life.augmented

STSAFE
for authentication and embedded security

Contents

Introduction to Authentication

Authentication products are secure elements to be used for brand protection, platform integrity, PC and IT security, secure connection to cloud and remote servers.

With superior ability to store and handle secrets, authentication products contribute to safeguarding a company's image, reputation and revenues against cloning and theft, and ensure secure and trusted services.

PROTECTING BUSINESSES & BRANDS

A simple mistake in implementing security measures or incorrect data measurement can generate a denial of services impacting either end-user safety or privacy, and can affect a company's brand reputation. To help companies maintain their reputation and protect their brand, ST offers a wide portfolio of products and solutions, as well as a complete set of hardware and software development tools.

HOW ST'S SOLUTIONS ADDRESS SECURITY THREATS

Threats

- Device cloning or counterfeiting
- Device integrity or data corruption
- Loss of confidential information

ST secure elements

Security services

- Authentication, unique ID
- Secure communication
- Platform integrity
- Usage monitoring
- Secure storage
- Key provisioning

Security services benefits

- Revenue protection
- Reputation
- Continuity and reliability of services
- Protection of customer assets and privacy
- Compliance to regulation
- Avoid additional investments in secure infrastructures

STSECURE

14+ billion
units of Secure MCUs shipped to date

STSAFE portfolio and markets

A SCALABLE SECURITY OFFER FOR BRAND PROTECTION AND EMBEDDED SYSTEMS

STSAFE is a secure element product range providing authentication, confidentiality and platform integrity services to protect OEMs against cloning, counterfeiting, malware injection and unauthorized production.

Compliant with the most demanding security certifications, STSAFE secure elements are turnkey solutions developed through a trusted supply chain with pre-provisioned secrets and certificates, that include a set of software librairies and drivers for secure, seamless integration.

STSAFE ENABLING END-TO-END SECURITY

Building secure and trusted systems, ST offers a full range of secure elements addressing multiple applications, from embedded platforms to gateways and servers.

Integrated into device design and connected to its processing unit, STSAFE secure elements help authenticate devices and ensure platform integrity and data confidentiality with end to end security.

PRODUCT PORTFOLIO

- STSAFE-A optimized for embedded systems
- STSAFE-J flexible with Java platform
- STSAFE-TPM standardized for trusted computing

STSAFE MAPPING IN MARKET SEGMENTS

STSAFE-TPM Standardized
TCG standardized platform for trusted computing and embedded systems

STSAFE-J Flexible
Flexible Java™ platform with optional default applet

STSAFE-A Optimized
Tuned for brand protection and secure connection

Consumer
consumables, accessories, printers, computers

Industrial
environmental sensors, actuators, factory automation

Infrastructure
gateway, base station, utilities

STSAFE-A optimized

Running on a CC EAL5+ secure element, STSAFE-A is a highly secure authentication solution with security features certified by independent third-parties.

Its command set is tailored to ensure strong device authentication, to monitor device usage, to assist a nearby host secure channel establishment (TLS), and to safeguard host platform integrity.

KEY BENEFITS

- Optimized for consumable and small platforms
- Personalization services
- Seamless integration using librairies compatible with STM32 and other general-purpose MCUs
- Available at eDistribution
- HW CC EAL5+-certified

STSAFE-A, OPTIMIZED TO PROTECT YOUR BUSINESS

STSAFE-A ecosystem for seamless security

The STSAFE-A product family is a secure solution with state-of-the-art security features that prevent the counterfeiting of genuine peripherals and IoT devices.

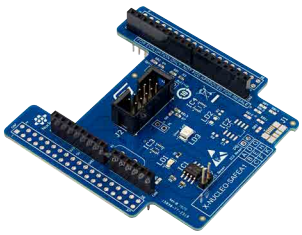
Key features

- Strong authentication (compliant with QI V2.0 and Matter)
- Secure channel establishment (TLS)
- Signature verification
- Decrement counter
- Secure data storage

Ecosystem

STSAFE-A ecosystem contains a complete set of tools for seamless integration:

- ODE STM32 Expansion board (X-NUCLEO-SAFExx)
- STM32 Cube development ecosystem (X-CUBE-SAFExx software package)
- Pre-personalized STSAFE-A available for fast evaluation
- Personalization service of customer's certificates and configuration at ST factory with no extra cost



Learn more at **www.st.com/stsafe-a**

Product portfolio

Product name	OS support	Interface	Certification	Package options	Operating temperature range	NVM storage
STSAFE-A110	• Strong authentication • Secure connection establishment • Usage monitoring • Host platform integrity	I^2C	HW CC EAL5+	SO8N DFN8 2x3	From -40 to +105 °C	6 Kbytes

STSAFE-J
flexible

STSAFE-J is a flexible solution based on Java Card operating system, which is freely available for customers who plan to run their own applet.

STSAFE-J is also available with a generic applet ensuring securing on the host platform: strong authentication, secure connection establishement, usage monitoring and platform integrity.

KEY BENEFITS

- Flexible Java solution with ST generic or customer-specific applets
- Seamless integration using librairies compatible with standard MCUs and MPUs
- HW CC EAL5+-certified

STSAFE-J, A FLEXIBLE JAVA PLATFORM

STSAFE-J100 with certified protection profiles

Key features

- CC EAL5+ certified platform
- Java 3.0.4 and GP 2.1.1 certified platform
- Generic ST applet:
  - Authentication
  - Secure connection
  - Secure data storage
  - Personalization service
- Customer specific applet

Development tools and services

- Expansion board compatible with STM32 Nucleo and Arduino boards
- Example code and librairies to be embedded in application microcontrollers (PKCS11 software package)

Learn more at **www.st.com/stsafe-j**

Product portfolio

Product name	OS support	Interface	Certification	Package options	Operating temperature range	NVM storage
STSAFE-J100	GP 2.1.1 / JC 3.0.4	Contact ISO/IEC 7816, I²C	HW CC EAL5+	DFN8 VFQFPN32	-40 to + 105 °C	80 Kbytes

STSAFE-TPM standardized

STSAFE-TPM family is a widely used and standardized Trusted Platform Module that serves as a cornerstone of security for PCs and servers.

TPMs are required by Microsoft Windows and natively supported by Linux operating systems.

The independent security certifications by Common Criteria, TCG and FIPS provide a high level of confidence and can be leveraged to meet regulatory requirements.

KEY BENEFITS

- Proven and standardized security solution
- High assurance based on Common Criteria, TCG, and FIPS 140 certifications
- Easy integration with Windows, Linux OS, and TCG TPM software stack
- Cryptographic services with improved performance
- Firmware upgradable to new standardized features and cryptography

ST33KTPM, NEW GENERATION OF TPM FOR CONSUMER AND INDUSTRIAL SYSTEMS

Future-proof Trusted Platform Module expanding trust from personal computing to connected devices

ST33KTPM, the latest addition to the STSAFE-TPM family, offers improved performance, enhanced security, and increased memory capacity to effectively address current and future security challenges. The ST33KTPM offer contains three products with different interfaces and lifetimes to support all ecosystem requirements.

Key applications

- PCs, workstations and
- Servers
- Network equipment
- Home and building automation
- Point of sales
- EV charging station

Key use cases

- Platform trusted identity
- Device health attestation
- Anti-couterfeiting
- Protection of keys and critical data
- Cryptographic toolbox
- Secure channel communication (TLS)

ECOSYSTEM

- Expansion board for Raspberry PI® and STM32MPx MPU for both SPI and I²C interfaces
- Software package with use cases and utilities (firmware upgrade)
- Windows HLK certification and major Linux distributions support

CERTIFICATIONS

ST33KTPM products received the following certifications:

- Common Criteria certificate EAL4+ conformant to TCG Protection Profile augmented with resistance to high-potential attacks (AVA_VAN.5)
- TCG certificate

ST33KTPM is compliant with

- FIPS 140-3 certificate with physical security level 3

To check the certification status, please refer to the list of certified products on the relevant websites.

SECURITY

ST33KTPM products benefit from advanced hardware and software security protections against state-of-the-art logical and physical attacks.

UPGRADABILITY

ST33KTPM products are designed to support the following evolutions through firmware upgrades

- Cryptographic services for EV charging standard ISO15118-20
- Future TCG standard
- Post-Quantum Cryptography (SP800-108, FIPS 203 and 204), and
- Security improvements to thwart new security attacks

Learn more at **www.st.com/stsafe-tpm**

KEY FEATURES

- Support of latest specifications of TCG TPM 2.0 standard (revision 1.59)
- Extended cryptography support (up to RSA 4096, ECC NIST P256 & P384, EC BN256, SHA1, SHA2-256 & 384, SHA3-256 & 384, AES 128-192-256)
- TCG compliant SPI or I^2C interface selectable dynamically
- Non-volatile memory (200kB)
- TPM firmware upgrade through fault tolerant loading process
- TPM firmware and critical data self-recovery (NIST SP800-193)
- Consumer & Industrial JESD-47 qualifications
- Available in thin UFQFPN32 standard package and small footprint package WLCSP24
- Extended operating temperature range (-40°c to 105°C)

Product summary

Product name	Application segment	TPM version	Interfaces	Packages	Certification	Temperature range [°C]	Lifetime
ST33KTPM2XSPI	Consumer	2.0 Rev 1.59	SPI	UFQFPN32	CC EAL4+ FIPS 140-3 (Physical Security Level 3)	-40 to +105	10 years
ST33KTPM2X	Consumer		SPI or I^2C				
ST33KTPM2I	Industrial (JESD-47 qualified)			UFQFPN32 WF WLCSP24			20 years

Order code: BR2401STSAFE

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

life.augmented