life.augmented

STM32Trust security ecosystem

STM32

Agenda

1. STM32Trust overview
2. Customer examples
3. Security functions & ST offer
4. Focus on SFI and SBSFU
5. Evaluations & certifications
6. Takeaways

life.augmented

STM32Trust overview

life.augmented

STM32Trust overview

- STM32Trust offers a robust multi-level strategy to enhance security in product designs, using our STM32 microcontrollers and STSAFE secure elements.
- STM32Trust is our security framework combining our ecosystem and security services.
- STM32Trust solution offers a complete toolset for code and execution protection.
- STM32Trust brings 12 security functions to align with customer use cases and security standards.

life.augmented

Customer examples

life.augmented

Customer example (1/6)
Focus on secure manufacturing

Bob is CEO of a company designing toys.
He would like to make sure the firmware developed by his team is protected from theft and will only run on the hardware developed by his team.

What Bob wants to achieve

- No firmware stealing at production
- No over-production by manufacturer
- No mean to program other devices

- No firmware stealing in the field

- Detection of attacks in the field

The Security Functions needed by Bob

- Secure Manufacturing

- Software IP Protection
- Secure Install / Update
- Silicon Device Lifecycle

- Abnormal Situations Handling
- Audit/Log

Customer example (2/6)
Focus on isolation and IP protection

Jon is at the head of a company selling firmware and receives royalty payments from customers.
The firmware developed by his team is very valuable to him. It features application options that can be further enabled by the user.

What Jon wants to achieve	**The Security Functions needed by Jon**
• Isolate his firmware from customer one	• Isolation • Software IP Protection
• Ensure that his firmware can independently be updated	• Secure Install/Update
• Set application macro-state in a way which cannot be altered	• Application Lifecycle

Customer example (3/6)
Focus on secure boot & secure update

Mark sells costly equipment.
He wants to offer a firmware update service.
He wants his service to only update his equipment and would like to make sure only his firmware runs on his devices.

What Mark wants to achieve

- Ensure only his equipment is targeted
- Always known product state
- Ensure the update is handled with integrity and that authenticity checks are carried out
- Authenticity of firmware running on devices

The Security Functions needed by Mark

- Identification/Authentication/ Attestation
- Secure Install/Update
- Secure Boot

Customer example (4/6)
Focus on secured communication

Oliver is selling devices that report sensitive data to a central server. Oliver needs to make sure the data cannot be exposed to people outside of his company and that it is protected.

What Oliver wants to achieve

- Ensure transmitted data is not exposed
- Ensure secret on data encryption keys
- Ensure data is sent from authenticated devices
- Ensure data is sent to authenticated servers

The Security Functions needed by Oliver

- Crypto Engine
- Secure storage
- Identification/Authentication/ Attestation

Customer example (5/6)
Focus on brand protection and identification

Rose controls her fleet of devices from a remote server. She wants to be sure no counterfeiting or malicious devices are running with her server and would like to have full control over the devices. Rose needs to be able to check the identity and access rights of network operating devices at any time.

What Rose wants to achieve	The Security Functions needed by Rose
• That every device shows a unique identity • Be able to authenticate the device • Be able to attest the device access rights	• Identification/Authentication/ Attestation
• Secure device communication	• Crypto Engine
• Ensure that identities and access right secrets cannot be leaked even at the manufacturing stage	• Secure Storage and Secure Manufacturing (Secure Personalization)

Customer example (6/6)
Focus on data protection

Jack is collecting user data within his devices as part of a larger system.
Jack's devices and system needs to be in line with regulations (such as GDPR) to be able to promote and sell devices.

What Jack wants to achieve	**The Security Functions needed by Jack**
• Ensure platform integrity	• Secure Boot • Abnormal Situations Handling
• Ensure user data is not exposed while communicating	• Crypto Engine • Identification/Authentication/Attestation
• Ensure user data is stored securely	• Secure Storage

Security functions and ST offer

life.augmented

The 12 security functions

- STM32Trust brings 12 Security Functions to align with Customer Use Cases and Security Standards
- STM32Trust brings assets (Documentation, Software, Tools…) to cover those 12 Security Functions

The 12 security functions
Summary of definitions

1- Secure Boot	2- Secure Install / Update	3- Secure Storage	4- Isolation
Ability to ensure the authenticity and integrity of an application that is inside a device	Installation or update of firmware with initial checks of integrity and authenticity before programming and executing	Ability to securely store secrets like data or keys	Isolation between trusted and non-trusted parts of an application

5- Abnormal Situations Handling	6- Crypto Engine	7- Audit / Log	8- Identification / Authentication / Attestation
Ability to detect abnormal situations (both hardware and software) and to take adapted decisions like secrets removals	Ability to process cryptographic algorithms, as recommended by a security assurance level	Keep trace of security events in an unchangeable way	Unique identification of a device and/or software, and ability to detect its authenticity, inside the device or externally

9- Silicon Device Lifecycle	10- Software IP Protection	11- Secure Manufacturing	12- Application Lifecycle
Control states to securely protect silicon device assets through a constrained path	Ability to protect a section or the whole software against external or internal reading. Can be multi-tenant	Initial device provisioning in unsecured environment with overproduction control. Potential secured personalization	Define unchangeable incremental states to securely protect application states and assets

life.augmented

Overview

Security functions versus STM32 & STSAFE

Security Function	STM32F4/F7/L1/WB/G0/G4/H7/L0/L4		STM32MP1		STM32L5 with TrustZone		+ STSAFE-A/TPM
	Silicon	Firmware	Silicon	Firmware	Silicon	Firmware	Silicon
Secure Boot	✓	✓ SBSFU	✓	✓ TF-A	✓	✓ TFM_SBSFU	✓
Secure Install/Update	✓		✓	✓ OPTEE	✓		✓
Secure Storage	✓ (L0/L4/H7/G0/G4)	✓ (WB) SBSFU KMS (L4)	✓	✓ OPTEE	✓	✓ TFM SPE	✓
Isolation	✓		✓	✓ OPTEE	✓	✓ TFM	✓
Abnormal situations handling	✓		✓		✓		
Crypto Engine	✓	✓ Crypto Libraries	✓	✓ OPTEE	✓	✓ Crypto Libraries TFM	✓
Audit/Log					✓	✓ TFM	
ID/Auth/Attestation	✓		✓		✓	✓ TFM Attestation	✓
Silicon Device LifeCycle	✓		✓		✓		
Software IP Protection	✓		✓	✓ OPTEE	✓	✓ TFM	
Secure Manufacturing	✓ SFI (H7/L4) with STM32HSM		✓ SSP with STM32HSM		✓ SFI with STM32HSM		✓
Application LifeCycle	✓		✓		✓		✓

Firmware to be developed by user
Reference firmware proposed by ST

life.augmented

1. Secure boot

STM32 Firmware / Tool Part Number	Benefit for Security Function	STM32 Series
X-CUBE-SBSFU	Example code implementing both a Secure Boot and a Secure Firmware Update mechanism	F4/F7/WB/G0/G4/H7/L0/L4
TFM_SBSFU Boot (Part of STM32CubeL5)	Example code implementing both a Secure Boot and a Secure Firmware Update mechanism	L5
TF-A (Part of OpenSTLinux)	First stage secure bootloader configuring STM32MP platform	MP1

STM32 Silicon Feature	Benefit for Security Function	STM32 Series
RDP (Read Protection)	Prevents a debugger from reading the secure boot	F4/F7/WB/G0/G4/H7/L0/L4/L5
WRP (Write Protection)	Prevents an application from altering the secure boot firmware	
MPU (Memory Protection Unit)	Ensures privileged access to some portion of application – task isolations	
MMU (Memory Management Unit)	Ensures privileged access to some portion of application – task isolations	MP1
UBE (Unique Boot Entry)	Ensures the silicon always boots at the secure boot location	G0/G4/L5
HDP (Hide Protect)	Temporal isolation ensuring secure boot is not seen after first execution	H7/G0/G4/L5
Secure Boot ROM code	Root of trust for loading first bootloader on STM32MP	MP1

STSAFE Feature	Benefit for Security Function
X509 certificate	Allow attest of executed firmware
One-way counter (decrement)	Supporting version control management using STSAFE-A

11. 11. Secure manufacturing

STM32 Firmware / Tool Part Number	Benefit for Security Function	STM32 Series
STM32HSM-V1 and V2	Hardware security module (HSM) used to secure the programming of STM32 products, and to avoid product counterfeiting at contract manufacturers' premises	STM32 series with SFI or SSP
STM32CubeProgrammer	Software tool able to program an HSM with encryption key and counter of permitted programming occurrences	NA
FastROM Programming Services	Pre-loading of customer software in STM32 done by ST manufacturing	All, except MP1

STSAFE Service	Benefit for Security Function
STSAFE-A pre-personalization (MoQ 5K)	Pre-loading of customer secret in STSAFE-A at ST secure manufacturing site

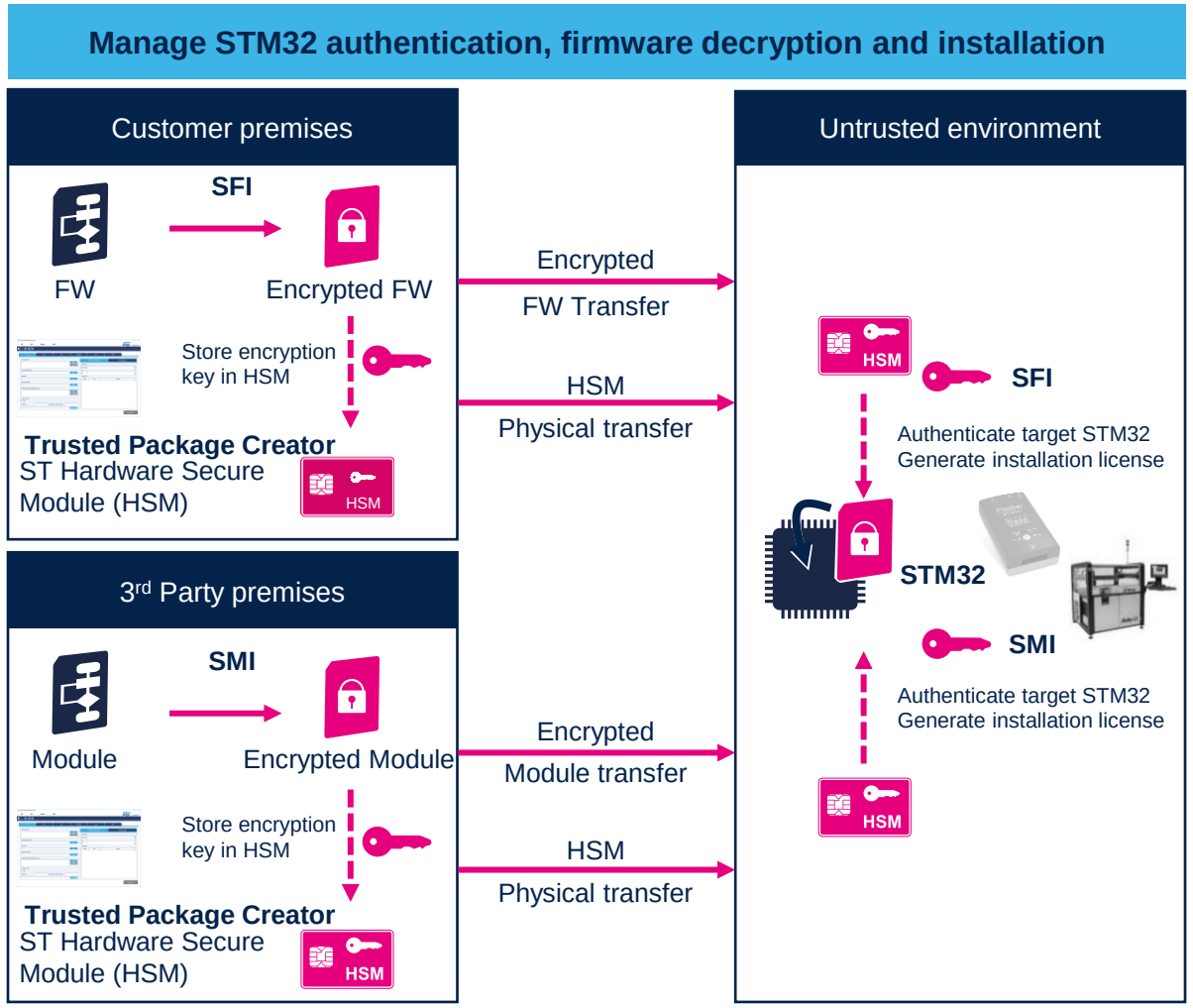
STM32 Silicon Feature	Benefit for Security Function	STM32 Series
RSS with SFI (Root Security Services with Secure Firmware Install)	Built-in service callable at reset, ensuring installation of an OEM firmware and option bytes, with authenticity, integrity, confidentiality, insurance to program a genuine STM32, and possibly limited overall quantity of programmed STM32	H7/L4/L5
Secure Boot with SSP (secure secret provisioning)	Built-in service callable at reset, ensuring secure provisioning of OEM credentials. Controllability of overall quantity of STM32MP1 provisioned	MP1

*: Special part numbers on demand. Contact nearest sales office

Focus on SFI and SBSFU

life.augmented

Focus
Embedded secure firmware install - SFI



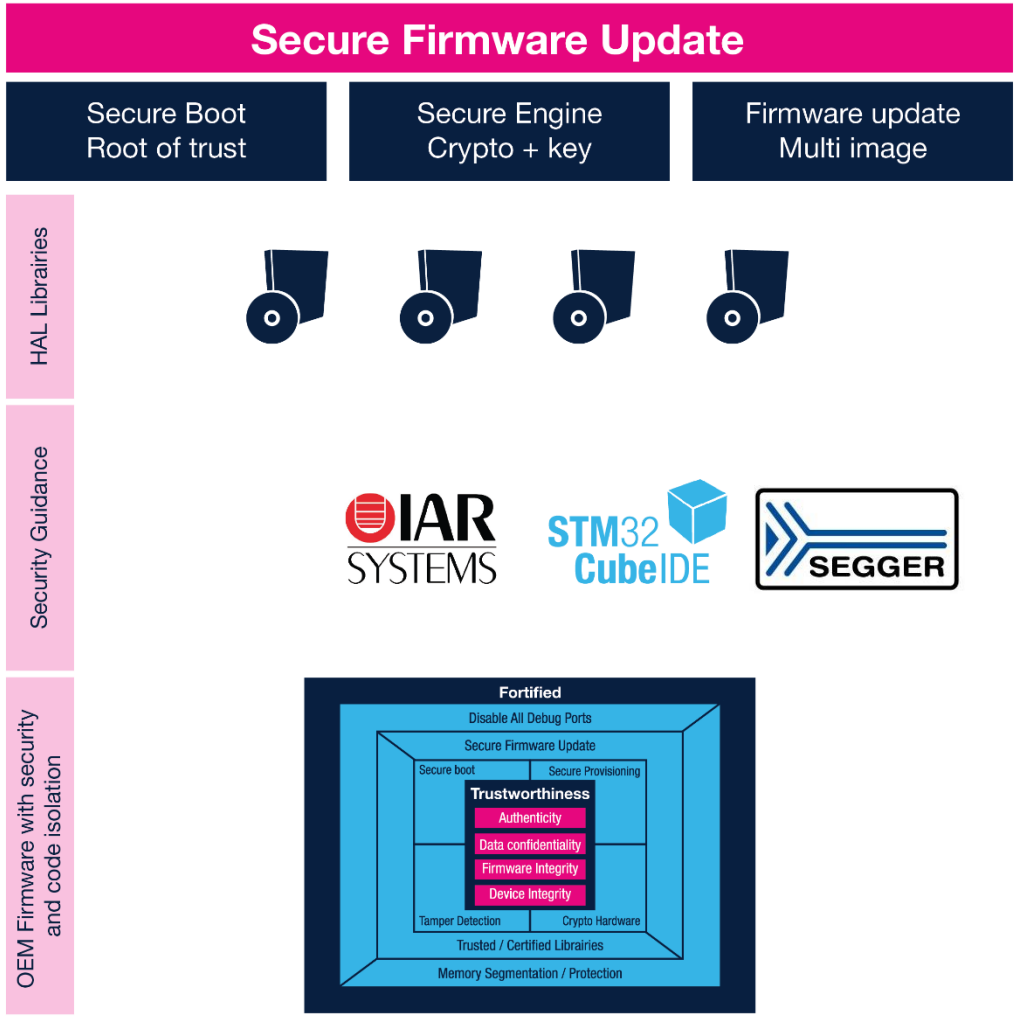
Secure Loader
embedded services provisioned by ST
➔ Mass Market approach

ST ecosystem
with
Encryption, HSM and programming tools

Firmware cloning
protection on the first installation
via
UART / SPI / USB

Protect 3rd party Software IP (SMI)

Focus
Secure boot secure FW update - SBSFU



Reference library source code for In-application Programming

Demonstrate SW modules for:
- Secure Boot
- Secure Engine for Crypto and key
- Firmware Update image management

Ensure authentication and secure programing of in the field products

Reference implementation of STM32 hardware memory protections

Evaluations and certifications

life.augmented

First solution certified SESIP level 3: STM32L476 with X-CUBE-SBSFU

- SESIP = **S**ecurity **E**valuation **S**tandard for **I**oT **P**latforms, by Global Platform.
- SESIP describes the security functional and assurance requirements.
- STM32L476 with X-CUBE-SBSFU package is the 1st GP MCU platform to pass SESIP level 3.

TRUSTCB

TRUST AND VERIFY

Certificate ID	SESIP-2000002-01
	TrustCB B.V. declares that
Product	XCUBE SBSFU on STM32L476RG, version 2.2.0
	of
Sponsor (and developer)	ST Microelectronics in Rousset, France
	complies to the requirements described in the standard and ST
Standard	Common Criteria for Information Technology Security Evaluation (CC) Version 3.1 Revision 5 (ISO/IEC 15408)
ST Reference	Security Target for XCUBE SBSFU on STM32L476RG, version 0.4
	Summarized:
Assurance Package	SESIP 3
Protection Profile	None
	As evaluated by:
Evaluation Facility	Brightsight B.V. located in Delft, The Netherlands
	Under scheme:
	SESIP — TrustCB Scheme Procedures for SESIP V2.0; Security Evaluation Standard for IoT Platforms (SESIP) v1.3
Validity	Date of 1st issuance: 2020-02-20 Date of expiry: 2022-02-20

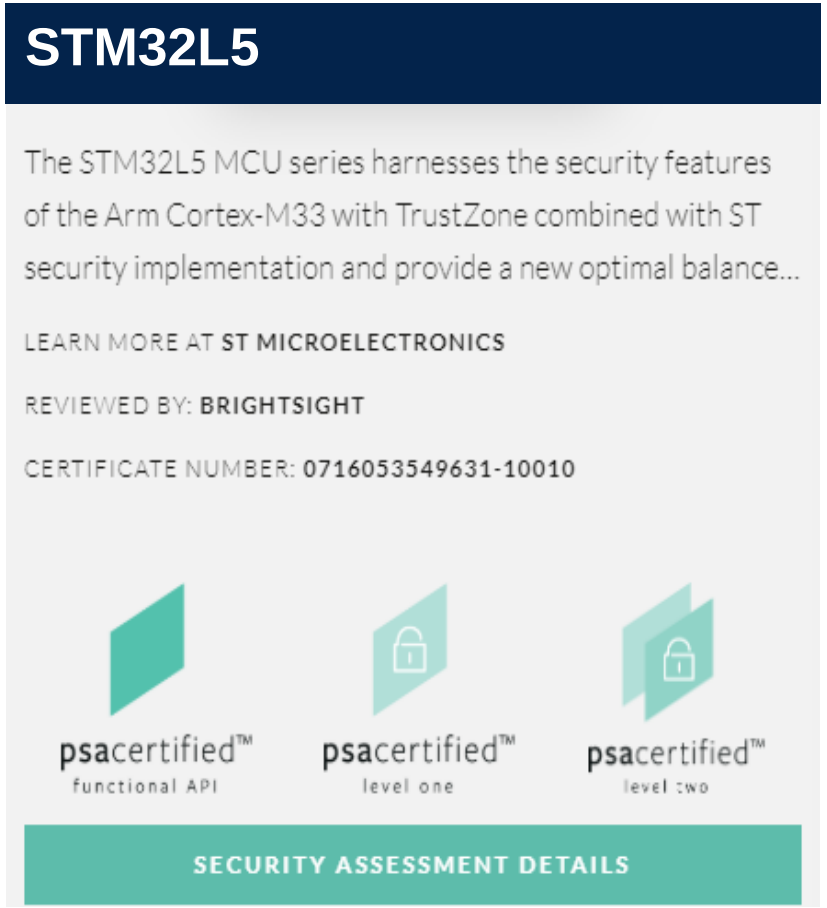
Wouter Slegers, CEO TrustCB B.V.

TrustCB B.V. | www.trustcb.com | trustcb@trustcb.com
Van den Berghlaan 48 | 2132 AT Hoofddorp | The Netherlands

life.augmented

First solution certified PSA level 2: STM32L5 with TF-M

- PSA certification is the ARM-based security assurance scheme for IoT devices and services.
- PSA provides 3 levels of assurance and robustness and a set of easy-to-use built-in security functions.
- The STM32L5 with TF-M is the 1st GP MCU platform to pass PSA levels 1 and 2 and PSA functional API.



Certifications summary

Certifications	Available Now	
ARM PSA • Level 1 (Self Assessment) • Level 2 (White box – Time Limited) • Level 3 (Smartcard-like)	ARM PSA Level 1 • STM32L4 • STM32L5	ARM PSA Level 2 • STM32L5 (TFM) ARM PSA API Compliant • STM32L5 (TFM)
SESIP • Level 1 (Self Assessment) • Level 2 (Black box) • Level 3 (White box – Time Limited) • Level 4 (White box) • Level 5 (Smartcard-like EAL4+)	SESIP Level 1 • STM32L4 (SBSFU)	SESIP Level 3 • STM32L4 (SBSFU)
COMMON CRITERIA • EAL5+ Smartcard	CC EAL5+ • STSAFE-A110 • STSAFE-TPM	

Evaluations		Available Now
PCI POS	Point of Sale application	• STM32L4

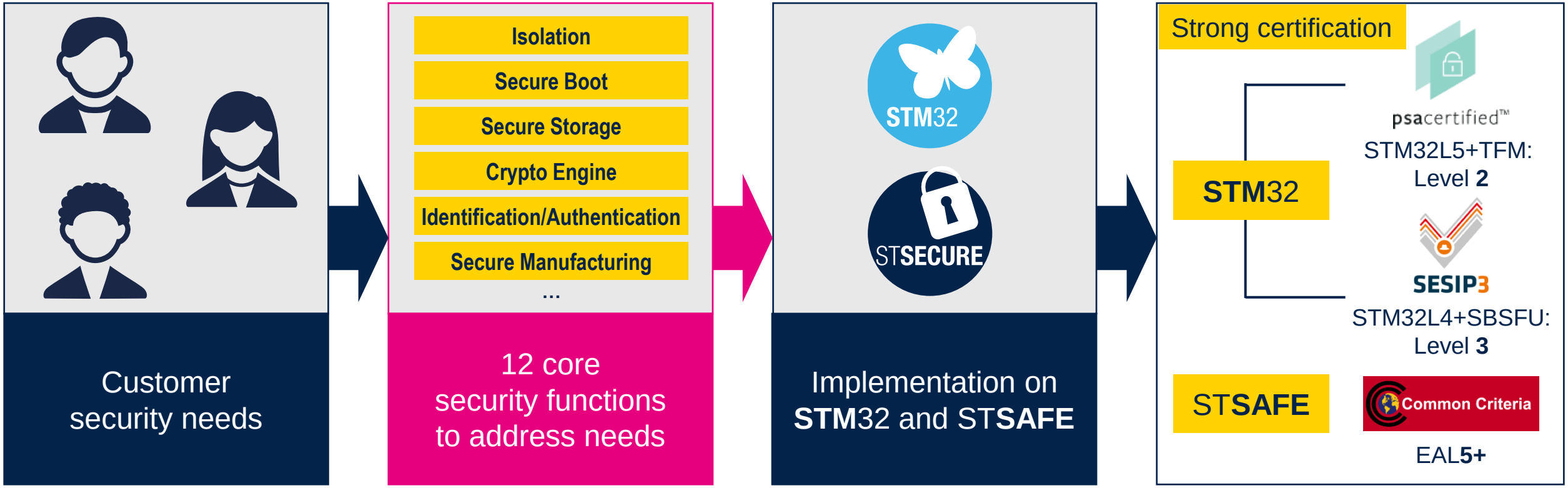
- Certification documents and links available at www.st.com/stm32trust
- Evaluations material is not public

Takeaways

life.augmented

STM32Trust security ecosystem
the one stop shop solution to implement security

First solution on the market certified PSA Level 2
First solution on the market certified SESIP Level 3



PSA = **P**latform **S**ecurity **A**rchitecture, by ARM
SESIP = **S**ecurity **E**valuation **S**tandard for **I**oT Platforms, by Global Platform

Thank you

Up-to-date information available
at www.st.com/stm32trust

life.augmented