life.augmented

Fast-track your embedded security journey

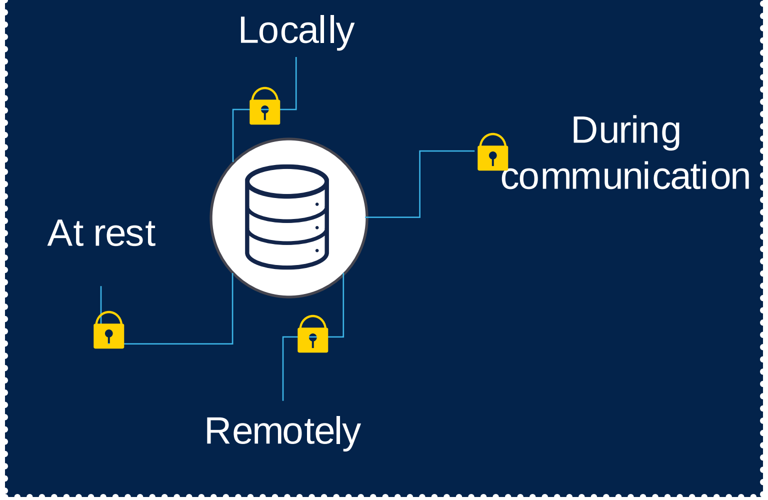
Discover the STM32Trust TEE Secure Manager for STM32H5 MCUs

STM32 Trust

STM32

Embedded security
What are developers typically trying to achieve?

Easily protect my critical data & secrets and those of my end customers



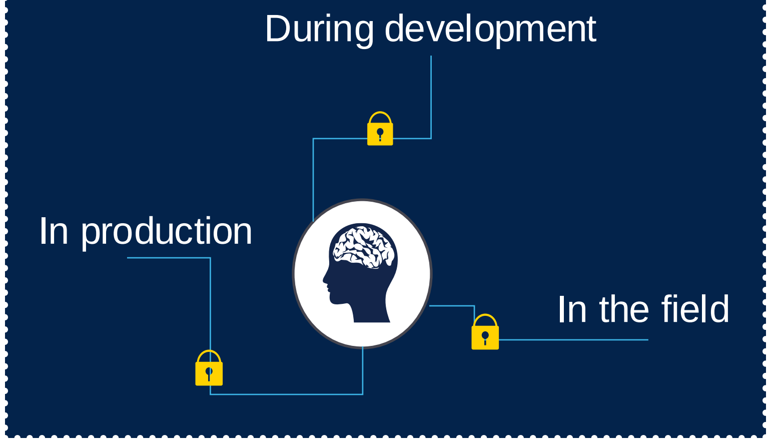
Locally

During communication

At rest

Remotely

Easily protect my IP and my partner’s IP in a strong and effective way

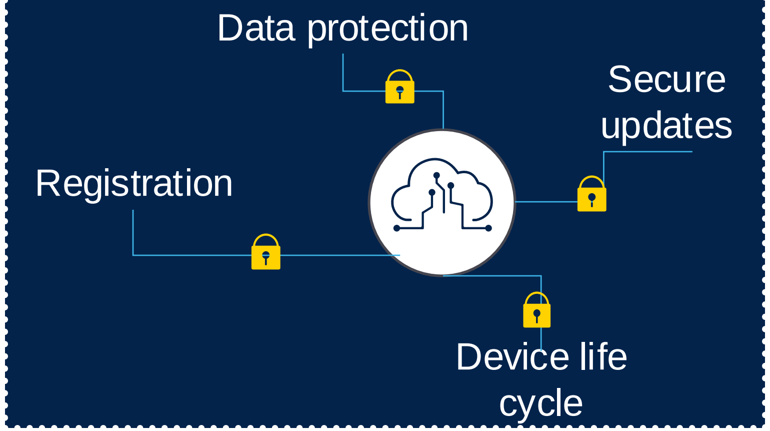


During development

In production

In the field

Easily & securely connect to clouds & servers without painful digital identities management



Data protection

Secure updates

Registration

Device life cycle

Discover the Secure Manager

Secure Manager

A **trusted execution environment** (TEE) integrating core security services

A set of turnkey security services developed, maintained, and certified by ST

Addressing your security requirements

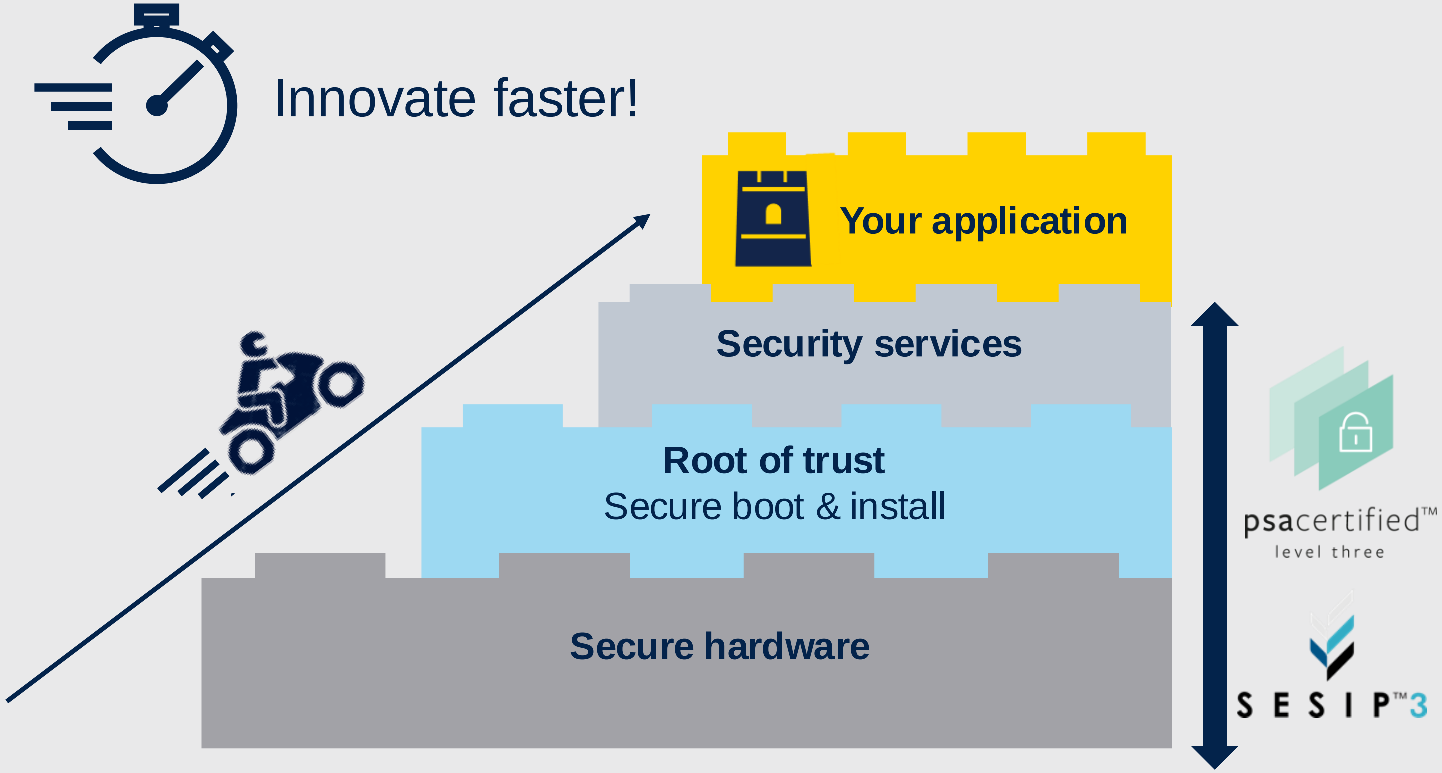
STM32H5 security offer

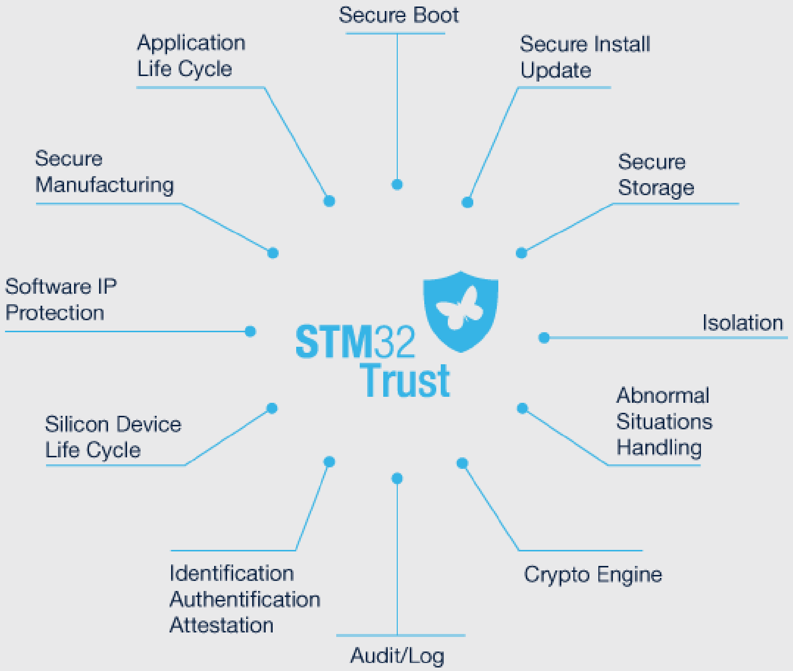
life.augmented

A scalable security offer to address your needs

Choose your preferred security track, from secure hardware to the entire STM32Trust function coverage

Innovate faster!





The 12 STM32Trust security functions

Addressing the security challenges & gaps

Security challenges for our customers

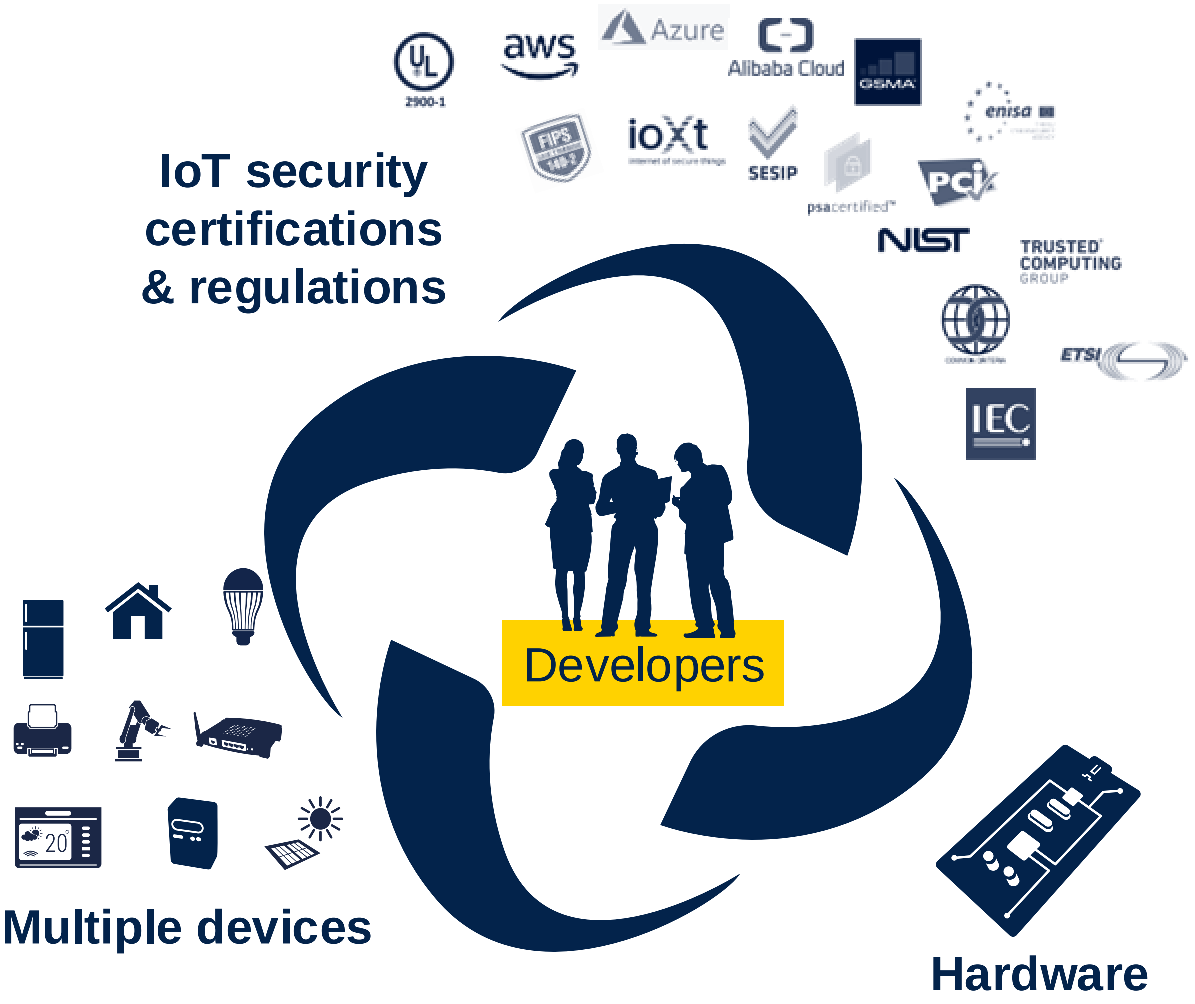
Complex

High cost

Time to market

More effort to obtain

Scalability, certification, maintenance
core security hardware and services



IoT security certifications & regulations

Developers

Multiple devices

Hardware

STM32Trust TEE – Secure Manager

life.augmented

STM32 Trust TEE

Accelerate your time to market

Secure Manager

A **trusted execution environment** (TEE) integrating core security services

A simplified customer journey

Seamless cloud/server support

Supporting remote provisioning

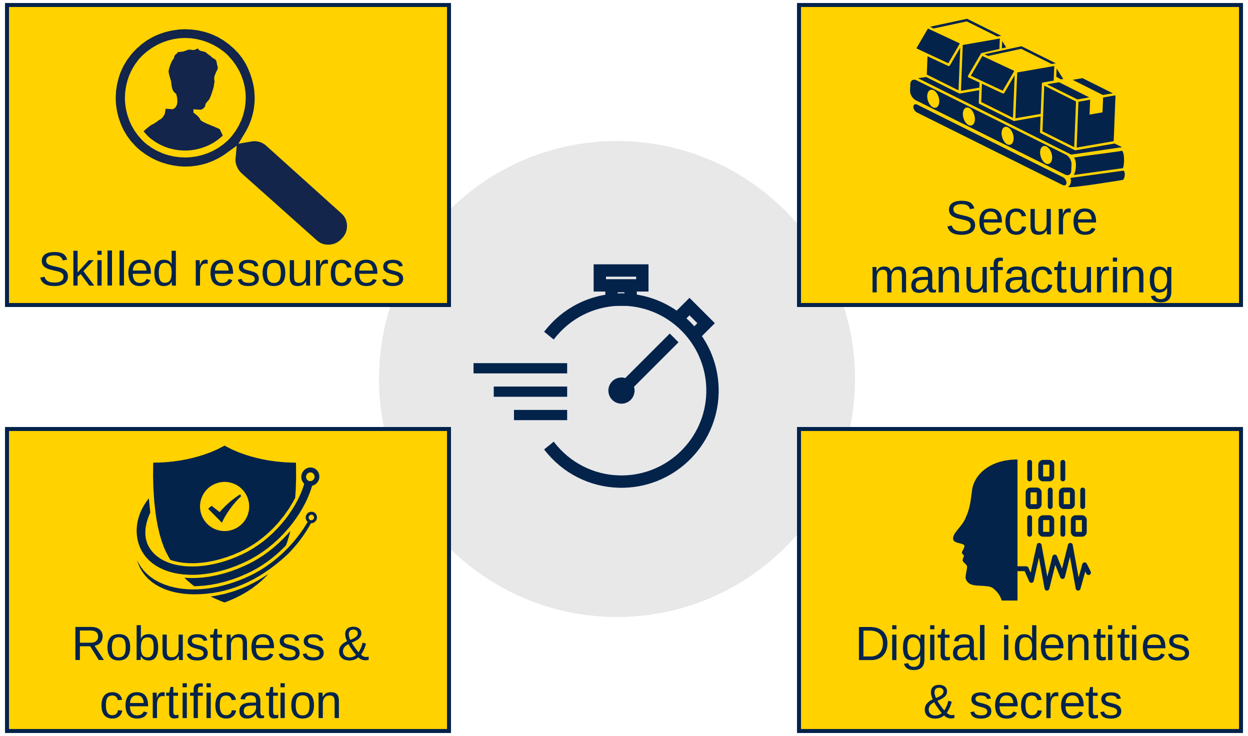
Multi-tenant IP protection

The first MCU supplier to offer a certified and maintained TEE solution to customers

life.augmented

What are the main benefits of using the Secure Manager

The Secure Manager reduces the cost of enhanced security



Skilled resources

Secure manufacturing

Robustness & certification

Digital identities & secrets

STM32 Trust TEE

Secure Manager overview

Enhance security while reducing costs and complexity

Multitenant IP protection

- Multiple business case made possible
- Isolation for confidentiality at installation & runtime
- Protected development flow

Cloud / Server

- Seamless cloud/server registration
- Pre-provisioned keys & certificate
- PSA compliant attestation

Simplified customer journey

- Turnkey TEE security solution including services
- Full certified secure implementation
- TrustZone® complexity abstraction
- Designed for LTS – long term service
- Arm® PSA API compliant

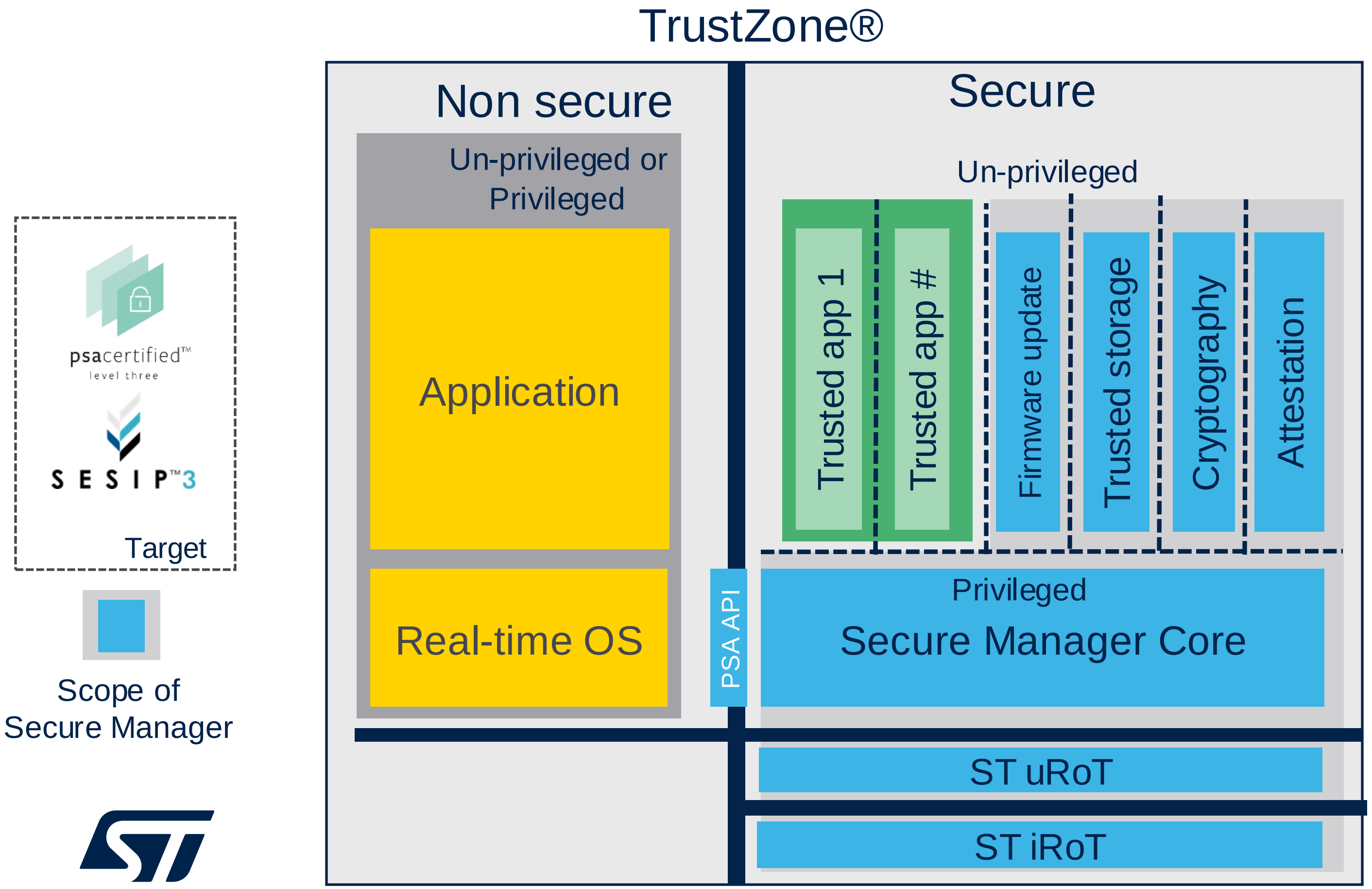
Remote secret admin.

- Remote PKI lifecycle management **enabled**
- Customizable (e.g. Matter)
- Certificate installation/rotation/ revocation …
- Via partnership (NOT an ST service)

STM32 Trust TEE

Secure Manager on STM32H5 MCU

Protect IP and simplify the journey to strong security

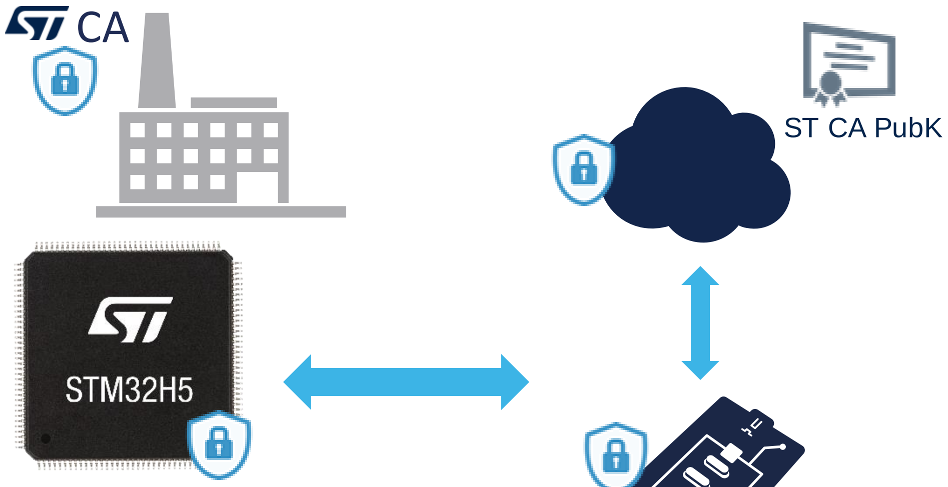


- ST platform ownership
- Turnkey set of security services
- Arm® PSA API compatible
- Modular secure update capable
- Secure Manager Core to handle isolation
- Multi-tenant software IP protection
- Designed for Long-Term-Support
- To be certified and maintained by ST
- Optimized certification properties

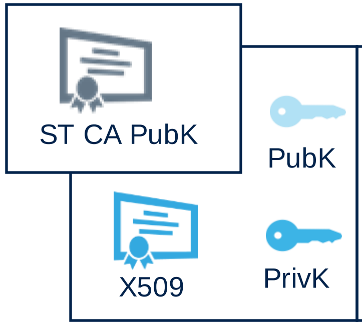
life.augmented

STM32 Trust TEE

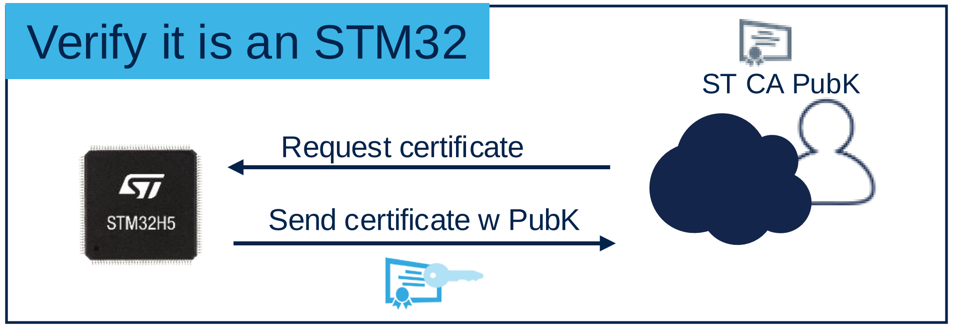
STM32H5 - Attestation
Available thanks to Secure Manager



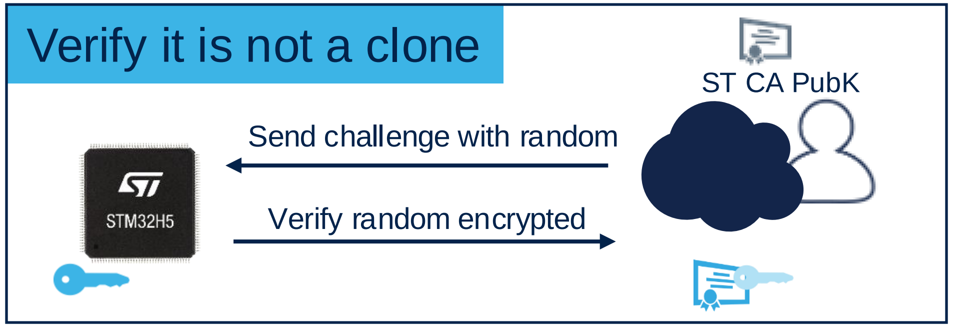
In-factory provisioned identity



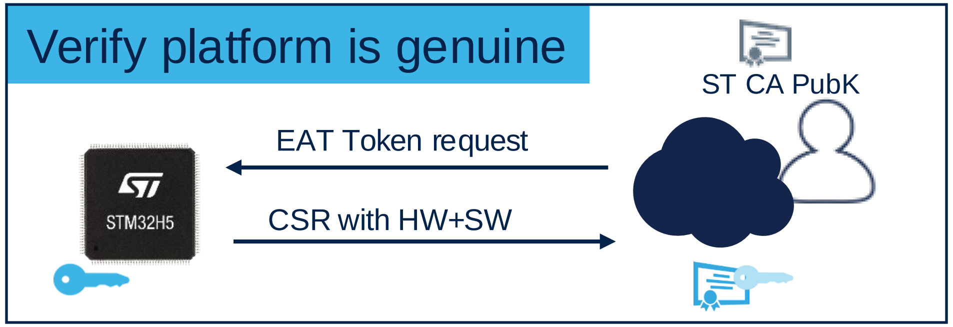
- 2 x key pair + 2 x certificate
  - Pre-provisioned on STM32H5 by ST
- ST CA public key
- **PSA** or **USER** Attestation



Verify it is an STM32



Verify it is not a clone



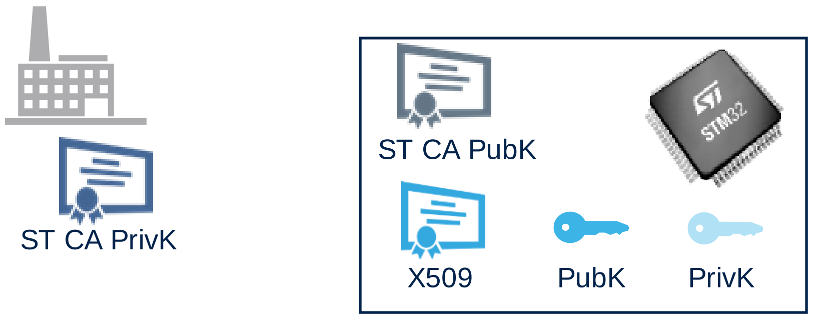
Verify platform is genuine

Arm® PSA Initial attestation

🟦 Service developed by ST

STM32H5 - Digital identities
Available thanks to Secure Manager

PSA initial attestation



ST CA PrivK

ST CA PubK

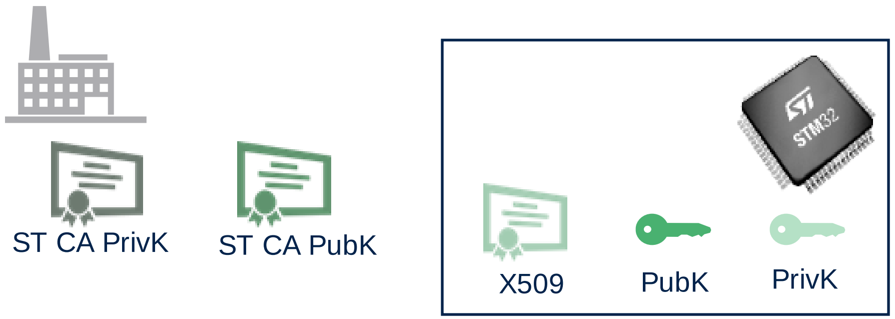
X509

PubK

PrivK

- Key pair + Certificate
  - Pre-provisioned on STM32H5 by ST manufacturing
- ST CA public key
  - Distributed **under license** to service providers
- Attestation via PSA Attestation APIs
  - Get the initial attestation token (EAT Token)
    - **Containing device measures**
      - Hardware revision / Device lifecycle / software components

User attestation



ST CA PrivK

ST CA PubK

X509

PubK

PrivK

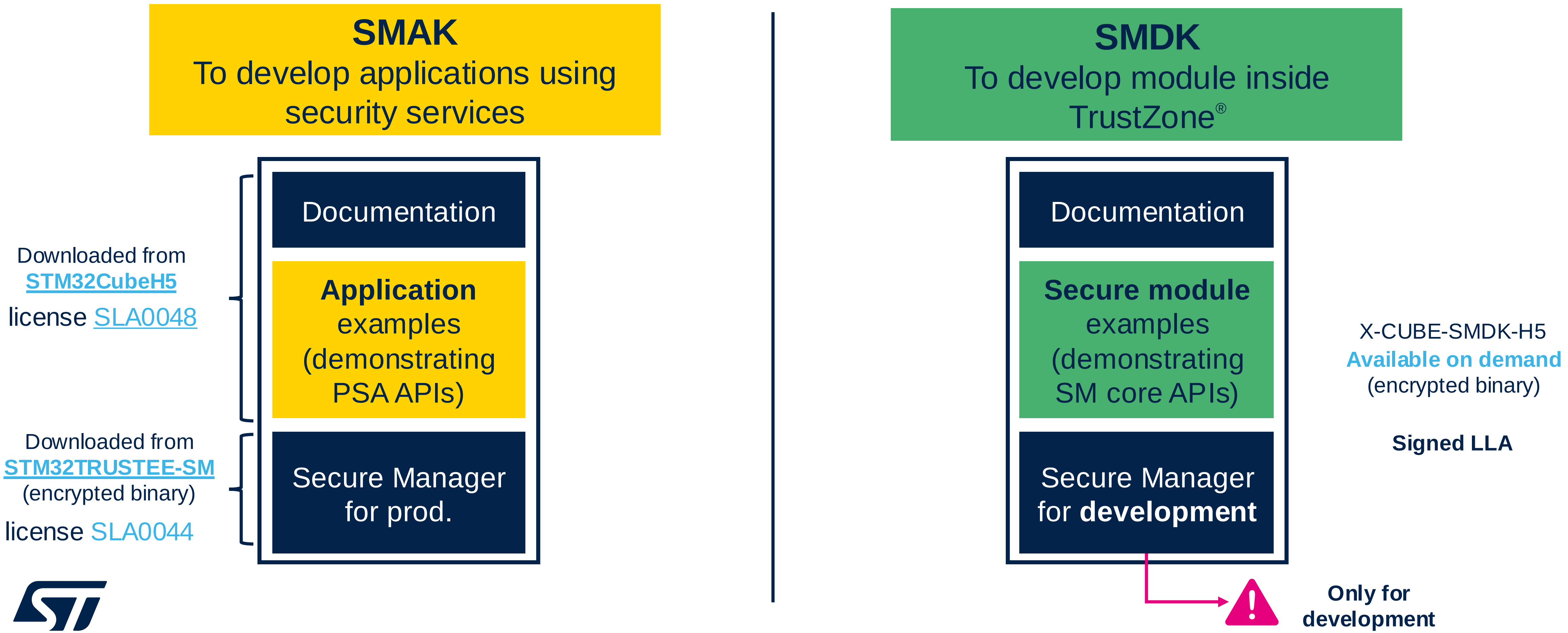
- Key pair + Certificate
  - Preprovisioned on STM32H5 by ST manufacturing
- ST CA public key
  - **Publicly** distributed within the Secure Manager
- Attestation via PSA Cryptographic APIs

Development and installation

STM32 Trust TEE

Secure Manager Development kits

Simplifying developers' experience to ensure security in embedded systems



SMAK
To develop applications using security services

Documentation

Application examples (demonstrating PSA APIs)

Secure Manager for prod.

Downloaded from STM32CubeH5
license SLA0048

Downloaded from STM32TRUSTEE-SM
(encrypted binary)
license SLA0044

SMDK
To develop module inside TrustZone®

Documentation

Secure module examples (demonstrating SM core APIs)

Secure Manager for **development**

X-CUBE-SMDK-H5
Available on demand
(encrypted binary)

Signed LLA

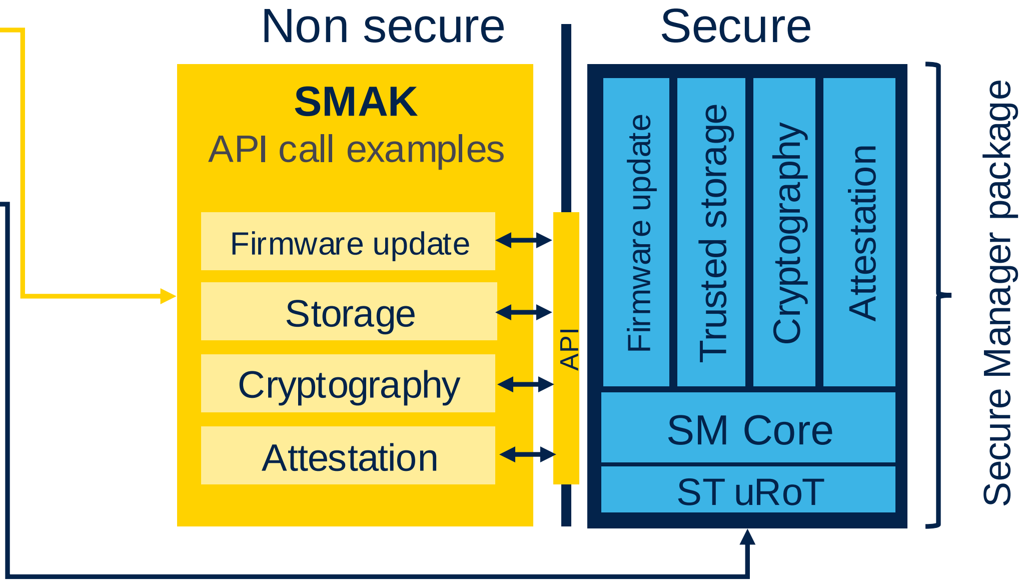
⚠ **Only for development**

life.augmented

How to evaluate the secure manager
Focusing on application using security services

1. Download STM32CubeH5 – SMAK examples
2. Download the Secure Manager binary
3. Configure & install Secure Manager batch
   - Start w/ **default settings** (or configure ITS, Memory, Key, DA)
4. Build and load the NS project batch

- Application can be modified/debugged
- Security APIs can be used
  - Based on examples provided
- Secure area is protected -TEE locked



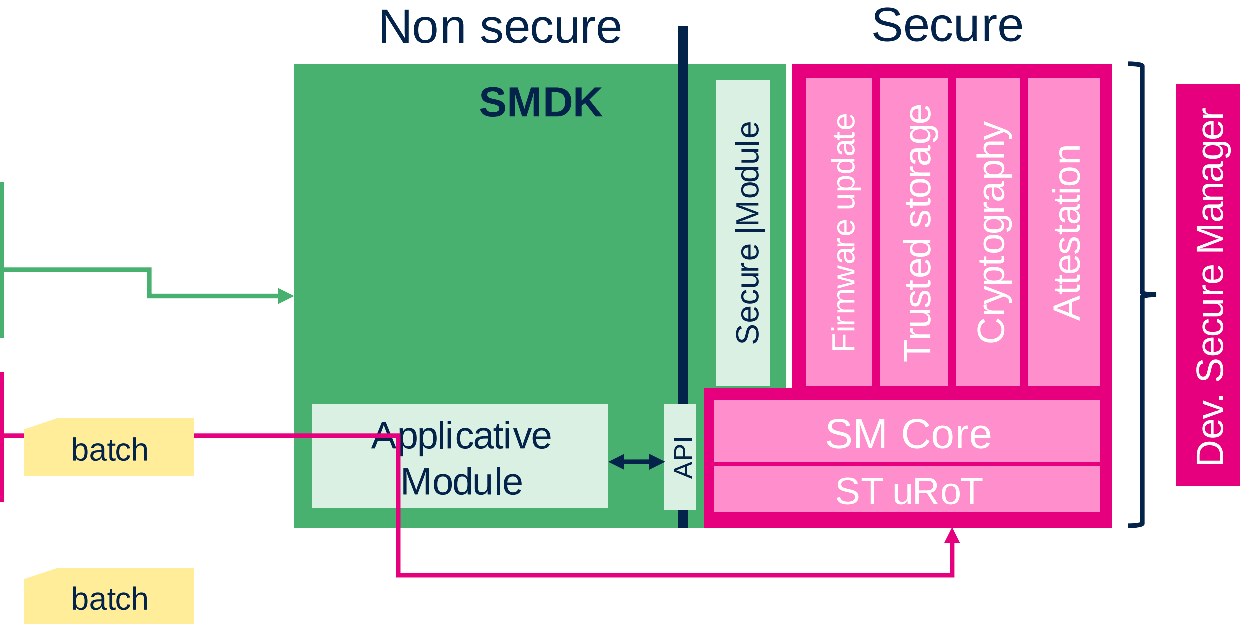
STM32H573I-DK

How_to_start_with_Secure_Manager_on_STM32H573

Wiki

How to develop a **secure module** with **SMDK**

1. Download CubeH5
2. Sign license – contact your ST representative
3. Get SMDK ➔ X-CUBE-SMDK-H5
   channel provided by ST after signature of the license
4. Configure & Install Dev. Secure Manger
5. Build and load the project



- Module can be modified/debugged
- Interface with secure module via APIs

SMDK is **ONLY** for development

STM32H573I-DK

Getting started SMDK

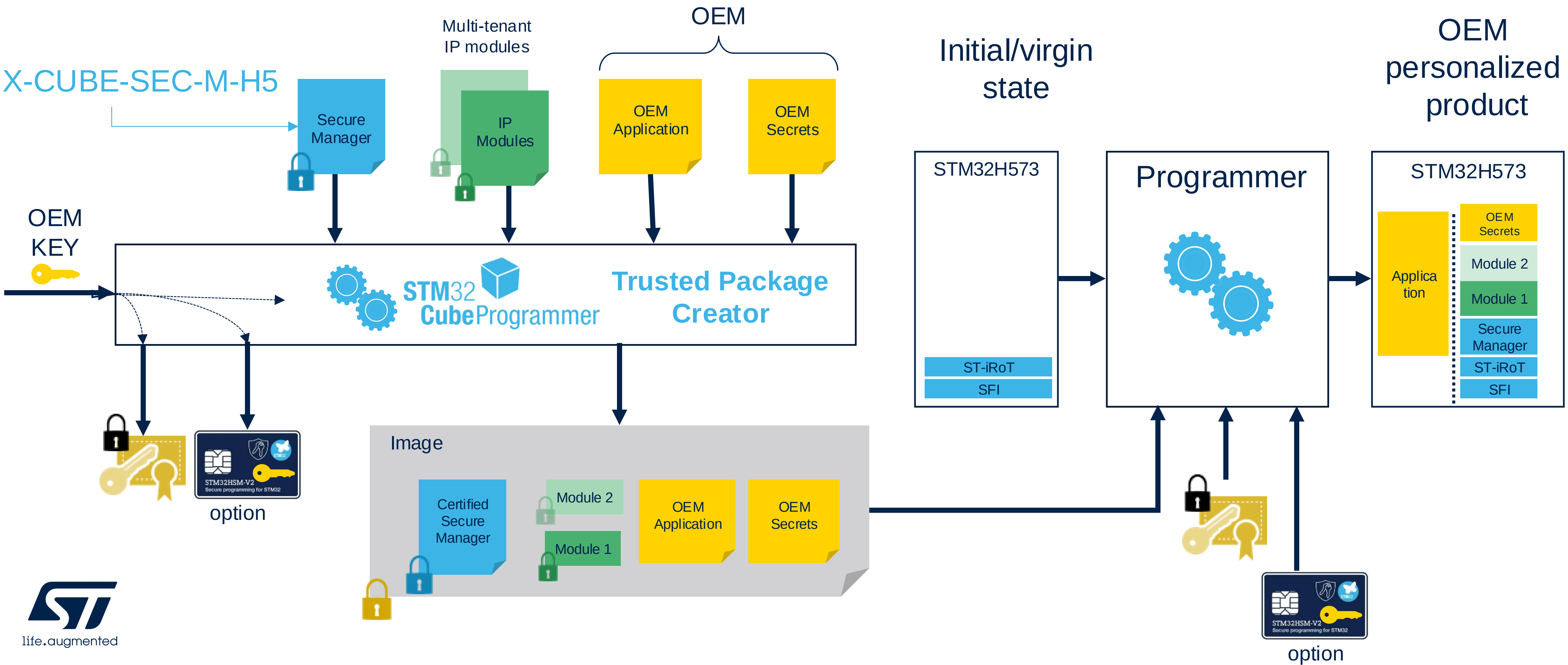
Wiki

Secure Manager
Preparation & installation flow

🔒 Protected by ST specific Key
🔒 Protected by Module Key
🔒 Protected by OEM Key
🔒 Protected by ST public Key for OEM

Application creation flow

OEM installation flow



life.augmented

Documentation

Documentation and useful links

- STM32Trust web page
- STM32CubeH5 – inc. API & SMAK examples
- STM32H5 RM0481
- STM32TrustTEE-SM web page
  - X-CUBE-SEC-M-H5 H5 SM binary
  - Reference manual
- Online trainings
- X-CUBE-SMDK-H5 SMDK – on demand
- Discovery kit with STM32H573
- STM32H5 security FAQ
- Secure Manager Blog article

Wiki

- Wiki security
  - Wiki Security H5
  - Wiki Secure Manager
  - Getting started with H5 security

- ST Community specific tags
  - Secure Manager
  - STM32H5 Series

- IoT kits including Secure Manager
  - Azure X-CUBE-AZURE-H5
  - AWS X-CUBE-AWS-H5

Partner Program

Partner support services

life.augmented

STM32Trust TEE Secure Manager Service offering from PROVENRUN

	Standard support	Premium support
Annual subscription per platform	$15k	$35k
Customer code implementation questions	✓	✓
Customer code optimization questions		✓
Number of tickets	Unlimited	Unlimited
Assistance directly from ProvenRun	✓	✓
Dedicated team and direct access to experts		✓
Support on current major version	✓	✓
Support on one previous major (LTS) version		✓
Debug on your target hardware		✓
Response time	5 business days	2 business days

- ST Partner since 2018
- Deep proven security expertise
- Long-term support
- Know-how from various fields of application
  - Automotive, industrial, aerospace
  - Payment and others
- Dedicated support tools for tracking tickets
- Terms & conditions – please contact us

Contact: sales@provenrun.com

STM32Trust TEE Secure Manager Additional services from PROVENRUN

Optional services

- Proactive security monitoring of the client's platform
- Debug on closed third-party OS, access to specific IP
- Support all previous LTS versions as well as Customer target hardware (based on ST Platform)
- Faster response time for severe issues

Professional services

- Expert coaching, code optimization
- Secure Manager coding training
- Cybersecurity landscape overview
  - Regulation: CRA, NIS2, RED,…
  - Scheme: CC, SESIP, 21434, 62443, ...
- Certification coaching
  - Scope definition
  - Certification framework definition
  - Certification project monitoring
    - ✓ cost, delays
  - Interface with Lab/Certification Body

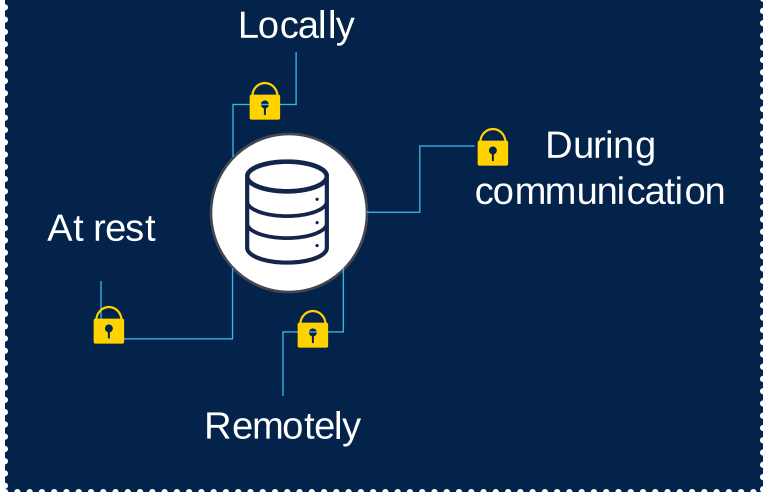
Contact: sales@provenrun.com

Conclusion & takeaways

life.augmented

Embedded security
What are developers typically trying to achieve?

Easily protect my critical data & secrets and those of my end customers



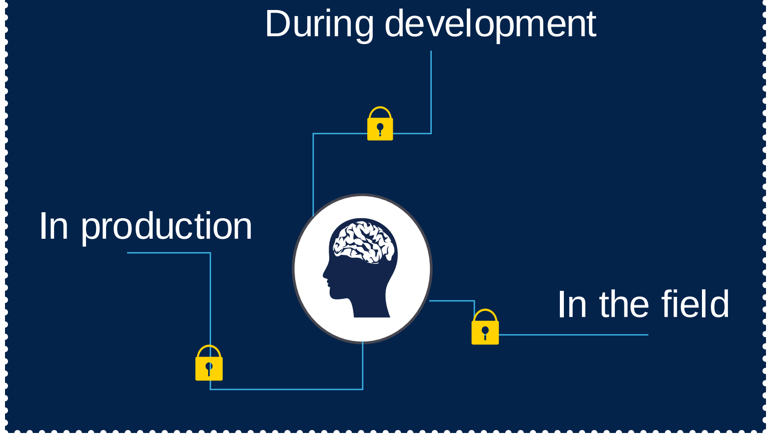
Locally

During communication

At rest

Remotely

Easily protect my IP and my partner’s IP in a strong and effective way

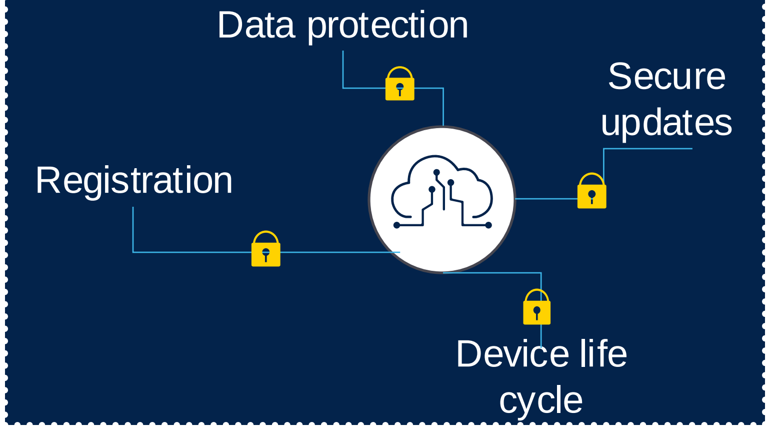


During development

In production

In the field

Easily & securely connect to clouds & servers without painful digital identities management



Data protection

Secure updates

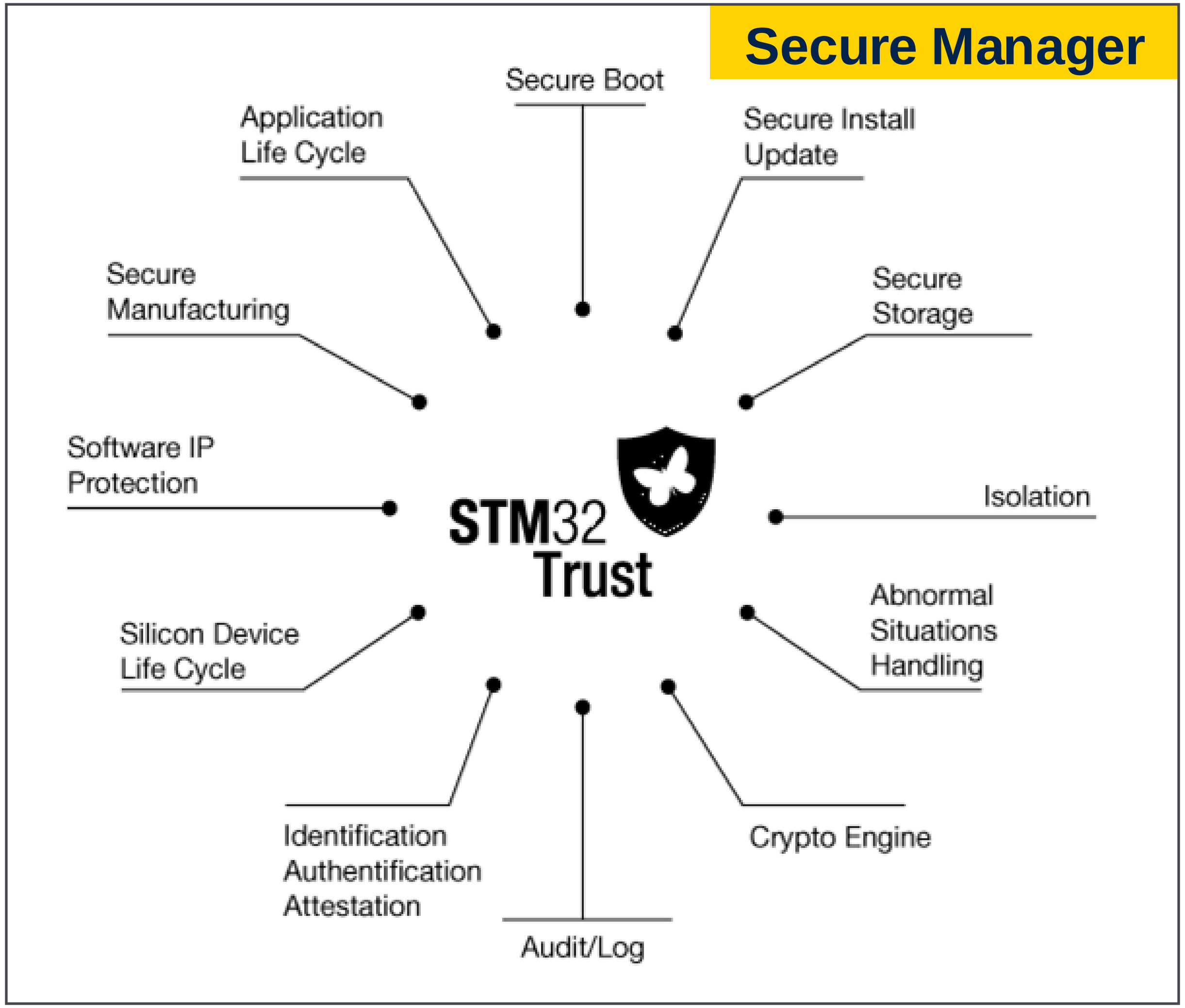
Registration

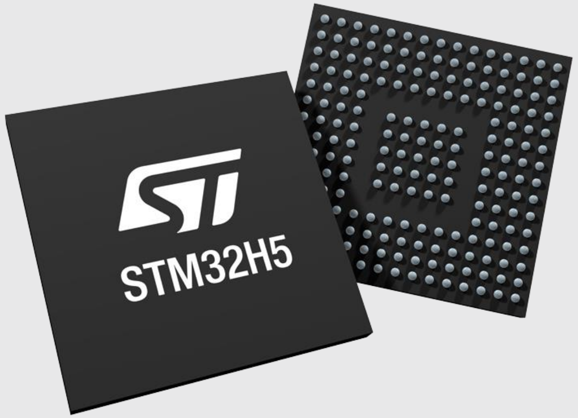
Device life cycle

STM32 Trust TEE

Accelerate your time to market

Secure Manager





STM32**H5 MCU**

SESIP™3

psacertified™ level three

Target certifications

Our technology starts with You

life.augmented