

STM32
Trust



life.augmented

STM32Trust security ecosystem



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.

Customer examples



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



- Isolate his firmware from customer one
- Ensure that his firmware can independently be updated
- Set application macro-state in a way which cannot be altered

The Security Functions needed by Jon



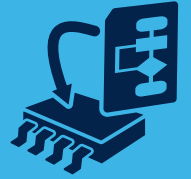
- Isolation
- Software IP Protection
- Secure Install/Update
- Application Lifecycle

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



- 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)



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



- Ensure platform integrity
- Ensure user data is not exposed while communicating
- Ensure user data is stored securely

The Security Functions needed by Jack



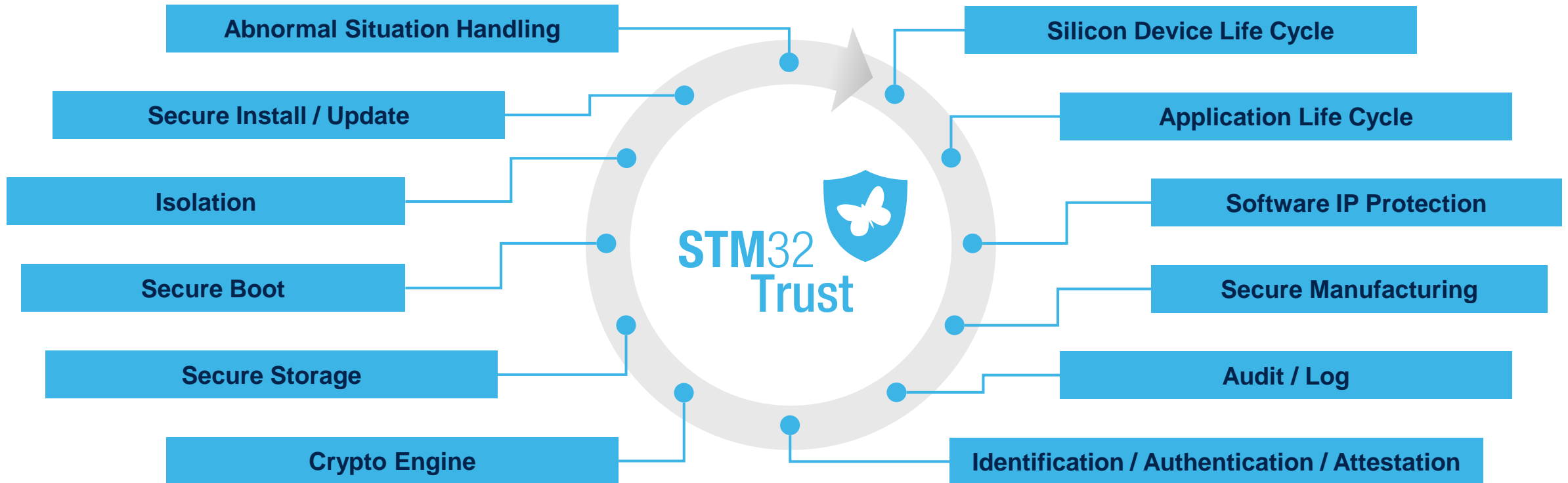
- Secure Boot
- Abnormal Situations Handling
- Crypto Engine
- Identification/Authentication/Attestation
- Secure Storage

Security functions and ST offer






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



ST scalable security offer


Non Invasive / Logical Attack Resistant

 Product Invasive Attack Resistant

 Silicon Invasive Attack Resistant



IEC 62443-4-2 Level

SL1

SL2

SL3



MCU / MPU Software

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



Crypto Hardware

- Basic crypto accelerators



MCU / MPU with Enhanced Security

- Embedded hardware crypto services
- Countermeasures against remote software and board level attacks
- Integrated One Time Programmable (OTP) memory
- Secure Boot and firmware update
- ARM TrustZone and code isolation
- Trusted Execution Environment (TEE) capabilities
- Self-evaluated solution



+



Secure MCU

- Strong trusted components**
- Crypto functions isolated from MCU
 - Secure nonvolatile data / key store
 - Tamper proof solution (Hardware and Code)
 - Proven against all attacks (Remote software, Board level and Silicon level attacks)
 - Independently certified : Common criteria, EMVCo, ...
- Secure Manufacturing and Provisioning**
- Secure personalization and key provisioning services
 - Secure supply chain
 - Site certified Common criteria

Evaluations and certifications





IEC 62443-4-2 component identification and authentication control

Feature	SL1	SL2	SL3	SL4
Identify and authenticate human users	X	X	X	X
Component shall enable the management of accounts	X	X	X	X
Component shall support the management of identifiers	X	X	X	X
Component shall support authenticator management	X	X	X	X
Password based authentication with defined password strength	X	X	X	X
Obscure authentication feedback during authentication process	X	X	X	X
Enforce unsuccessful login attempt limit, lock account	X	X	X	X
Provide warning message to individuals attempting to access the system	X	X	X	X
Uniquely identify and authenticate all human users		X	X	X
Software process and device identification and authentication		X	X	X
When PKI is used, the component shall integrate with PKI infrastructure		X	X	X
When PKI is used, the component shall check validity of certificates		X	X	X
Support for symmetric key based authentication		X	X	X
Unique software process and device identification and authentication			X	X
Authenticators shall be protected by hardware mechanisms			X	X
Prevent password reuse for configurable number of generations human users			X	X
Protection of public key via hardware			X	X
Protection of symmetric key data via hardware			X	X
Multifactor authentication for all interfaces				X
Prevent password reuse for configurable number of generations software process or device				X

STM32

STSAFE

Certifications	Available Now	
 <p>ARM PSA</p> <ul style="list-style-type: none"> Level 1 (Self Assessment) Level 2 (White box – Time Limited) Level 3 (Smartcard-like) 	<p>ARM PSA Level 1</p> <ul style="list-style-type: none"> STM32L4 STM32L5 	<p>ARM PSA Level 2</p> <ul style="list-style-type: none"> STM32L5 (TFM) <p>ARM PSA API Compliant</p> <ul style="list-style-type: none"> STM32L5 (TFM)
 <p>SESIP</p> <ul style="list-style-type: none"> Level 1 (Self Assessment) Level 2 (Black box) Level 3 (White box – Time Limited) Level 4 (White box) Level 5 (Smartcard-like EAL4+) 	<p>SESIP Level 1</p> <ul style="list-style-type: none"> STM32L4 (SBSFU) 	<p>SESIP Level 3</p> <ul style="list-style-type: none"> STM32L4 (SBSFU)
 <p>COMMON CRITERIA</p> <ul style="list-style-type: none"> EAL5+ Smartcard 	<p>CC EAL5+</p> <ul style="list-style-type: none"> STSAFE-A110 STSAFE-TPM 	
Evaluations	Available Now	
 <p>PCI POS Point of Sale application</p>	<ul style="list-style-type: none"> STM32L4 	

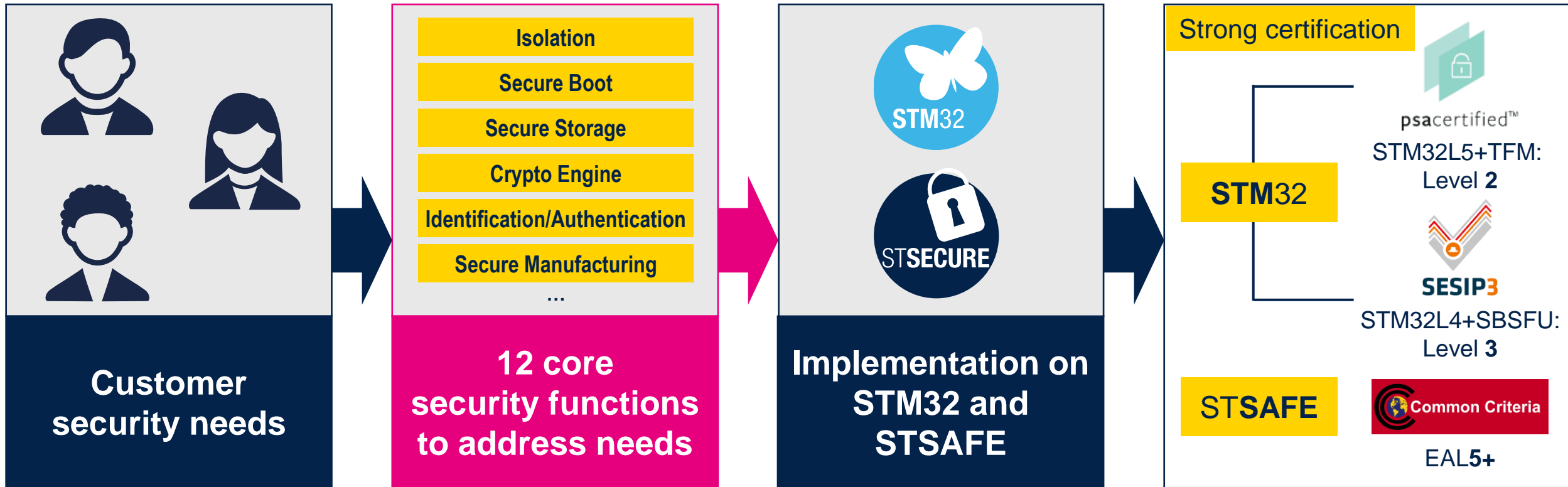
Takeaway



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



Questions



Thank you

© STMicroelectronics - All rights reserved.

ST logo is a trademark or a registered trademark of STMicroelectronics International NV or its affiliates in the EU and/or other countries.

For additional information about ST trademarks, please refer to www.st.com/trademarks.

All other product or service names are the property of their respective owners.



life.augmented