STM32Trust security ecosystem for STM32

Agenda

1 STM32Trust Overview

2 Security Assurance

3 Enhancing STM32 Security assurance with STSECURE

4 Real-world examples

5 Security functions & offer

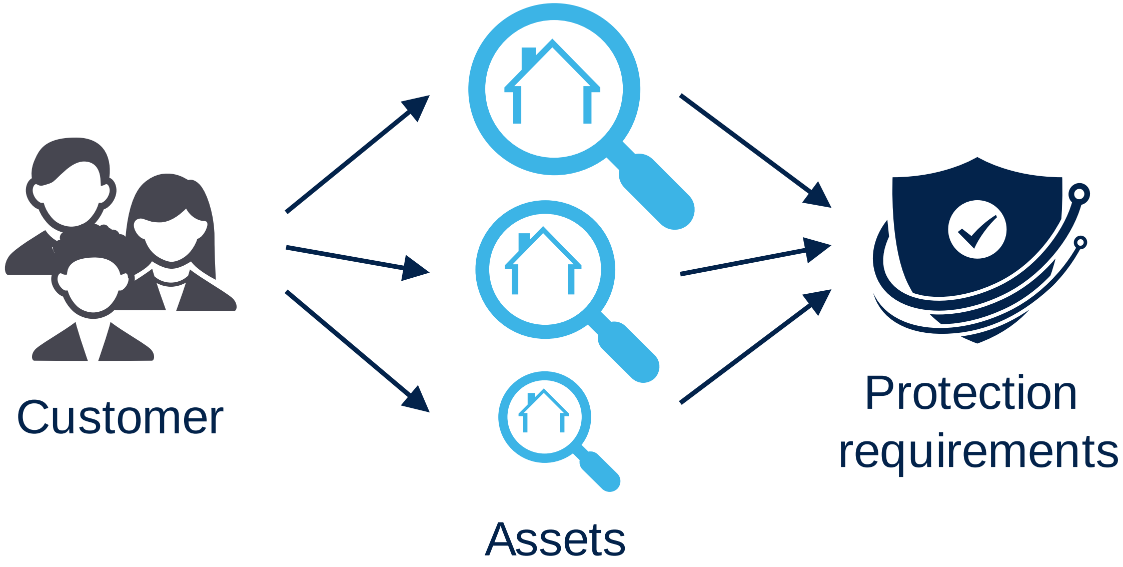
6 Focus on SFI and SBSFU

7 Security functions by product

life.augmented

What security means for us?

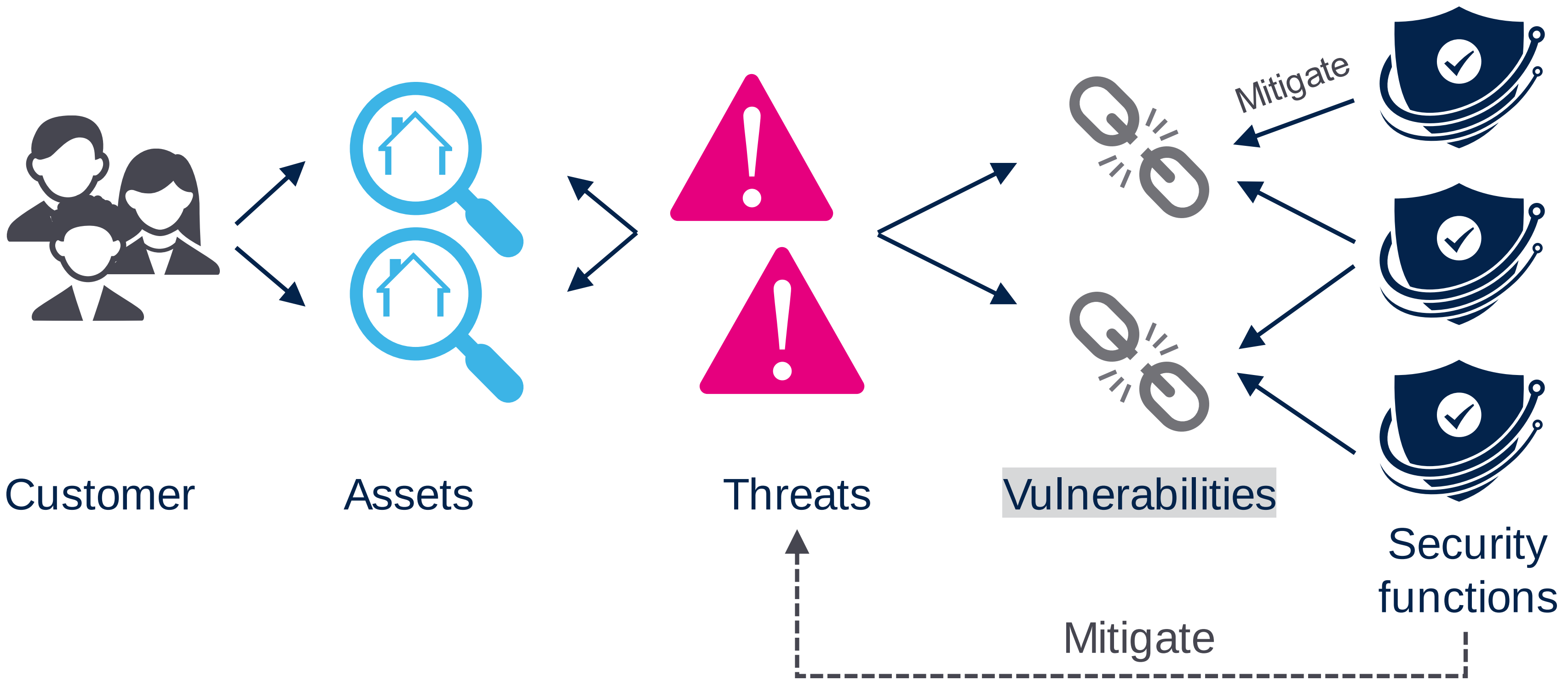
Security is protecting **Customer Assets**



- Assets guaranty our customer revenues
- Customers value their assets
- ST need to provide means to help our customers secure these assets

STM32 Trust

Security is a threat’ mitigation model



Threats exploit **Vulnerabilities** and damage **Assets**.

Protections mitigate **Vulnerabilities** and therefore might mitigate **Threats**.

Identify Assets, Threats and Vulnerabilities to define Protections and Countermeasures mitigating them to an acceptable level

life.augmented

What is STM32Trust ?

A security framework proposal

1. Identify threats according to customer assets categories
2. Propose mitigations via Security Functions & Services
3. Rely on recognized Security Assurance levels

To help customers protect their assets and
reach the required Security Assurance levels

Our goal:
protect our customer’s assets

Data

Confidentiality

Secrets

Regulations

Authenticity

IP

Software

Data

Processes

Secrets

Connectivity

Regulations

Network access

Data transfer

Confidentiality

Availability

System trust

Regulations

Reliability

Availability

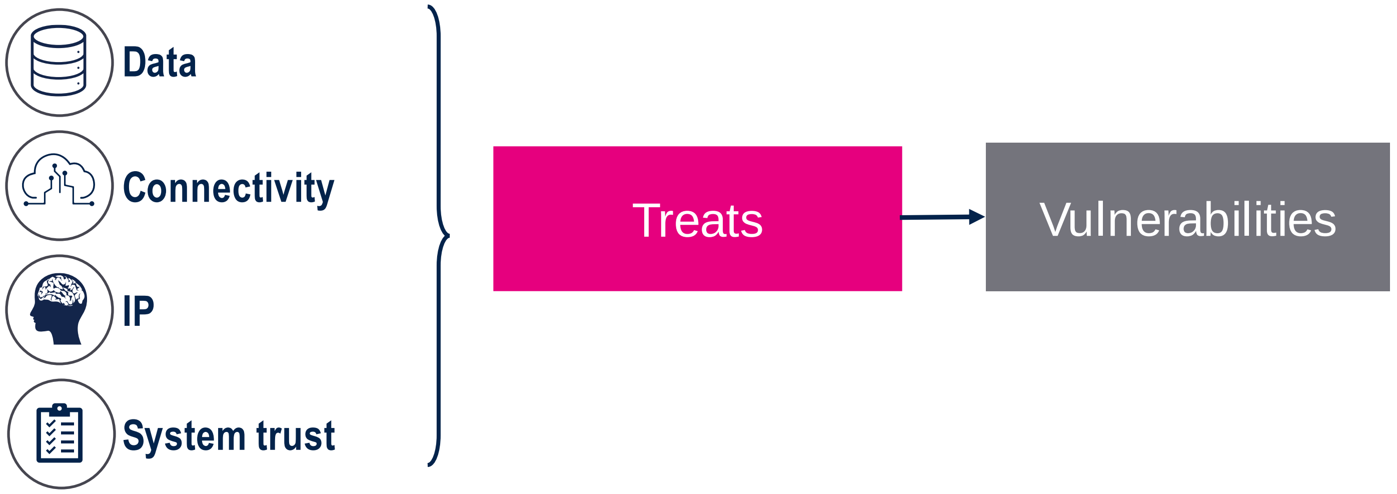
Authentication

Confidentiality

From assets to security functions

STM32Trust simplifies the mitigation model analysis with:

- Pre-analyzed threats and vulnerabilities
- Mitigation with ready to use Security Functions & Services



STM32Trust Security Functions

- Identification / Authentication / Attestation
- Application Life Cycle
- Secure Manufacturing
- Software IP Protection
- Silicon Device Life Cycle
- Secure Install / Update
- Secure Storage
- Isolation
- Abnormal Situations Handling
- Secure Boot
- Crypto Engine
- Audit / Log

STM32 Trust

From device to application security assurance level

- STM32Trust focusing on 2 de-facto product certification schemes:

SESIP

Security Evaluation Standard for IoT Platforms (SESIP)
Published by Global Platform for IoT devices

psacertified™

Platform Security Assurance by ARM® (PSA)
Focusing to protect IoT devices

- Aligned to multiple national & applicative security standards
- Fitting most customers application Security Assurance requirements

enisa THE EU CYBERSECURITY AGENCY

GLOBALPLATFORM

TRUSTED® COMPUTING GROUP

PCI

ETSI
EN 303 645

GSMA

UL
2900-1

FIPS Level 1 Validated 140-2

Common Criteria

IEC
IEC 62443

EMVCo

Security assurance & certifications

life.augmented

STM32 Trust

Product certification status

Certifications	Available Now	
ARM PSA • Level 1 (Self Assessment) • Level 2 (White box – Time Limited) • Level 3 (Physical attack)	ARM PSA Level 1 • STM32L4 • STM32L5	ARM PSA Level 2 • STM32L5 (TF-M) ARM PSA API Compliant • STM32L5 (TF-M)
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) • STM32L5 (TF-M)
Common Criteria FIPS Level 1 Validated 140-2 TRUSTED COMPUTING GROUP GSMA	STSECURE CC EAL5+ • STSAFE-A110 • STSAFE-TPM • ST4SIM FIPS-140-2 • STSAFE-TPM	TCG • STSAFE-TPM GSMA • ST4SIM

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

life.augmented

Enhancing STM32 security assurance with STSECURE

life.augmented

Security gradation

Crypto engine

- Basic crypto services embedded in dedicated ICs

Computer firmware

- Pure software countermeasures against remote software attacks mainly
- Self-evaluated solution

MCU / MPU with embedded security

Broad MCU portfolio

- Countermeasures against remote software and board level attacks
- **STM32Trust** Security framework
- MPU with ARM TrustZone
- **SESIP** & **PSA** Certifications
- Secure Programming services

STM32

MCU + Secure element

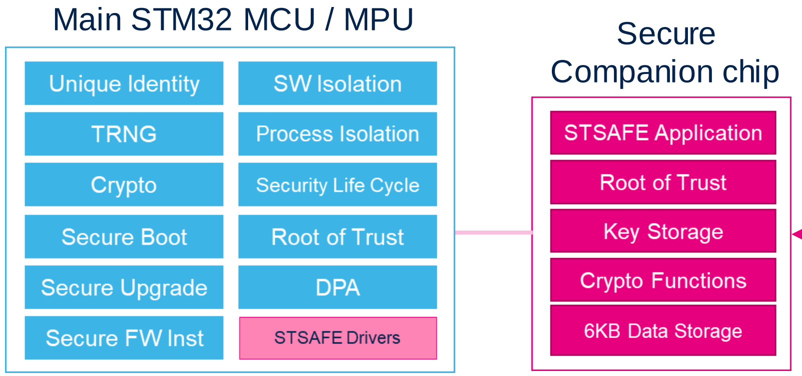
Trusted components

- Tamper resistance (Hardware & SoC)
- **Common Criteria**, **GSMA**, TCG certifications
- Proven against all attacks (remote software, board level and silicon level attacks)

Lifecycle Security Centric devices

- Secure development methodology
- Secure personalization & key provisioning
- Secure supply chain
- Certified Common Criteria sites

STSECURE



Main STM32 MCU / MPU

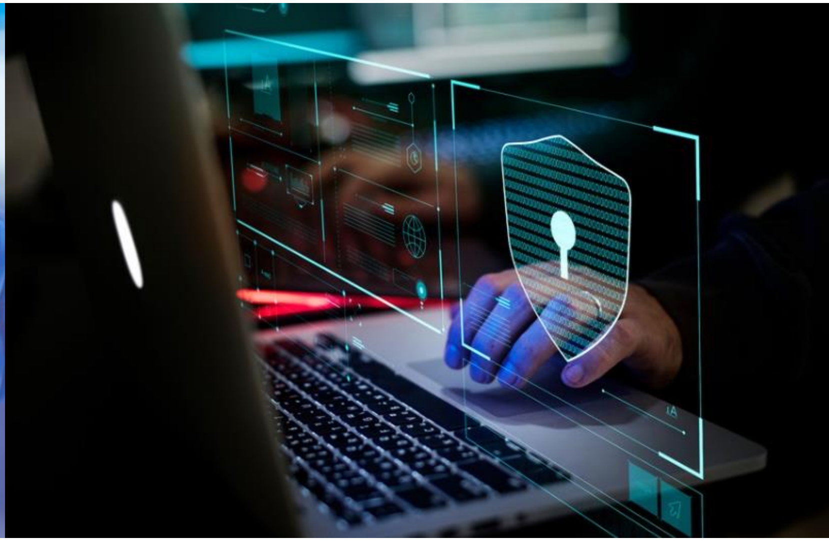
Unique Identity	SW Isolation
TRNG	Process Isolation
Crypto	Security Life Cyclo
Secure Boot	Root of Trust
Secure Upgrade	DPA
Secure FW Inst	STSAFE Drivers

Secure Companion chip

- STSAFE Application
- Root of Trust
- Key Storage
- Crypto Functions
- 6KB Data Storage

A large range of certified STM32 companion secure elements

Storage & Authentication	Communication	Platform integrity



STSAFE / ST4SIM

www.st.com/STSAFE www.st.com/ST4SIM

Security assurance & certifications

STM32 Trust	STM32 MCUs & MPUs	STSECURE	STSAFE Secure Element
Product Security Assurance*	psacertified™ SESIP3		Common Criteria EAL**5+**

Bridge for Application Assurance level

Application Security Assurance

enisa THE EU CYBERSECURITY AGENCY

GLOBALPLATFORM

TRUSTED® COMPUTING GROUP

PCI

ETSI

GSMA

UL 2900-1

FIPS Level 1 Validated 140-2

Common Criteria

IEC

IEC 62443

EMVCo

** product certifications depends on each products*

- **Security Evaluation Standard for IoT Platforms (SESIP)**
  - Published by Global Platform to align protection profiles to multiple security assurance schemes
- **Platform Security Assurance (PSA) by ARM©**
  - Focusing to protect IoT devices
- **Common Criteria EAL5+**
  - Enhance security with highest hardware resistance based on companion secure elements

Real-world examples

life.augmented

Customer example (1/6) focus on secure manufacturing

My asset is my product

Bob is the CEO of a company designing toys.
He needs to be protected against counterfeiting and device cloning

What Bob needs to achieve

- No firmware stolen during production
- No over-production by manufacturer
- No mean to program other devices
- No firmware stolen in the field

IP Protection

The Security Functions needed by Bob

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

STM32 Trust

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

My asset is my IP

Jon owns a company selling firmware
His firmware is of highest value, as his revenue comes from royalties. It features user-enable application options.

What Jon wants to achieve

- Protect its firmware
- Isolate his firmware from customer one

- Ensure independent firmware updates

- Set application macro-state in a way which cannot be altered

IP Protection

The Security Functions needed by Jon

- Software IP Protection
- Code Isolation

- Secure Install/Update

- Application Lifecycle

STM32 Trust

Customer example (3/6)
focus on secure maintenance & update

My asset is product trust

Mark’s company sells costly equipment.
He wants to offer remote maintenance and updates.
He wants to only update his equipment and would like to make sure only his firmware runs on his devices.

What Mark wants to achieve

- Ensure he connects to his equipment
- Ensure connection is liable
- Ensure the update is handled with integrity and authenticity
- Authenticity and integrity of firmware running on devices

Secure Connectivity

System integrity

The Security Functions needed by Mark

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

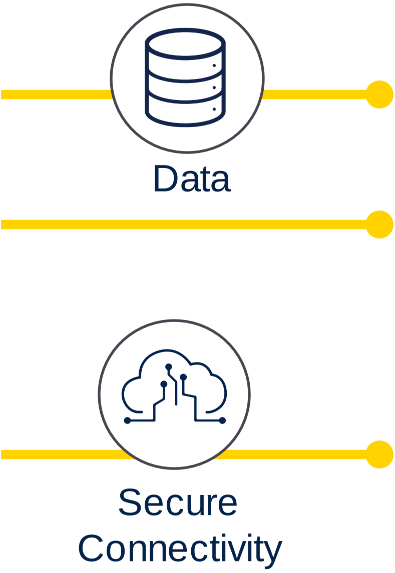
Customer example (4/6) focus on data management

My asset is my data

Oliver sells devices that report sensitive data to servers. Oliver needs to make sure the data cannot be exposed outside of his company.

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 remote access & control

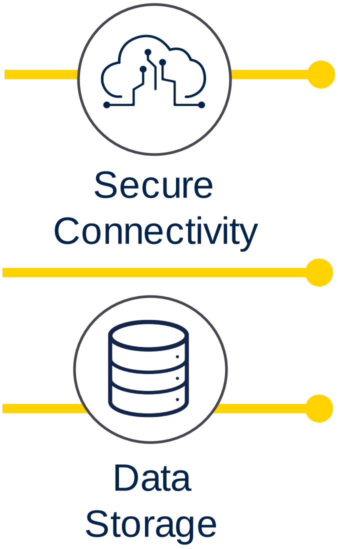
My asset is device trust

Rose controls her device fleet remotely.
She wants to be sure no malicious devices are part of the fleet and would like to have full control over the devices.
Ensuring device access control at anytime is key

What Rose wants to achieve

- That every device shows a unique identity
- Be able to authenticate the device
- Be able to attest the device access rights
- Secure device communication
- Ensure that identities and access right secrets cannot be leaked even at the manufacturing stage

The Security Functions needed by Rose



- Identification/Authentication/ Attestation
- Crypto Engine
- Secure Storage and Secure Manufacturing (Secure Personalization)

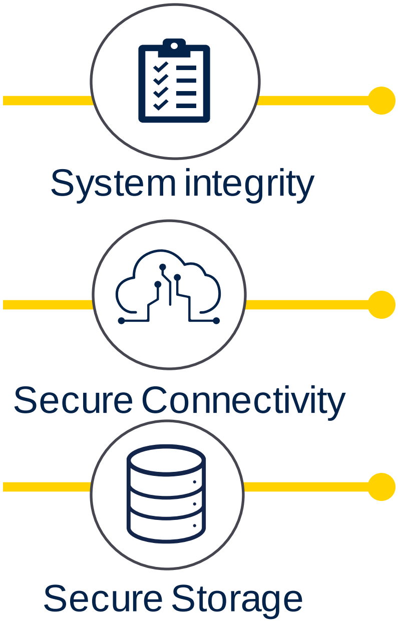
Customer example (6/6) focus on data protection

My asset is my data

Jack sell IoT devices that need to collect user data to run.
Jack’s devices and large-scale systems needs to be in line with regulations (such as GDPR) to be able to promote & sell devices.

What Jack wants to achieve

- Ensure platform integrity
- Ensure user data integrity
- Ensure user data is stored securely


System integrity

Secure Connectivity

Secure Storage

The Security Functions needed by Jack

- Secure Boot
- Abnormal Situations Handling

- Crypto Engine
- Identification/Authentication/Attestation

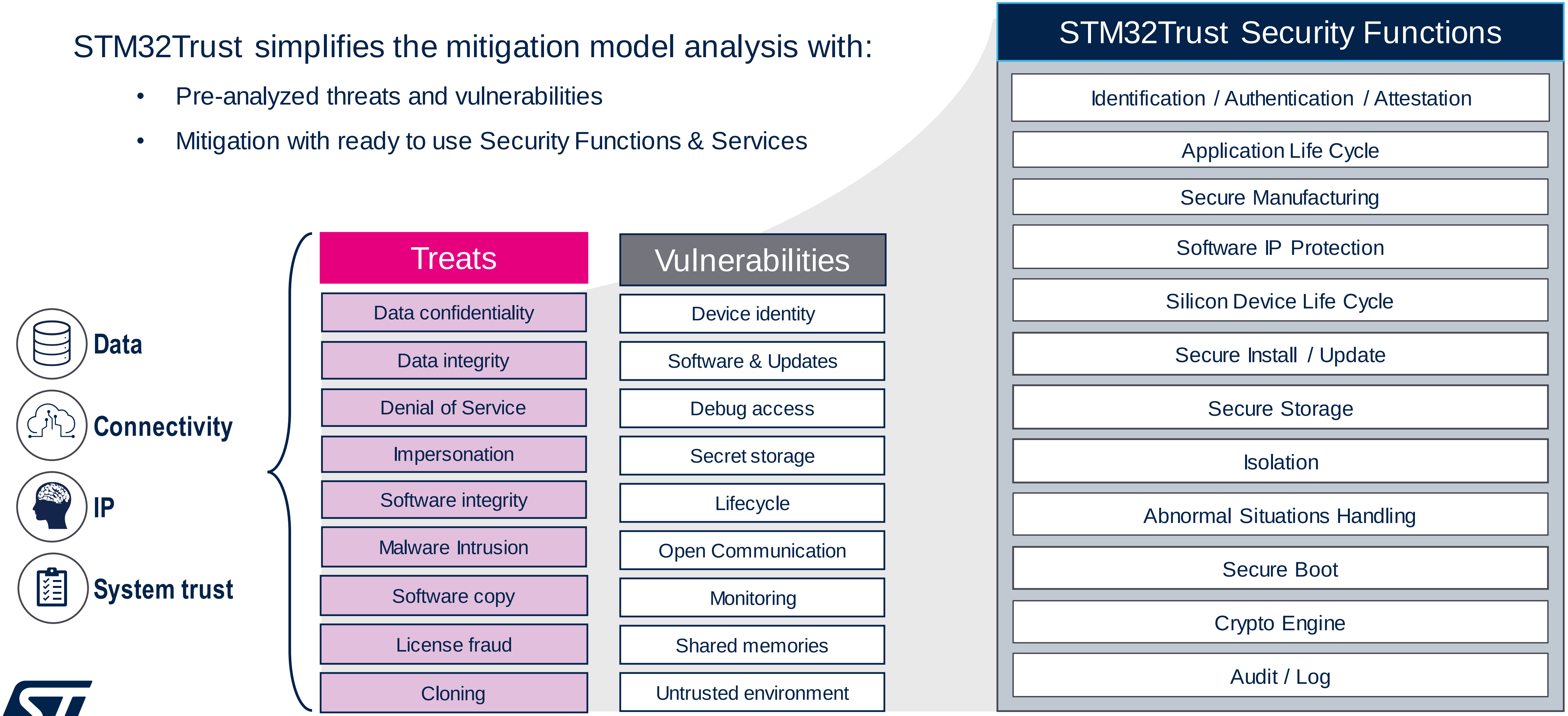
- Secure Storage

Security functions and ST offer

From assets to security functions

STM32Trust simplifies the mitigation model analysis with:

- Pre-analyzed threats and vulnerabilities
- Mitigation with ready to use Security Functions & Services



Data

Connectivity

IP

System trust

Treats

- Data confidentiality
- Data integrity
- Denial of Service
- Impersonation
- Software integrity
- Malware Intrusion
- Software copy
- License fraud
- Cloning

Vulnerabilities

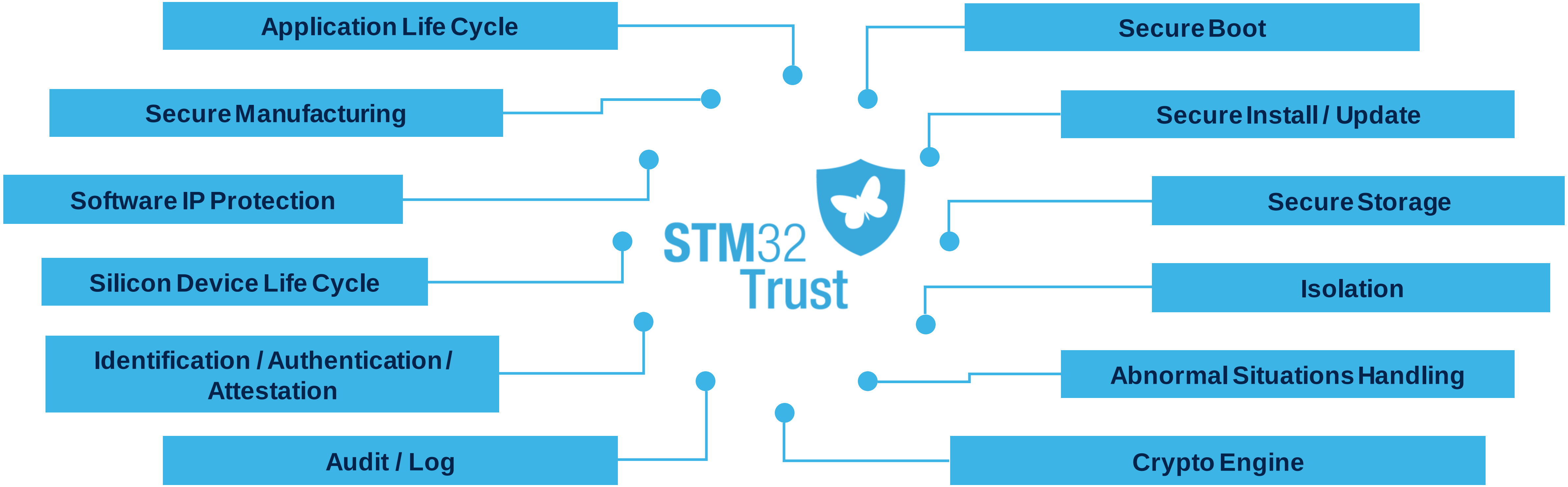
- Device identity
- Software & Updates
- Debug access
- Secret storage
- Lifecycle
- Open Communication
- Monitoring
- Shared memories
- Untrusted environment

STM32Trust Security Functions

- Identification / Authentication / Attestation
- Application Life Cycle
- Secure Manufacturing
- Software IP Protection
- Silicon Device Life Cycle
- Secure Install / Update
- Secure Storage
- Isolation
- Abnormal Situations Handling
- Secure Boot
- Crypto Engine
- Audit / Log

The 12 security functions

- STM32Trust brings **12 Security Functions** to align with Customer Use Cases and Security Assurance
- STM32Trust brings material (Documentation, Software, Tools…) to cover those 12 Security Functions
- Security functions to embed support of companion STSAFE secure elements



Application Life Cycle

Secure Manufacturing

Software IP Protection

Silicon Device Life Cycle

Identification / Authentication / Attestation

Audit / Log

Secure Boot

Secure Install / Update

Secure Storage

Isolation

Abnormal Situations Handling

Crypto Engine

www.st.com/STM32Trust

STM32 Trust

The 12 security functions definitions

1- Secure Boot

Ensure device application authenticity and integrity

2- Secure Install / Update

Secure Firmware Installation & Update
Integrity & Authenticity checks
License management

3- Secure Storage

Ability to securely store secrets like data or keys

4- Isolation

Isolation between trusted and non-trusted parts of an application

5- Abnormal Situations Handling

Ability to detect and react to abnormal hardware and software situations

6- Crypto engine

Cryptographic libraries supported by hardware

7- Audit / Log

Keep trace of security events in an unchangeable way

8- Identification / Authentication / Attestation

Unique identification of a device and/or software, and ability to detect its authenticity

9- Silicon Device Lifecycle

Control states to securely protect silicon device assets through its lifetime

10- Software IP Protection

Ability to protect a section or the whole software against illegal access.
Can be multi-tenant

11- Secure Manufacturing

Device provisioning or personalization in untrusted environment with overproduction control

12- Application Lifecycle

Protect application lifecycle states and assets

life.augmented

STM32 Trust

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 firmware attestation
One-way counter (decrement)	Supporting version control and anti-rolling using STSAFE-A
TPM Root of Trust	Ensure STM32 software integrity / MP1

2. Secure install / update

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
OP-TEE (Part of OpenSTLinux)	Trusted Execution Environment for STM32MP, embedding trusted application installation/update	MP1

STM32 Silicon Feature	Benefit for Security Function	STM32 Series
RDP (Read Protection)	Prevents a debugger from reading the secure install/update	F4/F7/WB/G0/G4/H7/L0/L4/L5
MPU (Memory Protection Unit)	Ensures privileged access to secure install/update	
MMU (Memory Management Unit)	Ensures privileged access to secure install/update	MP1
UBE (Unique Boot Entry)	Ensures the silicon always boots at the secure install/update location	G0/G4/L5
HDP (Hide Protect)	Temporal isolation blocking access to secure install/update code after execution	H7/G0/G4/L5
Trustzone	Runtime isolation technology allowing 2 distinct worlds, secure and non-secure	L5/MP1
Secure FSBL (First Stage Boot Loader)	Secure Boot loader, loaded and authenticated by secure boot rom code	MP1

STSAFE Feature	Benefit for Security Function
X509 certificate	Allow firmware attestation
One-way counter (decrement)	Supporting version control and anti-rolling using STSAFE-A
TPM Root of Trust	Ensure STM32 software integrity

3. Secure storage

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. Specific version of STM32L4 includes a Key Management service, i.e. Secure Key Storage	L4
TFM (Part of STM32CubeL5)	Trusted Execution Environment over Cortex-M, featuring Secure Storage service	L5
OP-TEE (Part of OpenSTLinux)	Trusted Execution Environment for STM32MP, featuring Secure Storage service	MP1

STM32 Silicon Feature	Benefit for Security Function	STM32 Series
TrustZone	TrustZone is a complete set of hardware mechanisms to isolate two main security application domains: one trusted (ensuring the Secure Storage) and one non-trusted	L5/MP1
Firewall	Simple isolation in two domains for RAM and flash. Permits to isolate Secure storage firmware from application	L0/L4
AES Key Storage	Write-only key registers in AES engine	L5
OTFDEC (On The Fly Decryption)	Decryption of encrypted content stored on external flash	L5/H7
HDP (Hide Protect)	Temporal isolation ensuring keys stored there are no more accessible	H7/G0/G4/L5

STSAFE Feature	Benefit for Security Function
Key Storage	Secured storage in secure element in STSAFE-A and TPM
Data packet encryption/decryption	Packets of data can be AES encrypted / decrypted with secret keys using STSAFE-A

4. Isolation

STM32 Firmware / Tool Part Number	Benefit for Security Function	STM32 Series
TF-M (Part of STM32CubeL5)	Trusted Execution Environment over Cortex-M, adding further software handling for application portions sandboxing	L5
OP-TEE (Part of OpenSTLinux)	Trusted Execution Environment for STM32MP, adding further software handling for application portions sandboxing	MP1

STM32 Silicon Feature	Benefit for Security Function	STM32 Series
MMU (Memory Management Unit)	Ensures privileged access to some portion of application – task isolations	MP1
MPU (Memory Protection Unit)	Ensures privileged access to some portion of application – task isolations	F4/F7/WB/G0/G4/H7/L0/L4/L5
HDP (Hide Protect)	Temporal isolation ensuring a portion of code is not R/W after first execution	H7/G0/G4/L5
TrustZone	Runtime isolation technology allowing 2 distinct worlds, secure and non-secure	L5/MP1
Firewall	Simple isolation in two domains for RAM and flash. Isolates portion of an application from the rest of the code	L0/L4
PcRoP (Proprietary code Read out Protection)	Ability to set some flash sectors as execute-only, thus preventing other sectors to read them	F4/L0/L4/H7/G0/G4
TZC (Trust Zone Controller)	Ability to isolate in particular Cortex-A cores from Cortex-M one	MP1

STSAFE Feature	Benefit for Security Function
Crypto Services	Crypto services isolated from STM32

5. Abnormal situations handling

STM32 Silicon Feature	Benefit for Security Function	STM32 Series
Anti tamper / Active tamper / Backup registers	Protect against a wide range of physical attacks on HW system outside the MCU. Erases backup registers information when tamper is detected	F4/F7/WB/G0/G4/H7/L0/L4/L5/MP1
RTC (Alarm timestamp)	Timestamp on tamper events, or internal events	
GPIO Locking	Lock of selected GPIO. Impossible to unlock until next reset. Ability to lock communication channels after tamper detection	
CSS (Clock Security System)	Internal clock available for secured program execution independently from external source clock	F4/F7/WB/G0/G4/H7/L0/L4/L5/MP1
ECC (Error Correction Code)	Robust memory integrity. Hardened protection against fault injection attacks thanks to error detection	
Temperature Sensor	Check if device is operating in expected temperature range. Hardened protection against temperature attacks	
Watchdogs	Independent watchdog and window watchdog for software timing control.	
PVD (Power Voltage Monitoring)	Monitors changes on power	

6. Crypto engine

STM32 Firmware / Tool Part Number	Benefit for Security Function	STM32 Series
X-CUBE-CRYPTOLIB	This ECCN 5D002-classified software is based on STM32Cube architecture package and includes a set of crypto algorithms based on firmware implementation (symmetric, asymmetric, hash…)	All, except MP1
DPA Resistant Crypto Library* (FIPS-140)	DPA resistant version of Cryptographic library. Available on specific part numbers after on demand adaptation	L4*
TF-M (Part of STM32CubeL5)	Trusted Execution Environment over Cortex-M, featuring Crypto algorithms	L5

STM32 Silicon Feature	Benefit for Security Function	STM32 Series
Symmetric Hardware Crypto Accelerators	Implements a given algorithm by hardware implementation, like AES for instance	F4/F7/WB/G0/G4/H7/L0/L4/L5/MP1
HASH	Hash algorithms implemented by hardware, like SHA	F4/F7/WB/G0/G4/H7/L0/L4/L5/MP1
PKA (Public Key Accelerator)	Asymmetric algorithms (Public key), implemented by hardware, for RSA/ECC/DH	WB/L5
OTFDEC (On The Fly Decryption)	Decryption of encrypted image on external flash	L5/H7
RNG (Random Number Generator)	True RNG done entirely by hardware	F4/F7/WB/G0/G4/H7/L0/L4/L5/MP1

STSAFE Feature	Benefit for Security Function
ECDH key pair generation and share secret generation	Assist device to establish TLS secure connections
RNG (Random Number Generator)	True certified RNG done entirely by hardware
Data packet encryption	AES encryption/decryption using hardware secret keys by the STSAFE-A

*: Contact your nearest sales office

7. Audit / log

STM32 Firmware / Tool Part Number	Benefit for Security Function	STM32 Series
TF-M (Part of STM32CubeL5)	Trusted Execution Environment over Cortex-M, featuring Audit/Log	L5
Customer can implement his software to handle this Security Function		All

STM32 Silicon Feature	Benefit for Security Function	STM32 Series
GTZC (Global TrustZone Controller)	Illegal access tracking and internal log/action	L5

8. Identification / authentication / attestation

STM32 Firmware / Tool Part Number	Benefit for Security Function	STM32 Series
TF-M (Part of STM32CubeL5)	Trusted Execution Environment over Cortex-M, featuring Attestation	L5

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
Device 96-bit Unique ID	Enables product traceability. Can be used for security key diversification	F4/F7/WB/G0/G4/H7/L0/L4/L5/MP1
Certificate (unique per chip)	Enables to authenticate a genuine STM32	H7/WB/L5/MP1
SSP (Secure Secret Provisioning)	Secure provisioning of OTP Secret values	MP1

STSAFE Feature	Benefit for Security Function
Device 7-Byte Unique ID	Enables product traceability.
ECDSA signature/verification based authentication	Allow device identity verification
X509 certificate	Allow attest device access rights

9. Silicon device lifecycle

STM32 Firmware / Tool Part Number	Benefit for Security Function	STM32 Series
STM32CubeProgrammer	Software tool able to control the RDP cycle	All

STM32 Silicon Feature	Benefit for Security Function	STM32 Series
BSEC & BootRom	Device life cycle managed through OTP and BSEC	MP1
RDP (Read Protection)	Ability to gradually choose accessible / modifiable features (like ability to debug, or ability to access Flash content) depending on RDP level	F4/F7/WB/G0/G4/H7/L0/L4/L5
WRP (Write Protection)	Flash sector becomes not writeable anymore when write protected and RDP2 is set	
HDP (Hide Protect)	Temporal isolation	H7/G0/G4/L5
PcRoP (Proprietary code Read out Protection)	Ability to set some flash sectors as execute-only	F4/L0/L4/H7/G0/G4

life.augmented

STM32 Trust

10. Software IP protection

STM32 Firmware / Tool Part Number	Benefit for Security Function	STM32 Series
TF-M (Part of STM32CubeL5)	Trusted Execution Environment over Cortex-M, adding further software handling for application portions sandboxing	L5
OP-TEE (Part of OpenSTLinux)	Trusted Execution Environment for STM32MP, adding further software handling for application portions sandboxing	MP1

STM32 Silicon Feature	Benefit for Security Function	STM32 Series
RDP (Read Protection)	Prevents the reading of a software stored in flash	F4/F7/WB/G0/G4/H7/L0/L4/L5
TrustZone	TrustZone is a complete set of hardware mechanisms to isolate two main security application domains: one trusted and one non-trusted. A software IP can be put in trusted area, becoming non-accessible from non-trusted one	L5/MP1
Firewall	Simple isolation in two domains for RAM and flash. Permits to protect a software IP	L0/L4
PcRoP (Proprietary code Read out Protection)	Ability to set some flash sectors as execute-only	F4/L0/L4/H7/G0/G4
MMU (Memory Management Unit)	Ensures privileged access to some portion of application – task isolations	MP1
MPU (Memory Protection Unit)	Ensures privileged access to some portion of application – task isolations	F4/F7/WB/G0/G4/H7/L0/L4/L5

life.augmented

STM32 Trust

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

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

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

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

12. Application lifecycle

STM32 Firmware / Tool Part Number	Benefit for Security Function	STM32 Series
TF-M (Part of STM32CubeL5)	Trusted Execution Environment over Cortex-M, featuring Secure Storage service. Application LifeCycle can be stored within such mechanism	L5
Customer can implement his software to handle this Security Function		All

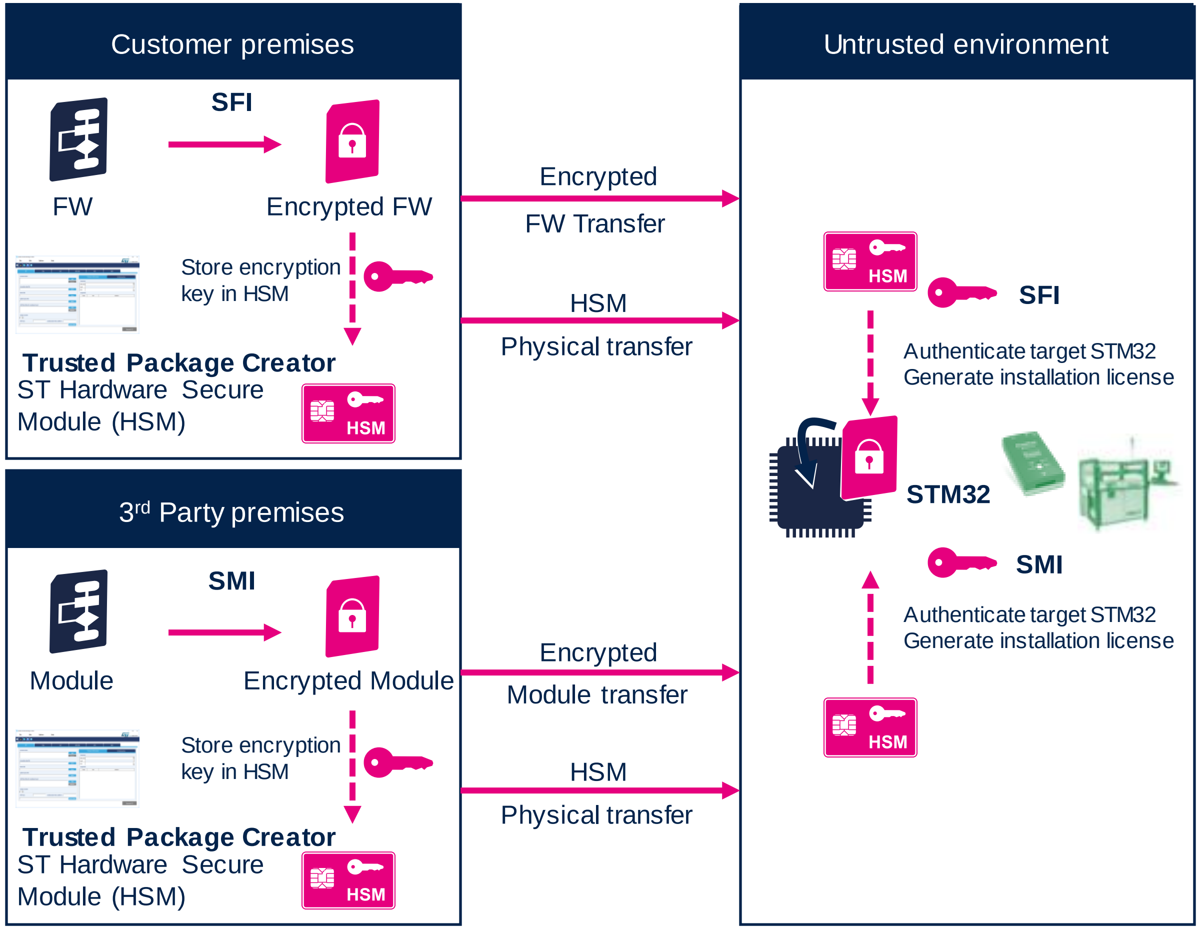
STM32 Silicon Feature	Benefit for Security Function	STM32 Series
OTP (One Time Programmable) Memory	OTP zones where application credentials or life cycle state can be stored.	F4/F7/WB/G0/G4/H7/L0/L4/L5/MP1

Focus on secure firmware installation & secure boot

life.augmented

Focus
embedded secure firmware install - SFI

Manage STM32 authentication, firmware decryption and installation



Customer premises

SFI

FW

Encrypted FW

Store encryption key in HSM

Trusted Package Creator
ST Hardware Secure Module (HSM)

HSM

Encrypted FW Transfer

HSM Physical transfer

3rd Party premises

SMI

Module

Encrypted Module

Store encryption key in HSM

Trusted Package Creator
ST Hardware Secure Module (HSM)

HSM

Encrypted Module transfer

HSM Physical transfer

Untrusted environment

HSM

SFI

Authenticate target STM32
Generate installation license

STM32

SMI

Authenticate target STM32
Generate installation license

HSM

Secure Loader
embedded services provisioned by ST
➔ Mass Market approach

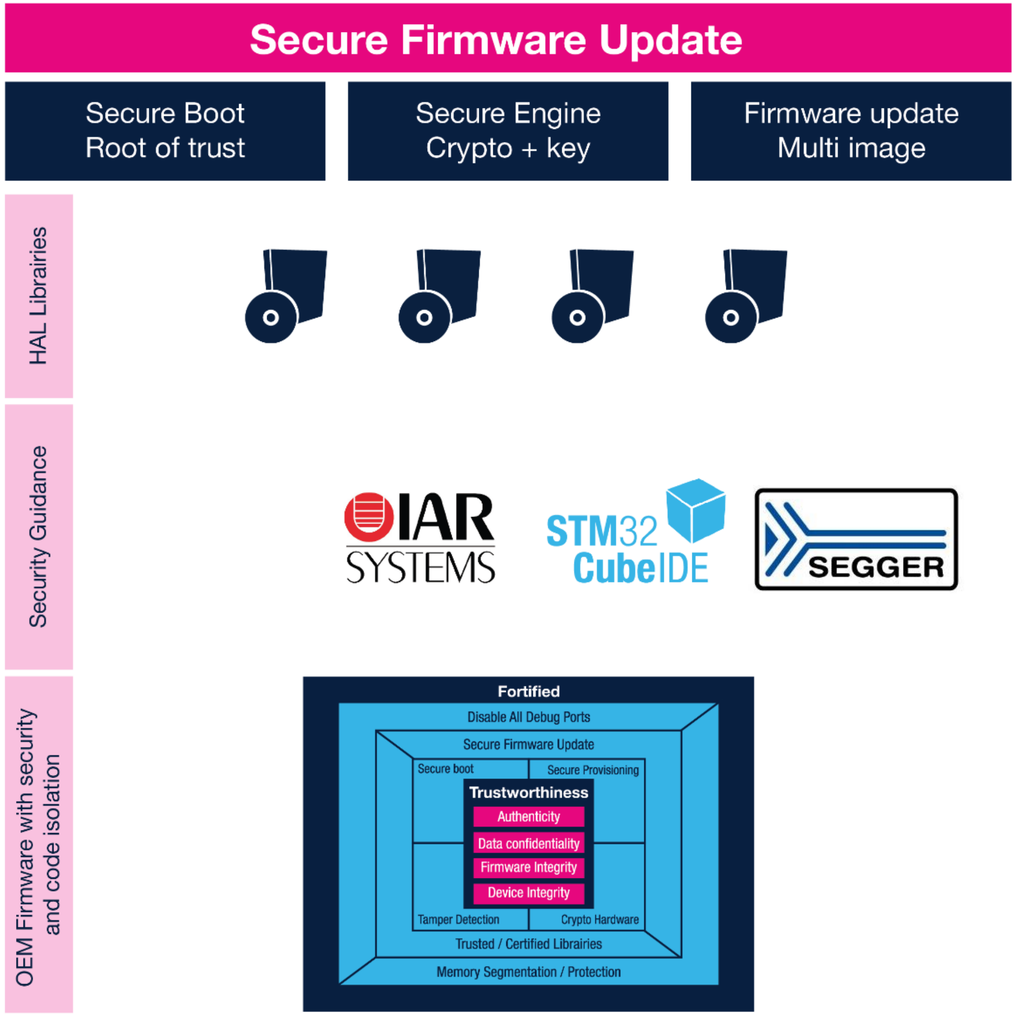
ST ecosystem
with
Encryption, HSM and programming tools

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

Protect 3rd party Software IP
(SMI)

life.augmented

Focus
secure boot secure FW update - SBSFU



Secure Firmware Update

Secure Boot
Root of trust

Secure Engine
Crypto + key

Firmware update
Multi image

HAL Librairies

Security Guidance

OEM Firmware with security
and code isolation

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

Security functions by product

life.augmented

Security functions by product

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	√	TF-M SPE	√
Isolation	√	🟦	√	OPTEE	√	TFM	√
Abnormal situations handling	√	🟦	√	🟦	√	🟦	
Crypto Engine	√	Crypto Libraries	√	OPTEE	√	Crypto Libraries TF-M	√
Audit/Log		🟦		🟦	√	TF-M	
ID/Auth/Attestation	√	🟦	√	🟦	√	TF-M Attestation	√
Silicon Device LifeCycle	√		√		√		
Software IP Protection	√	🟦	√	OPTEE	√	TF-M	
Secure Manufacturing	SFI (H7/L4) with STM32HSM		SSP with STM32HSM		SFI with STM32HSM		√
Application LifeCycle	√	🟦	√	🟦	√	🟦	√

🟦 *Firmware to be developed by user*

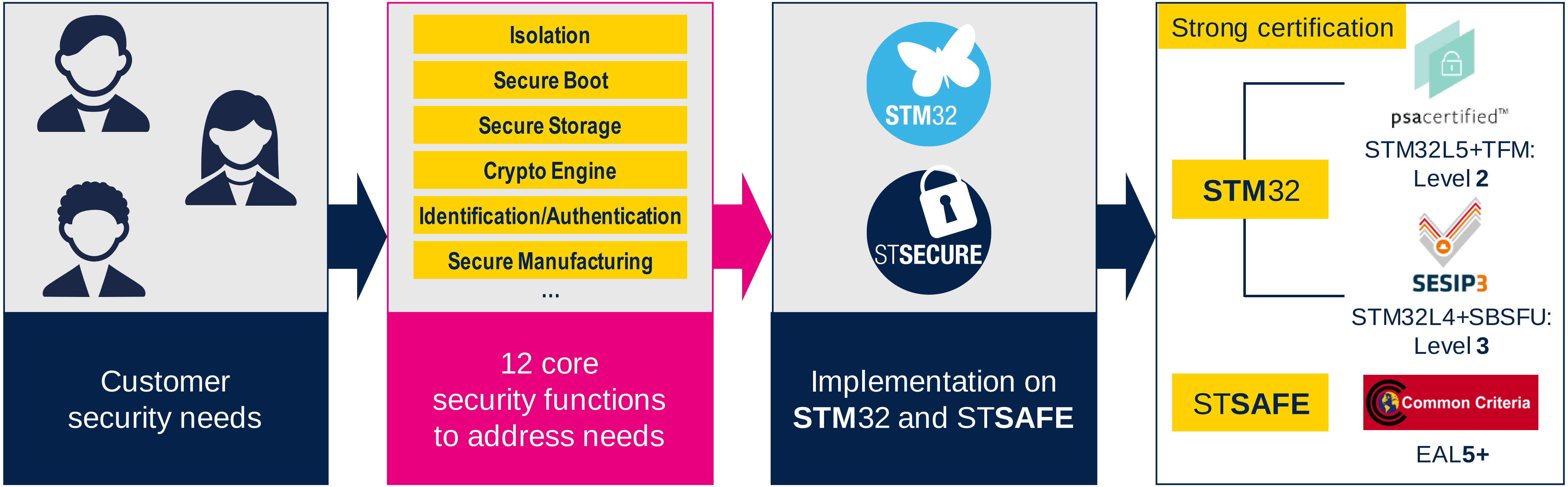
🟨 *Reference firmware proposed by ST*

life.augmented

Takeaways

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



Customer security needs

Isolation

Secure Boot

Secure Storage

Crypto Engine

Identification/Authentication

Secure Manufacturing

...

12 core security functions to address needs

STM32

STSECURE

Implementation on **STM32 and STSAFE**

Strong certification

STM32

psacertified™

STM32L5+TFM: Level **2**

SESIP3

STM32L4+SBSFU: Level **3**

ST**SAFE**

Common Criteria

EAL**5+**

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

Thank you

Latest information available at www.st.com/stm32trust

life.augmented