STM32Trust offers a robust multi-level strategy to enhance security in new product designs utilizing our STM32 Microcontrollers & microprocessor augmented with STSAFE secure elements.

STM32Trust is the security framework combining our knowledge, ecosystem and security services.

The solution offers a complete toolset for code and execution protection, ensures IP protection, data secured, and validated credentials are used, and helps to get firmware authenticity and secure firmware update.

A whole security ecosystem around STM32

THE SECURITY FUNCTIONS
STM32Trust offers results for accurate analysis of customer cases, ending up in the coverage of the base 12 security functions required for their needs

- Secure Boot
- Secure Install/Update
- Secure Storage
- Isolation
- Abnormal situations handling
- Crypto Engine
- Audit/Log
- Identification / Authentication / Attestation
- Silicon Device Lifecycle
- Software IP Protection
- Secure Manufacturing
- Application Lifecycle

www.st.com/stm32trust
STM32Trust | MORE TRUST WITH STM32

1- **Secure boot**
   Ability to ensure the authenticity and integrity of an application that is inside a device

2- **Secure Install/Update**
   Installation or update of firmware with initial checks of integrity and authenticity before programming and executing

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 abnormal situations (both hardware and software) and to take adapted decisions like secrets removals

6- **Crypto Engine**
   Ability to process cryptographic algorithms, as recommended by a security assurance level

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, inside the device or externally

9- **Silicon Device Lifecycle**
   Control states to securely protect silicon device assets through a constrained path

10- **Software IP Protection**
   Ability to protect a section or the whole software against external or internal reading. Can be multi-tenant

11- **Secure Manufacturing**
   Initial device provisioning in unsecured environment with overproduction control. Potential secured personalization

12- **Application Lifecycle**
   Define unchangeable incremental states to securely protect application states and assets

---

**CERTIFICATIONS**

ST is fully committed at certifying its solutions by independent recognized authority.

To discover this complete offer, please visit www.st.com/stm32trust

---

**Available now**

<table>
<thead>
<tr>
<th>Security Function</th>
<th>STM32F4/F7/L1/WB/G0/G4/H7/L0/L4</th>
<th>STM32MP1</th>
<th>STM32L5 with TrustZone</th>
<th>+ STSAFE-A/TPM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Boot</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>Secure Install/Update</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>Secure Storage</td>
<td>❌ (L0/L4/H7/G0/G4)</td>
<td>❌ (L0/L4/H7/G0/G4)</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>Isolation</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>Abnormal situations handling</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>Crypto Engine</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>Audit/Log</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>ID/Auth/Attestation</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>Silicon Device LifeCycle</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>Software IP Protection</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>Secure Manufacturing</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>Application LifeCycle</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
</tbody>
</table>

*All those solutions are defined at www.st.com/stm32trust

---

**CERTIFICATIONS**

- **ARM PSA**
  - Level 1
    - STM32L4
    - STM32L5
  - Level 2
    - STM32L5 (TFM)
  - API Compliant
    - STM32L5 (TFM)

- **COMMON CRITERIA**
  - CC EAL5+
    - STSAFE-A110
    - STSAFE-TPM

- **SESIP**
  - Level 1
    - STM32L4 (SBSFU)
  - Level 3
    - STM32L4 (SBSFU)

- **PCI**
  - Point of Sale application
    - STM32L4

---

Order code: FLSTM32TRUST0320

For more information on ST products and solutions, visit www.st.com/stm32trust

© STMicroelectronics - March 2020 - All rights reserved

The STMicroelectronics corporate logo is a registered trademark of the STMicroelectronics group of companies

All other names are the property of their respective owners