancy
Secure Boot	2 level boot stages (1 immutable and 1 updatable)
PSA initial attestation API	Asymmetric key algorithm
PSA internal trusted storage API	ITS file system in user flash, encrypted, configurable size
PSA firmware update API	Yes, with independent secure module installation and udpate
PSA crypto API	AES, RSA, ECDSA, ECDH, HASH, HMAC, DES, Triple DES
ITS provisioning	Secure factory ITS provisioning, with key/data diversification
Software IP protection	Multiple-tenant software IP protection Sandboxed secure services (PSA level 3 isolation)
ST preprovisioned key and certificate	Key and X509 certificate for Initial Attestation Service Key and X509 certificate for User Service (TLS communication…)
System	Secure IRQ, secure DMA, FPU (NSPE)
Security certification target	PSA Certified L3, GlobalPlatform SESIP3
Development kits	Secure Manager Access Kit (SMAK) Secure Module Development Kit (SMDK)

life.augmented

7

The current version of Secure Manager supports an exhaustive set of features, for example exhaustive crypto algorithm sets. It corresponds to the Large profile. Note that additional profiles will be proposed in the next Secure Manager versions to fulfil specific customer requirements.

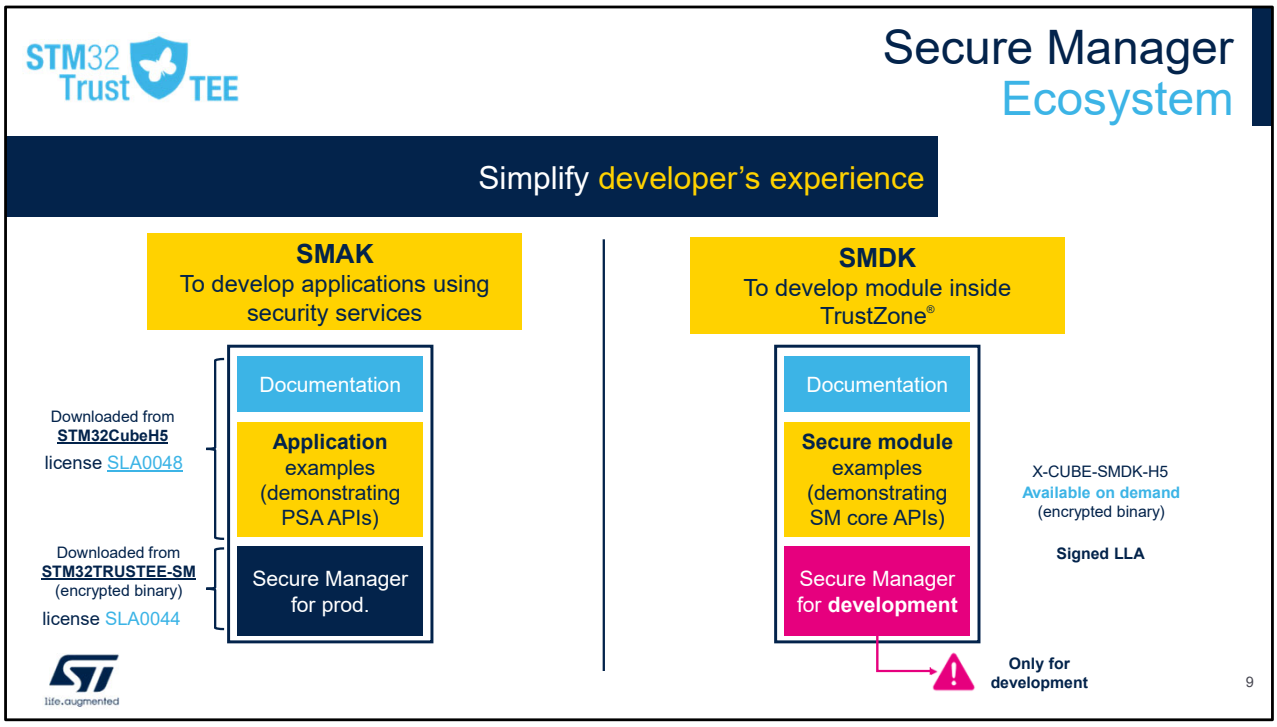
Main Secure Manager features are:

- Compliance with PSA standard and PSA standard APIs
- 2 level boot stages
- PSA initial attestation, with asymmetric key algorithm
- PSA internal trusted storage with encrypted file system of configurable size
- PSA firmware update, with independent secure module installation and update
- PSA cryptography with exhaustive crypto algorithm sets

- Secure factory ITS provisioning, including key/data diversification
- Multiple-tenant IP protection, with PSA level 3 isolation
- ST pre-provisioned X509 certificate and key
- Support of secure IRQ, secure DMA, and floating-point unit
- Security certification targeting PSA Certified Level 3 and GlobalPlatform SESIP3
- Secure Manager Access Kit (SMAK) and Secure Module Development Kit (SMDK)
    - Secure Manager Access kit to develop non-secure applications using Secure Manager services
    - Secure Module Development Kit for secure module development.

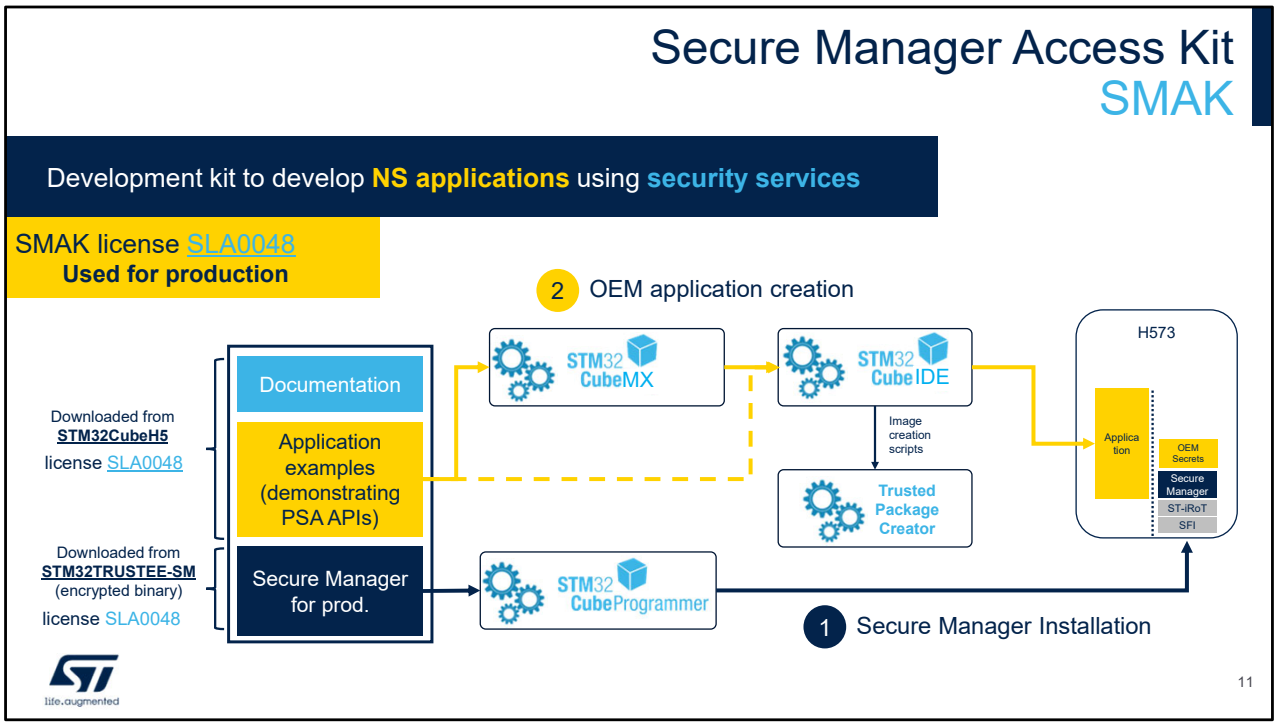
Secure Manager ecosystem

Let’s describe the Secure Manager ecosystem.



The Secure Manager encompasses two types of packages : the Secure Manager Access Kit (SMAK) and the Secure Module Development Kit (SMDK).
The Secure Manager Access Kit (SMAK) is used to develop non-secure application using Secure Manager security services via the standard PSA API.
The Secure Module Development Kit (SMDK) is used to develop trusted applications, also called secure modules.
Both development kits are delivered with a full set of tools, software, documentation and examples.

Let’s start with the Secure Manager Access Kit.



The SMAK provides the environment to develop non-secure application that uses the Secure Manager services.
It is composed of:

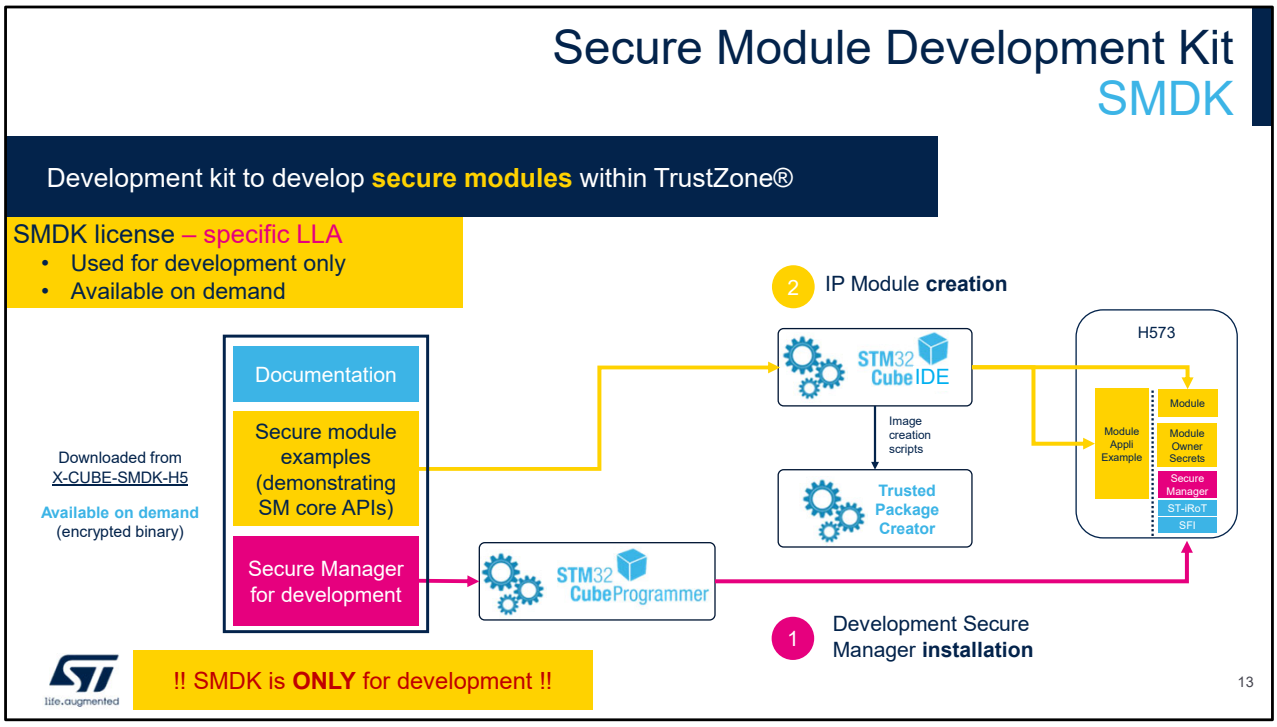
- Secure Manager, available as an encrypted image from st.com (STM32TRUSTEE-SM)
  - It is delivered under the SLA0048 software license agreement.
  - It can be used for production purposes
- STM32Cube embedded firmware package containing:
  - Templates and examples to develop a non-secure application
  - Scripts to provision/install the Secure Manager
- STM32 Trusted Package Creator to build signed and encrypted images
- STM32CubeProgrammer to program signed and encrypted

images
- STM32CubeMX to configure and generate non-secure application code (using Secure Manager APIs)
- IDEs (STM32CubeIDE, IAR or KEIL).

Once downloaded, SMAK allows the :
- Creation of the OEM application
- Installation of Secure Manager
- Installation and debug of the OEM application

Detailed documentation can be found in the user manual and wiki.

Let’s now present the Secure Module Development Kit (SMDK).



The SMDK provides the environment for developing secure modules.
The SMDK is composed of:

- Secure Manager, available as an encrypted image from st.com (STM32TRUSTEE-SM)
    - It must be used for development purposes only.
    - It features UART trace capability.
    - It is available under a signed license agreement - Contact your ST representative.
- STM32Cube embedded firmware package containing templates and examples to develop a secure module
- STM32 Trusted Package Creator to build signed and encrypted images
- STM32CubeProgrammer to program signed and encrypted images

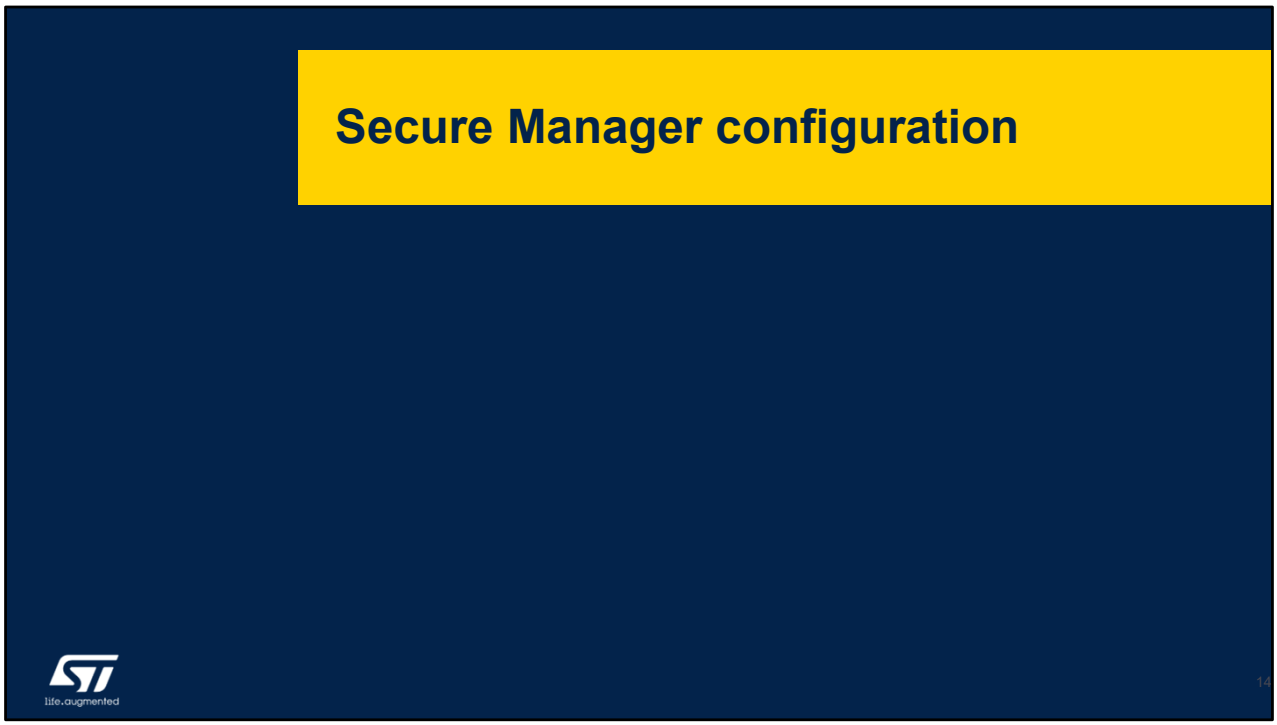
- IDEs

The SMDK can also be used to securely install and update secure modules.

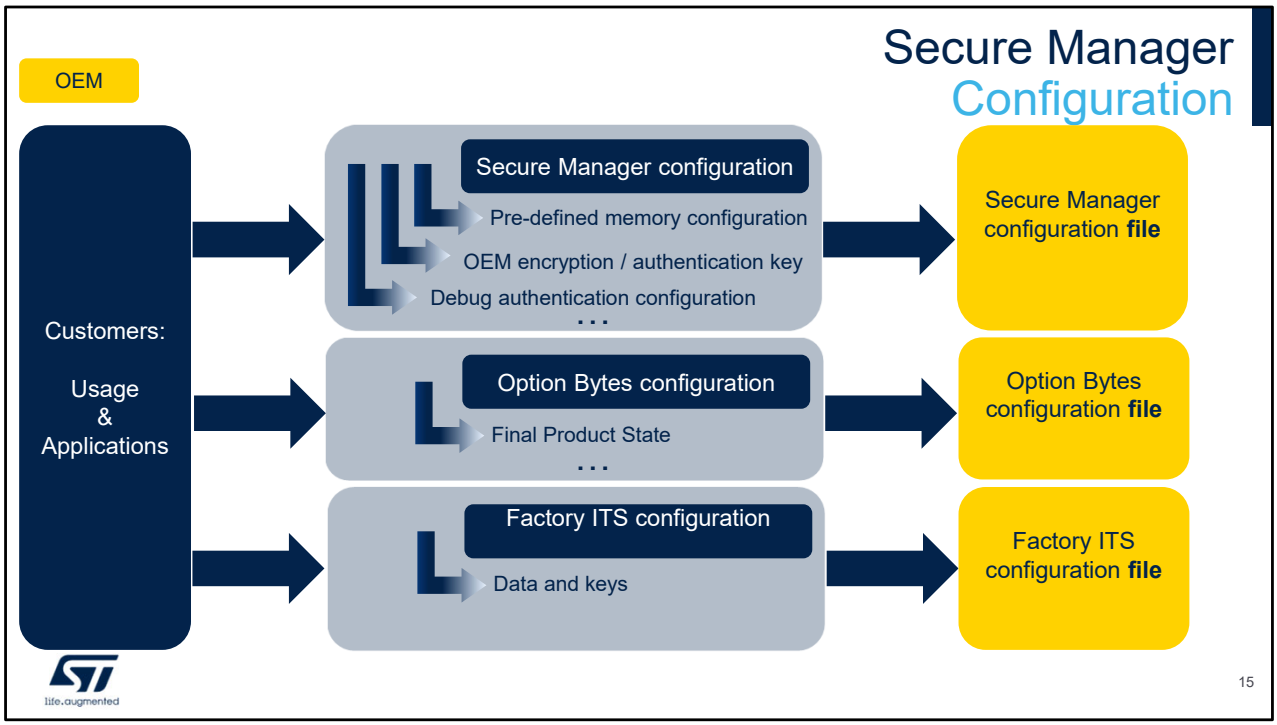
Once downloaded, SMDK allows the:

- Creation of the OEM application and IP module
- Installation of Secure Manager
- Installation and debug of the OEM application and IP module

Detailed documentation can be found in the user manual and wiki.



Before using the Secure Manager, the OEM should configure it.



This slide shows how the OEM can configure the Secure Manager.
This configuration is done once during the initial Secure Manager installation.
This configuration is optional as Secure Manager is supplied with default configuration parameters.

First, the OEM defines the Secure Manager configuration parameters to generate the Secure Manager configuration file:

- For example, the following configuration parameters must be selected:
  - The Secure Manager pre-defined memory configuration (who defines how if Secure modules are supported…),
  - The OEM firmware encryption and authentication keys

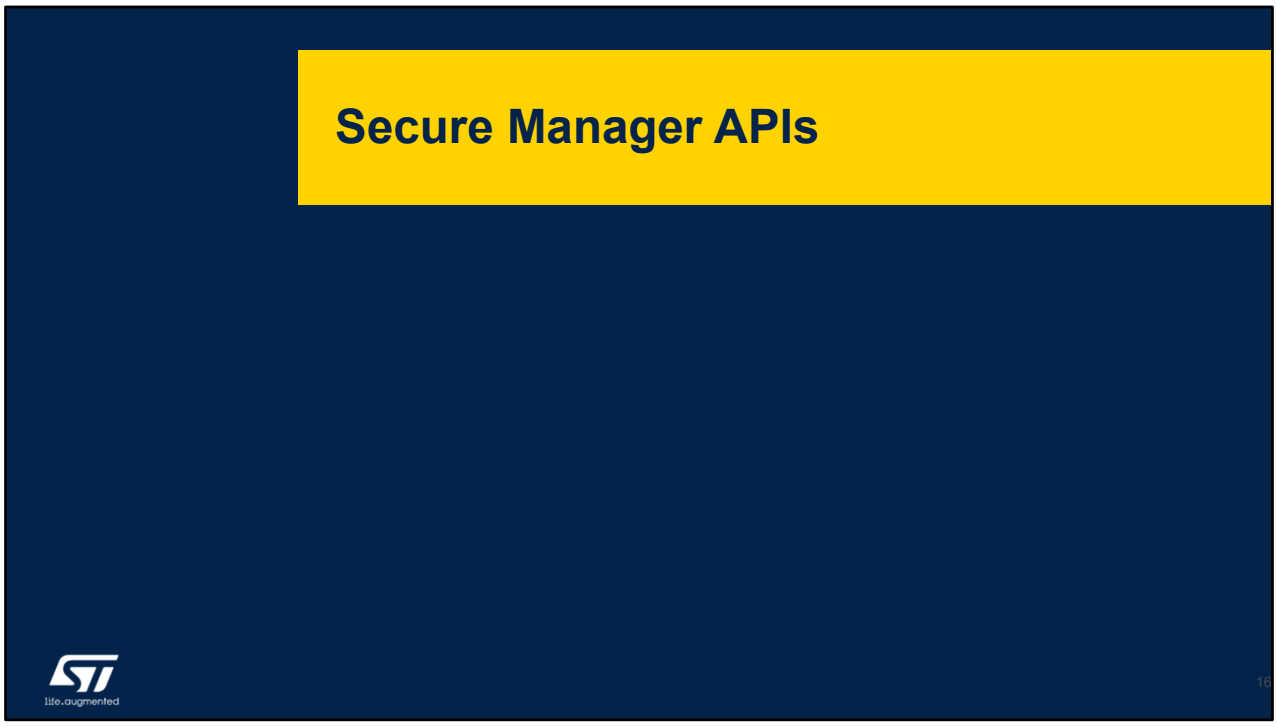
- The Debug authentication configuration (permission for non-secure debug opening, regression…).

Then, the OEM defines the STM32 device configuration

- Selection of the Option Bytes values, for example the final product state.

Finally, the OEM defines the factory internal trusted storage (ITS) provisioning values

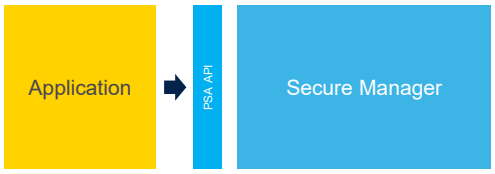
- Definition of key and data to securely provision in the ITS file system.



Once configured, the OEM can use Secure Manager using PSA standard Secure Manager APIs.

Secure Manager APIs

- Current Arm® PSA API versions supported
  - https://arm-software.github.io/psa-api/
    - PSA Attestation API 1.0.2 (ARM IHI 0085)
    - PSA Cryptography API 1.0.0 (ARM IHI 0086)
    - PSA Storage API 1.0.0 (ARM IHI 0087)
    - PSA Firmware Update API 0.7 Beta0 (ARM IHI 0093)
- Secure Manager detailed API description (included in STM32cubeH5)
  - ./Middlewares/ST/secure_manager_api/SecureManagerAPI.chm



life.augmented

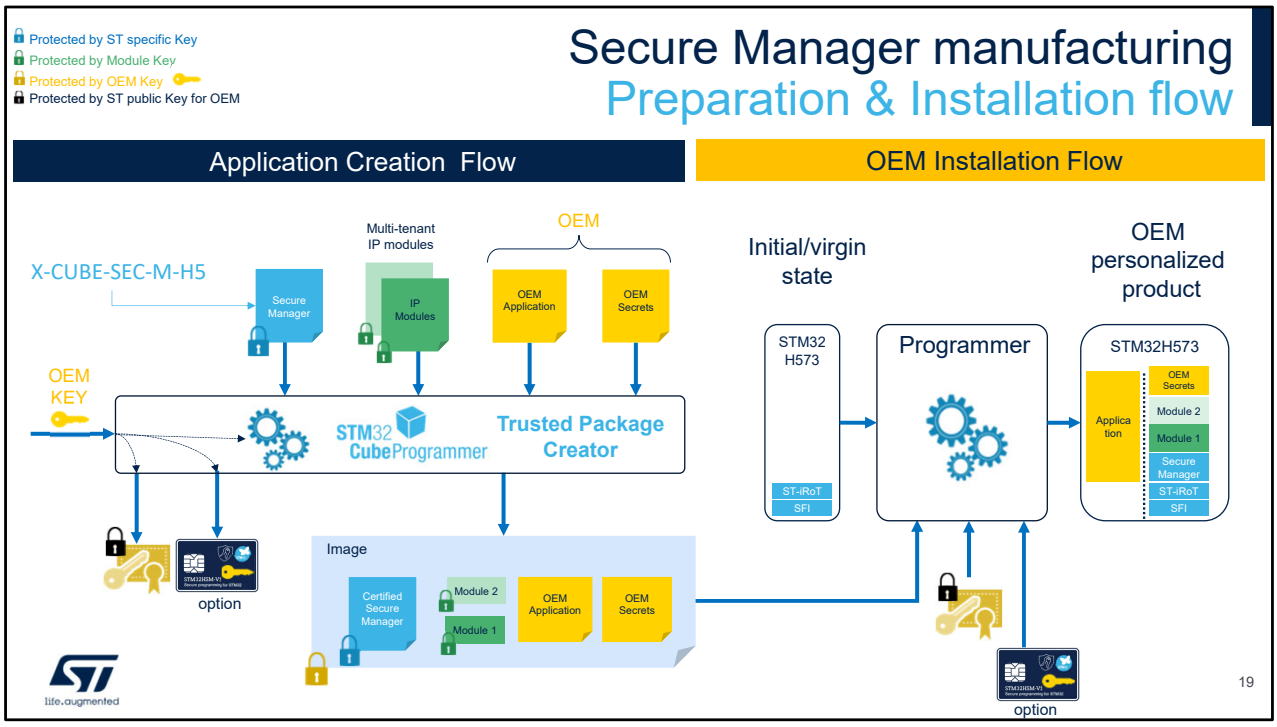
17

The Secure Manager security services are easy to use as they are compliant with standard Arm PSA APIs.

The following PSA standard APIs are supported and can be used by the non-secure application:
- PSA attestation API
- PSA cryptography API
- PSA storage API
- PSA firmware update API.

Secure Manager detailed APIs are described in the following documents:
- PSA standard API documentation (available on github)
- Detailed ST API description (available in STM32cubeH5 in Secure Manager API middleware).

The Secure Manager is also supplied with a full ecosystem for Secure Manager manufacturing, including OEM application and IP modules.
Let’s take a look at this.



ST provides the environment for Secure Manager manufacturing.

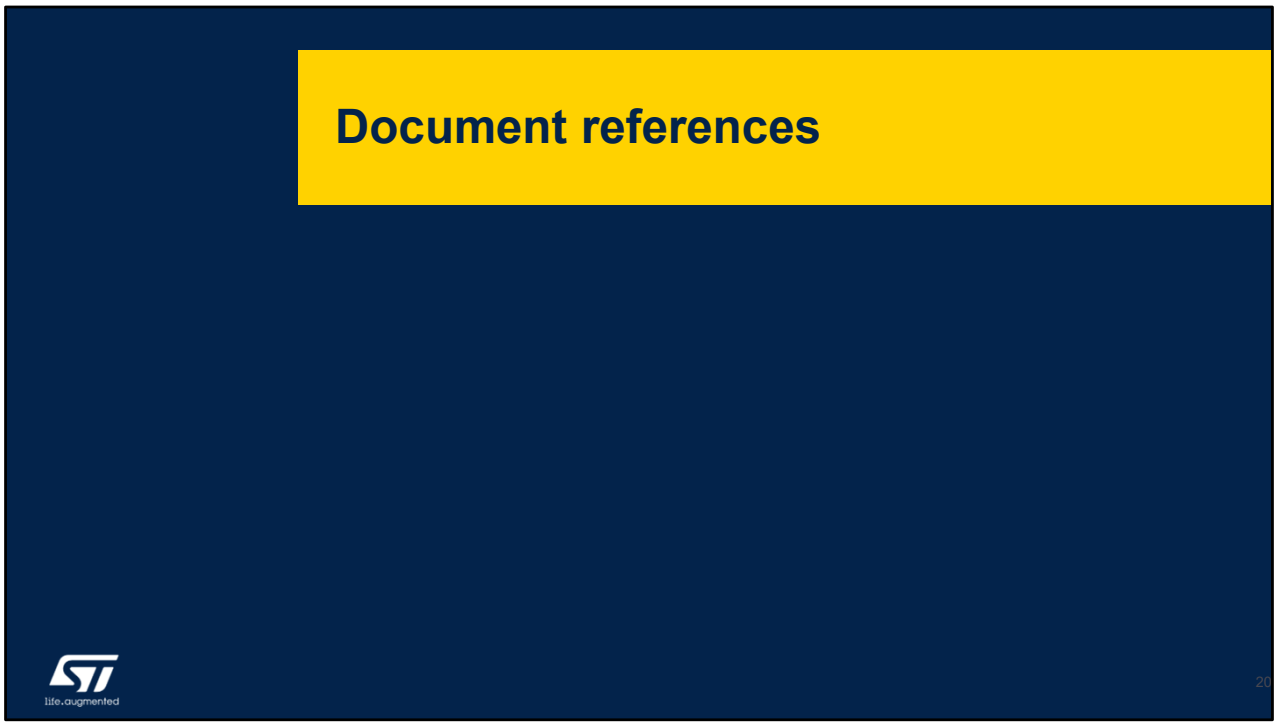
This environment is composed of:
•STM32 Trusted Package Creator to build signed and encrypted images
•STM32CubeProgrammer to program signed and encrypted images. Note that for the final manufacturing setup, the OEM must replace the STM32CubeProgrammer by the Programming tool.
•STM32HSM to protect the OEM encryption key and allow device installation counting.

The Secure Manager manufacturing flow is composed of 2 phases:

- Application creation flow done at OEM trusted offices
- Application installation flow done at OEM manufacturing.

During Application creation flow
- The OEM integrator gets all firmware
    - ST Secure Manager
    - Third party IP modules
    - OEM Application, secrets and IP modules (to be noticed that secrets are composed of configuration data and keys, ITS data and keys, and option bytes values)
- The OEM builds encrypted images containing all these firmware, using the STM32TrustedPackageCreator. The OEM uses their own key to generate this encrypted image and ensure their asset confidentiality.
- Optionally, the OEM can use the STM32HSM Hardware Security Module:
    - To protect their encryption key,
    - To generate installation licenses and control the number of devices programmed with their firmware in an untrusted programming location
    - This installation procedure is called SFI (Secure Firmware Installation) which is already deployed on other STM32 families.

During application installation in untrusted OEM manufacturing:
- The OEM gets STM32H573 device from ST
- The OEM gets encrypted firmware from their OEM trusted offices
- Optionally, the OEM gets the STM32HSM hardware security module a way to control the number of devices programmed with their firmware
- The OEM securely installs the encrypted firmware using their programmer tool.



Let’s now present references to detailed documentation.

Document references (1)

- Secure Manager wiki
  - Secure Manager
    - https://wiki.st.com/stm32mcu/wiki/Security:Secure_Manager
  - Secure Manager for STM32H5
    - https://wiki.st.com/stm32mcu/wiki/Security:Secure_Manager_for_STM32H5
  - SMAK for STM32H5
    - https://wiki.st.com/stm32mcu/wiki/Security:SMAK_for_STM32H5
  - SMDK for STM32H5
    - https://wiki.st.com/stm32mcu/wiki/Security:SMDK_for_STM32H5
    - For more information on SMDK, please contact STMicroelectronics (specific license needed)
  - Secure manufacturing for STM32H5
    - https://wiki.st.com/stm32mcu/wiki/Security:SFI_for_STM32H5
  - SMAK getting started for STM32H5
    - https://wiki.st.com/stm32mcu/wiki/Security:Secure_Manager_STM32H5_How_to_Intro
    - https://wiki.st.com/stm32mcu/wiki/Security:How_to_start_with_Secure_Manager_customized_config_on_STM32H5
    - https://wiki.st.com/stm32mcu/wiki/Security:How_to_start_with_Secure_Manager_default_configuration_on_STM32H5

life.augmented

21

The main documentation is available on wiki to describe:

- Generic Secure Manager solution
- Secure Manager solution for STM32H5
- SMAK for STM32H5
- SMDK overview (more SMDK information is available under specific license)
- Secure manufacturing for STM32H5
- And SMAK how to and getting started.

Document references (2)

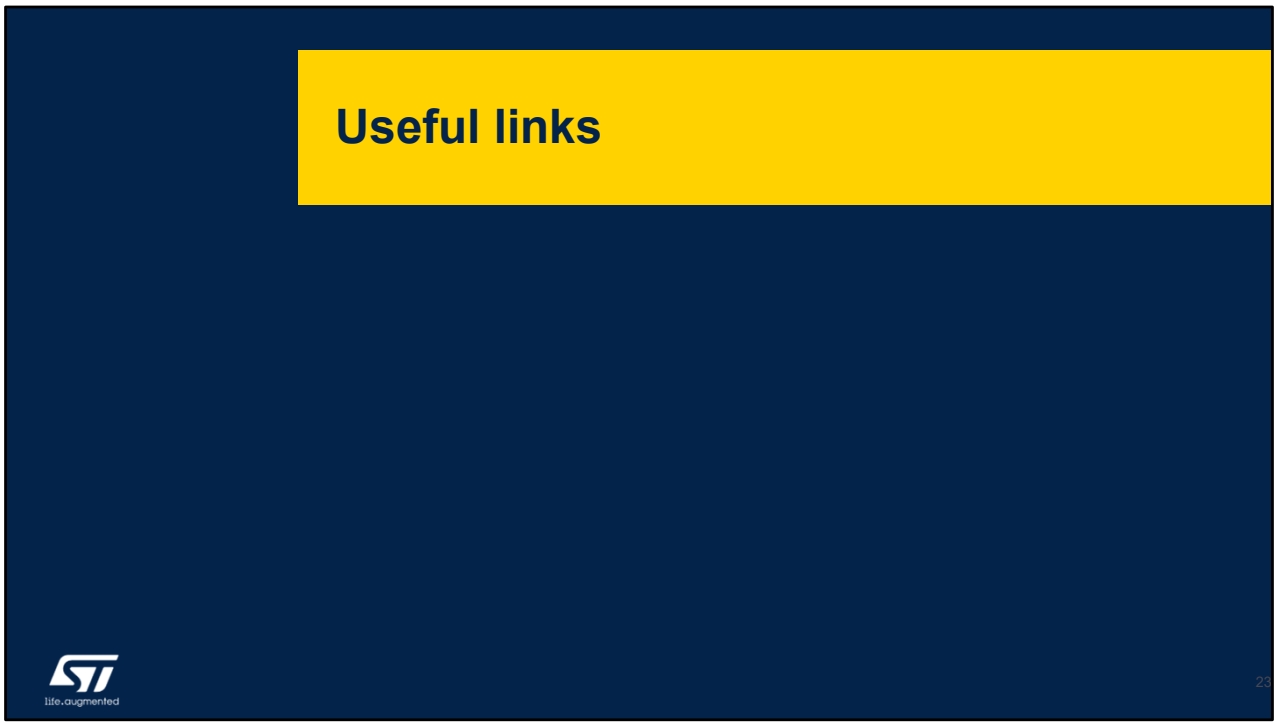
- Current Arm® PSA API versions supported
  - https://arm-software.github.io/psa-api/
    - PSA Attestation API 1.0.2 (ARM IHI 0085)
    - PSA Cryptography API 1.0.0 (ARM IHI 0086)
    - PSA Storage API 1.0.0 (ARM IHI 0087)
    - PSA Firmware Update API 0.7 Beta0 (ARM IHI 0093)
- Secure Manager detailed API description (included in STM32cubeH5)
  - ./Middlewares/ST/secure_manager_api/SecureManagerAPI.chm

life.augmented

22

Secure Manager APIs are described in the following documents:

- PSA standard API documentation (available on github)
- Detailed ST API description (available in STM32cubeH5 in Secure Manager API middleware).



Let us finish this presentation with some useful links related to Secure Manager and its ecosystem.

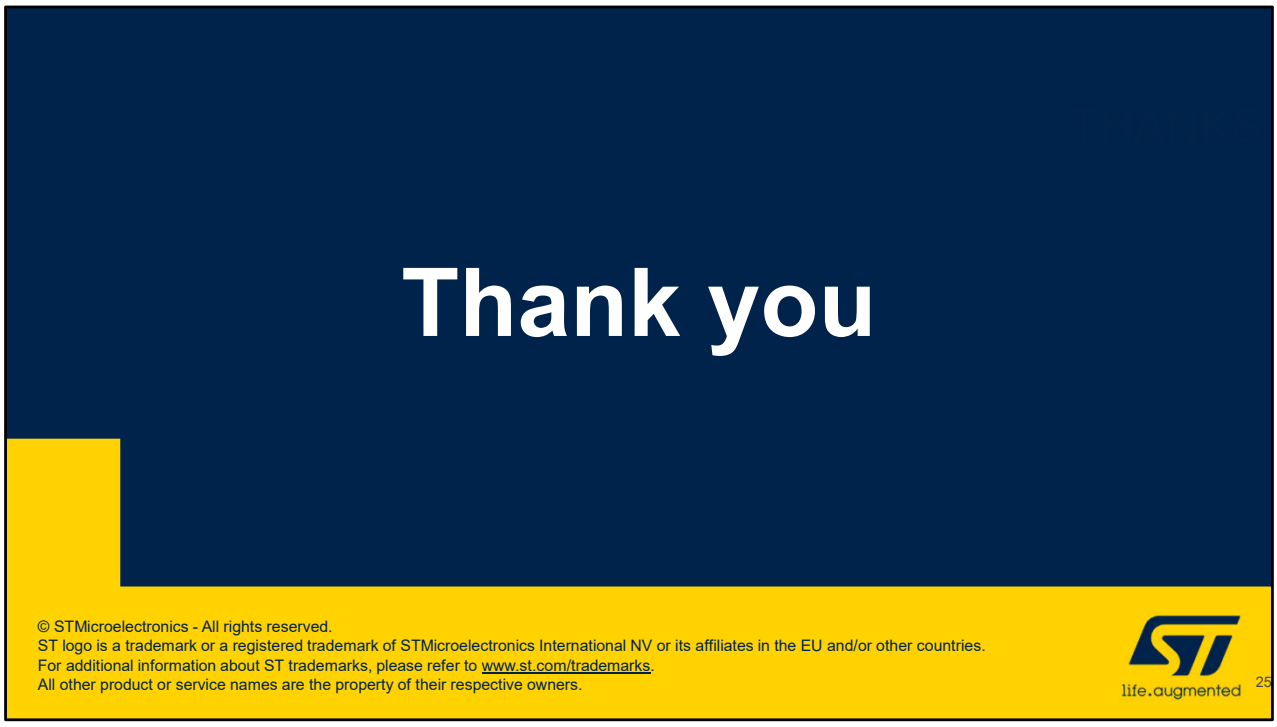
Useful links

- STM32Trust web page
- STM32CubeH5 – inc. API & SMAK examples
- STM32H5 RM0481
- STM32TrustTEE-SM web page
  - X-CUBE-SEC-M-H5 H5 SM binary
- On-line trainings
- X-CUBE-SMDK-H5 SMDK
- Discovery kit with STM32H573
- STM32H5 security FAQ
- Secure Manager Blog article
- IoT kits including Secure Manager
  - Azure X-CUBE-AZURE-H5
  - AWS X-CUBE-AWS-H5

life.augmented

To support development, a full set of documentation and tools are available.
A non exhaustive list is given on this slide to help developers find the information they require.
It starts with a generic solution overview through to deep technical information.
Getting started, on-line trainings and support via our ST Community are there to provide best class support.

Additionally, full implementations such as our IoT kits are also provided showing the Secure Manager integration, with seamless registration capabilities to Azure and AWS.



Thank you for attending this presentation on Secure Manager.
You can also refer to the following presentations:

- STM32H5 Security- Architecture overview
- STM32H5 Security - Debug Authentication Control
- STM32H5 Root Security Services.