STSAFE-TPM is a widely deployed, standardized Trusted Platform Module which is a key enabler of security in personal computers and servers. It is a perfect fit for ecosystems built on Windows and Linux operating systems.

Certified by Common Criteria, TCG and FIPS, all STSAFE-TPM secure elements meet security and regulatory requirements. Based on a ST33 hardware, the product portfolio is qualified for consumer, industrial and automotive applications.

**KEY BENEFITS**
- Integration with Linux and TCG TPM software stack
- Common Criteria-, TCG- and FIPS-certified
- Long lifetime products (up to 20 years)
- Delivered with keys and certificates already loaded

**KEY APPLICATIONS**
- Industrial and personal computing
- PC, servers and tablets
- Peripherals
- Network equipment
  - Routers and switches
  - Base stations and access points
- Home & building automation
  - Gateways
- Medical devices
- Automotive solutions

www.st.com/stsafe-tpm
STSAFE-TPM is a proven solution offering standardized trusted computing services (ISO / IEC 11889) which is ideal for Windows or Linux-based platforms.

**Key features**
- Extended cryptography support for long lifecycle devices (ECC384, SHA2-384, SHA3, AES 256)
- TPM firmware upgrade possible through fault tolerant loading process
- TPM firmware and critical data self recovery (NIST SP800-193)
- Penetration tests conducted at the highest CC assurance level (AVA_VAN.5)
- Available with TCG compliant SPI or I²C interface
- Consumer / AEC-Q100 / Industrial qualification
- Available in standardized and small footprint packages like WLCSP
- Extended operating temperature range (-40°C to 105°C)

**Ecosystem**
- A full development kit is available for easy integration
- Expansion board (STPM4RasPI) for Raspberry Pi® and STM32MP1 MPU for both SPI and I²C interfaces
- Software package with driver and utilities (communication driver and firmware upgrade)
- Smooth system integration thanks to Windows and Linux support, TCG Open Source or Third party TPM stacks

**Certification**
- First CC-certified TPM according to Trusted Computing Group protection profile augmented with resistance to high-potential attacks (AVA_VAN.5)
- FIPS 140-2 certificate level 2 with physical security level 3
- TCG certification

---

**Product table**

<table>
<thead>
<tr>
<th>Product name</th>
<th>Application segment</th>
<th>OS support</th>
<th>Interface</th>
<th>Certification</th>
<th>Package options</th>
<th>Operating temperature range</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST33TPHF20/2E</td>
<td>TPM / network, printer, IoT</td>
<td>TPM 1.2 / TPM 2.0</td>
<td>TCG SPI (33MHz)  TCG PC (400KHz)</td>
<td>CC EAL4+, TCG, FIPS 140-2</td>
<td>TSSOP28, VQFN32</td>
<td>-40 to +105°C</td>
</tr>
<tr>
<td>ST33TPHF2X</td>
<td></td>
<td>TPM 2.0</td>
<td>TCG SPI (18MHz)  TCG PC (200KHz)</td>
<td>CC EAL4+ (high attack potential), TCG, FIPS 140-2</td>
<td>VQFN32</td>
<td></td>
</tr>
<tr>
<td>ST33GTPMA</td>
<td>Automotive</td>
<td></td>
<td></td>
<td></td>
<td>TSSOP20</td>
<td></td>
</tr>
<tr>
<td>ST33GTPMI</td>
<td>Industrial</td>
<td></td>
<td></td>
<td></td>
<td>WLCSP</td>
<td></td>
</tr>
</tbody>
</table>

---

ST and ST logo are trademarks or registered trademarks 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.