life.augmented

Press release

P4036S

Next-Generation Security-on-a-Chip for Smart Things, from STMicroelectronics, Comes with Certified Protection Profiles for European Utilities

- *New STSAFE chip combines latest digital-security features to keep connected IoT objects safe*
- *Turnkey applets accelerate time to market for secure smart meters, data concentrators, and gateways*
- *Certified Common Criteria CC-EAL5+ and compliant with ENEDIS specification for French smart-metering market*
- *Certified by BSI for German smart-metering market: BSI-DSZ-CC-1037-2018*

Geneva, May 24, 2018 – STMicroelectronics (NYSE: STM), a global semiconductor leader serving customers across the spectrum of electronics applications, has brought together the latest digital security techniques in a single chip to protect Smart Things and Networks including those for utility infrastructure against cyber threats.

Focused on providing state-of-the-art security for connected objects, the STSAFE-J100 gives the object an unalterable identity that can be authenticated; it also handles encrypted communications and provides secure storage. It is easily integrated in IoT (Internet of Things) devices like smart meters, data concentrators, and utility gateways. Customizable with market-specific applets, the STSAFE-J100 secure element combines CC EAL5+[1] certified hardware and a CC EAL5+ certified secure operating system. Device designers can take advantage of the freedom to create their own security profiles, or get to market faster using ST's pre-certified profiles such as German BSI and French Enedis smart-utilities specifications.

[1] CC EAL: Common Criteria Evaluation Assurance Level: the internationally standardized (ISO/IEC 15408) framework for defining and evaluating security of IT equipment. Assurance levels range from 1 (functionally tested) to 7 (formally verified): EAL5+ is among the highest normally applicable for commercial/civil purposes.

The STSAFE-J100 extends ST's successful track record in robust, user-friendly, hardware-digital security for e-government, transportation, banking, and consumer projects, with over 1 billion embedded secure elements delivered yearly to protect devices and networks worldwide.

"Today's on-line services and connection to remote objects need a high level of protection against ever-evolving cyber threats. It is crucial to offer device makers state-of-the-art security for a minimum integration effort," said Laurent Degauque, Marketing Director, Secure Microcontroller Division, STMicroelectronics. *"The flexible STSAFE-J100 solution raises the bar with extra performance and support for the latest encryption algorithms and security standards, including security profiles for the important German and French smart-metering markets."*

To help customers take full advantage of the flexibility of the STSAFE-J100 and ensure uncompromising threat protection, ST provides secure device-personalization service. Personalizing each device with its unique identity and cryptographic keys is a fundamental part of the secure-element philosophy to create trusted hardware resistant to cloning or hacking. ST's service is safe and cost-effective, and relieves customers of responsibility for secure programming, preventing exposure of keys and secrets, and distributing programmed devices.

The STSAFE-J100 occupies minimal real-estate on the main system board, in either a 5mm x 5mm VFQFPN32, 6.0mm x 4.9mm SO8N, or 4.2mm x 4.0mm UDFN8 package. Please contact your local ST sales office for pricing options and sample requests.

Notes for Editors:

The STSAFE-J100 is backwards-compatible with its predecessor, ST's Kerkey embedded secure element, to preserve customers' existing investment in software and development expertise. The new chip adds extra memory, offering up to 66kB of user data storage; it executes cryptographic algorithms faster, leveraging its updated and higher-performing secure microcontroller embedding dedicated hardware accelerator.

Running on this improved hardware, the latest JavaCard secure OS, Version 3.0.4 Classic with GlobalPlatform provides advanced security features, including support for Password Authenticated Connection Establishment (PACE) protocol. Leveraging ST's crypto library including DES/3DES, RSA, ECC and AES, SHA-1, SHA-256, SHA-512, CRC32, and CRC16, the STSAFE-J100 is certified to Common Criteria (CC) EAL5+; the highest level for commercial electronic-security equipment. Middleware complying with the latest Public-Key Cryptography Standards (PKCS #11) further underlines the new chip's adherence to best-in-class security technologies.

Protection profiles, run as applets on the JavaCard OS, enable rapid customization to meet the needs of individual markets and use cases. The STSAFE-J100 can be supplied ready for customers to integrate their own applets, or with selected off-the-shelf applets from ST that dramatically reduce integration and certification overhead and allow faster time to market. ST has extended the selection of pre-certified applets available for the STSAFE-J100, which includes generic applets as well as the latest BSI-CC-PP-0077-V2 and Enedis protection profiles allowing users to quickly and cost-effectively configure solutions for the German and French smart-utility markets.

Also part of the STSAFE-J100 ecosystem, in addition to the turnkey applets and secure personalization service, the STS-J-PROGQ32ELx development board allows engineers to interact with the chip using general-purpose MCU development boards. The STSAFE-J100 is delivered with all documentation, software libraries, drivers, and test tool, and a code example to help personalize the device.

About STMicroelectronics

ST is a global semiconductor leader delivering intelligent and energy-efficient products and solutions that power the electronics at the heart of everyday life. ST's products are found everywhere today, and together with our customers, we are enabling smarter driving and smarter factories, cities and homes, along with the next generation of mobile and Internet of Things devices.

By getting more from technology to get more from life, ST stands for life.augmented.

In 2017, the Company's net revenues were $8.35 billion, serving more than 100,000 customers worldwide. Further information can be found at www.st.com.

PR Contact

STMicroelectronics
Michael Markowitz
Director Technical Media Relations
+1 781 591 0354
michael.markowitz@st.com