life.augmented

STM32Trust

STM32H5 Security
Secure Manager - Part 1

STM32Trust TEE
Secure Manager Introduction

Presenter: Mena Roumbakis

Agenda

1 Introduction

2 STM32H5 security features overview

3 Hands-On: Getting started with Secure Manager

4 Hands-On: SMAK Develop and Debug

5 Hands-On: Debug Authentication

6 Conclusion & takeaways

life.augmented

Introduction

OUR VISION

Be the reference for securing GP MCUs & MPUs

OUR MISSION

Provide our developers the means to build **Secure applications**

OUR STRATEGY

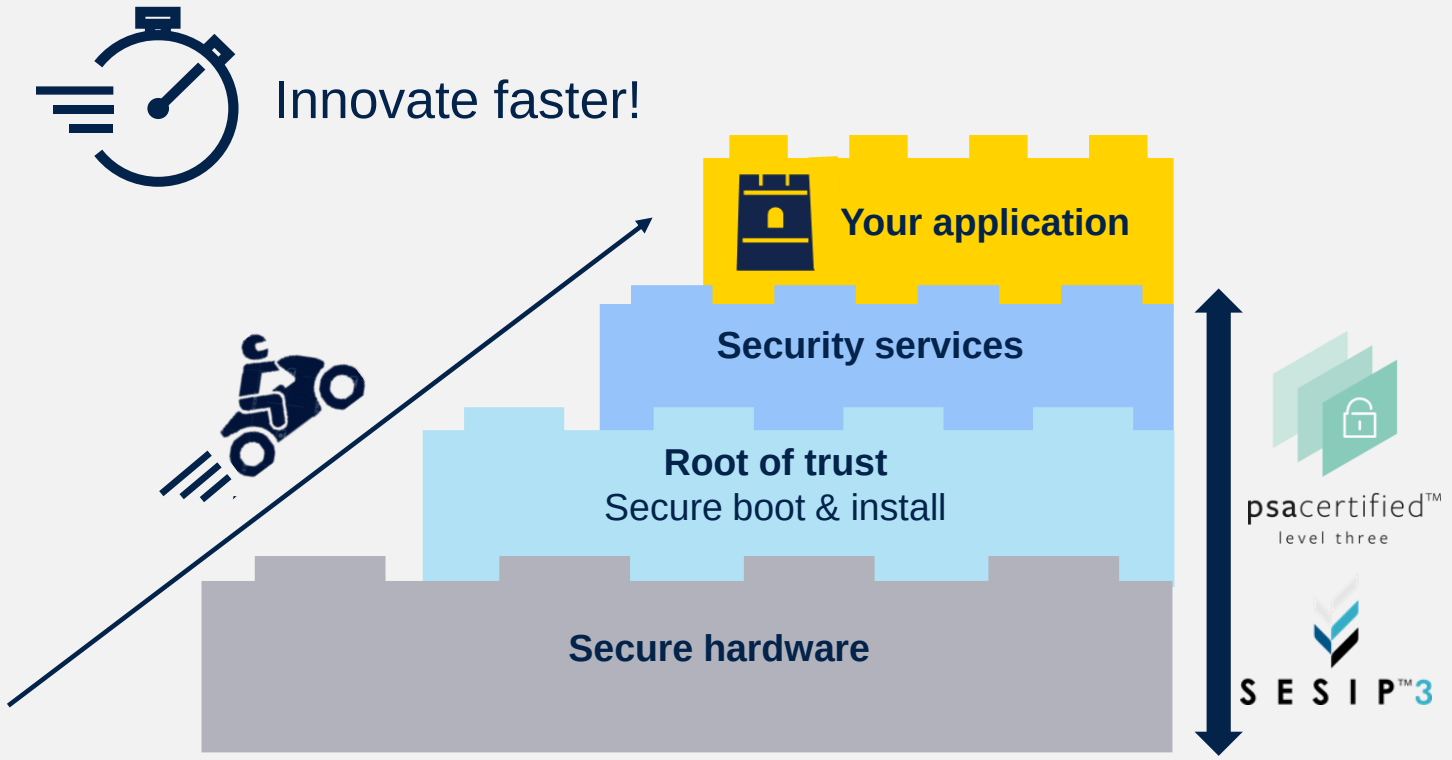
Security Robustness & Assurance

Portfolio consistency

Scalable & Turn-key solutions

STM32 Security Framework

Building Trust in Embedded Systems



life.augmented

www.st.com/STM32Trust

STM32Trust TEE – Secure Manager

STM32 Trust TEE

This is where we come in !

Secure Manager

A **Trusted Execution Environment** (TEE) integrating core security services

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

life.augmented

Scalable security to accelerate 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

STM32 Trust TEE

Secure Manager
Ecosystem development tools

Simplify developer's experience

SMAK
To develop applications using security services

Downloaded from **STM32CubeH5** license SLA0048

- Documentation
- **Application** examples (demonstrating PSA APIs)

Downloaded from **STM32TRUSTEE-SM** (encrypted binary) license SLA0044

- Secure Manager for prod.

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

STM32 Trust

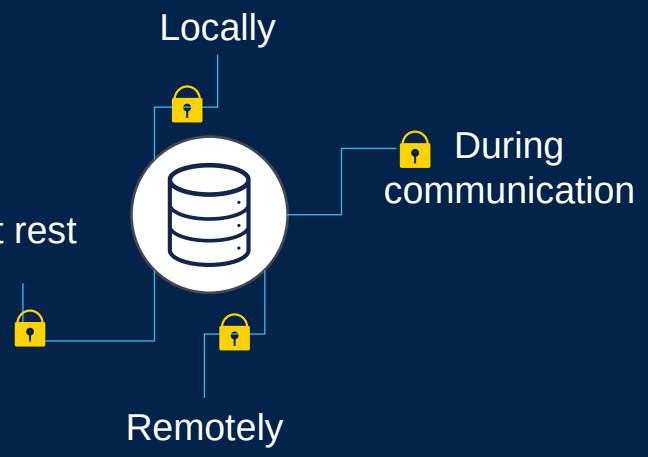
Secure Manager
Key messages

- A certified turnkey SoC set of security services
- In-ST-factory pre-provisioned identities for Clouds & OEM servers
- An exhaustive software IP protection solution
- Enabling 3rd party keys & certificates Lifecycle management

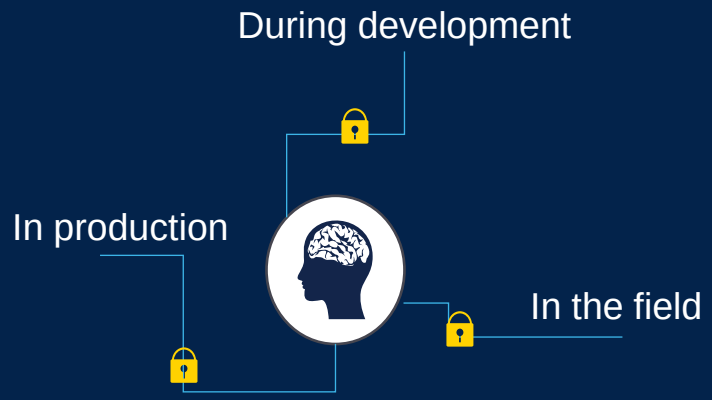
life.augmented

“If only

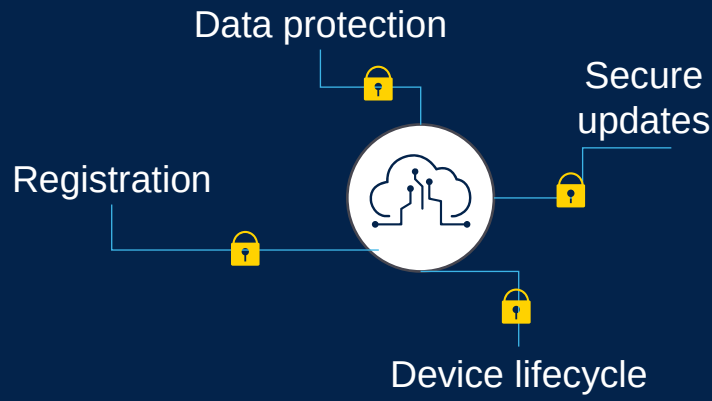
I could easily protect my critical data & secrets and those of my end customers



I could easily and strongly protect my IPs, and my partner’s IPs



I could easily & securely connect to Clouds & Servers without Painful digital identities management

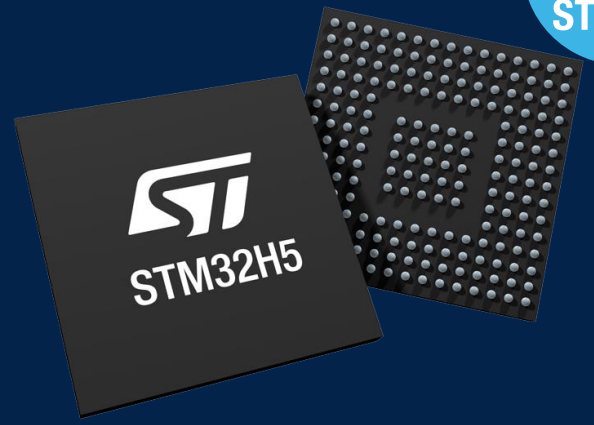


life.augmented

Scalable security

From **secure hardware** to **full solution** owned & maintained by ST

STM32 Trust TEE **Secure Manager**



STM32H5 MCU

SESIP™3

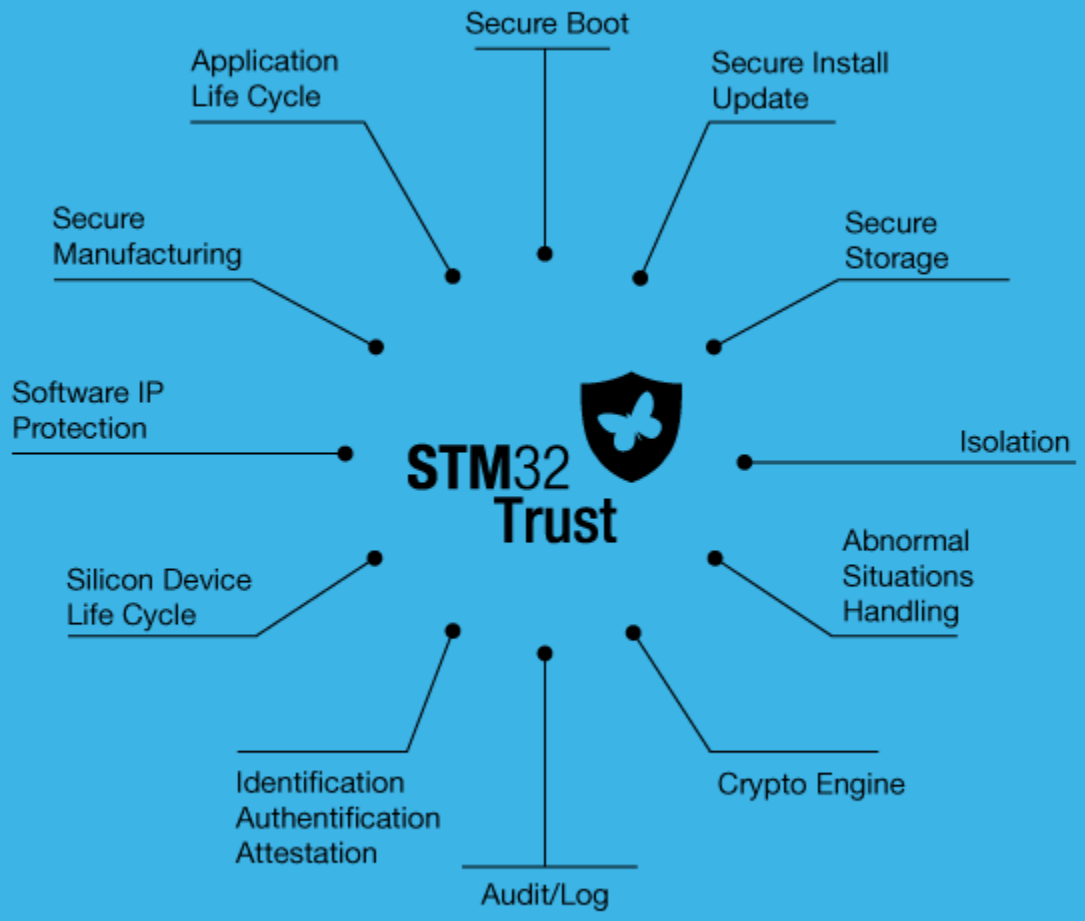
psacertified™ level three

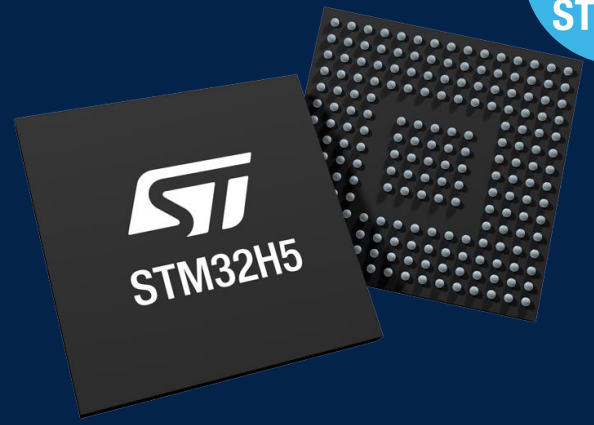
Target certifications

life.augmented

STM32 Trust TEE

Secure Manager





STM32H5 MCU

SESIP™3

psacertified™ level three

Target certifications

life.augmented

Agenda

1 Introduction

2 STM32H5 security features overview

3 Hands-On: Getting started with Secure Manager

4 Hands-On: SMAK Develop and Debug

5 Hands-On: Debug Authentication

6 Conclusion & Takeaway

life.augmented