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

8+ 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 crypto services

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+ platform, 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
- CC EAL5+-certified

STSAFE-A, OPTIMIZED TO PROTECT YOUR BUSINESS

STSAFE-A110 ecosystem for seamless security

STSAFE-A110 is an STSAFE-A secure element with state-of-the-art security features that prevent the counterfeiting of genuine peripherals and IoT devices.

Key features

- Strong authentication (compliant with UBS-C and QI)
- Secure channel establishment (TLS)
- Signature verification
- Decrement counter
- Secure data storage
- LPWAN Lora & Sigfox compliant

Ecosystem

STSAFE-A110 ecosystem contains a complete set of tools for seamless integration:

- ODE STM32 Expansion board (X-NUCLEO-SAFEA1)
- STM32 Cube development ecosystem (X-CUBE-SAFEA1 software package)
- Pre-personalized STSAFE-A110 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**

Order your X-NUCLEO-SAFEA1 online at **www.st.com/stsafe-A110**

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 • LoRa & Sigfox compliant	I²C	CC EAL5+ HW	SO8N DFN 2x3	From -40 to +105 °C	6 Kbytes
STSAFE-A1SX	• Sigfox authentication • Sigfox frames • Encryption/decryption (optional)					

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
- 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	CC EAL5+	DFN8 VFQFPN32	-40 to + 105 °C	80 Kbytes

STSAFE-TPM standardized

STSAFE-TPM is a widely deployed, standardized solution acting as the corner stone of Personal Computers and Server security. It is a perfect fit for ecosystems built on Windows and Linux operating systems.

Certified by CC and FIPS 140-2, all STSAFE-TPM products meet security and regulatory requirements. The product portfolio is qualified for consumer, industrial and automotive applications.

KEY BENEFITS

- Integration with Linux and TCG TPM software stack
- FIPS and CC certified
- Long lifetime
- Delivered with keys and certificates loaded

STSAFE-TPM, STANDARDIZED FOR TRUSTED COMPUTING

Expanding trust from personal computing to connected devices

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 SPI or I²C interface
- Consumer / AEC-Q100 / Industrial qualification
- Available in standardized and small footprint packages like WLCSP

Ecosystem

A full development kit is available for offer easy integration.

- Expansion board (STPM4RasPI) for Raspberry PI® and STM32-MP1 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

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

Product portfolio

Product name	Application segment	OS support	Interface	Certification	Package options	Operating temperature range
ST33TPHF20/2E	TPM PC / server, network, printer, IoT	TPM 1.2 / TPM 2.0	TCG SPI (33 MHz) TCG I²C (400 KHz)	CC EAL4+, TCG, FIPS 140-2	TSSOP28, VQFN32	-40 to + 105 °C
ST33TPHF2X		TPM 2.0		CC EAL4+ (high attack potential), TCG, FIPS 140-2	VQFN32	
ST33GTPMA	Automotive		TCG SPI (18 MHz) TCG I²C (200 KHz)		TSSOP20	
ST33GTPMI	Industrial				WLCSP	

life.augmented

Order code: BRSTSAFE0820

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

life.augmented