life.augmented

Press release

P3833S

STMicroelectronics Simplifies Design-In of State-of-the-Art Security for the IoT

- *New STSAFE-A100 optimized secure element provides built-in authentication, secure communication, key provisioning, and highest security standards for IoT devices (CC EAL5+)*
- *STSAFE-A100 secure element simplifies integration challenges for equipment designers, with full support ecosystem available*

Geneva, June 14, 2016 – STMicroelectronics (NYSE: STM), a global semiconductor leader serving customers across the spectrum of electronics applications, has announced a strong yet easy-to-use secure element to protect connected devices in the consumer and industrial Internet of Things (IoT) and to prevent cloning or copying of genuine products by ensuring authenticity.

Certified to the highest security industry standards, the new STSAFE-A100 can be designed-in by developers without specialist security expertise thanks to comprehensive support ecosystem.

Consumer devices, home appliances, industrial assets, and infrastructure controllers are already connected to the internet or will be soon. Many of them are designed to be autonomous and unattended. They now need state-of-the-art electronic security to prevent hackers from counterfeiting, cloning, stealing information, or misusing the equipment. ST's new STSAFE-A100 is a secure turnkey solution that brings the Company's proven expertise in electronic security for applications such as banking, e-commerce, and identity protection to the IoT. As a secure element that provides authentication services and can be used in conjunction with an ordinary microcontroller, it features an embedded secure operating system and is certified to Common Criteria EAL5+[1], banking-level security-industry standards.

"STSAFE-A100 delivers an economical and certified solution for state-of-the-art security in IoT and brand protection, presenting an alternative with clear advantages over existing approaches like software-based security running on a general-purpose

[1] CC EAL5+: Common Criteria Evaluation Assurance Level 5+

microcontroller or an uncertified crypto-companion IC," said Laurent Degauque, Marketing Director, Secure Microcontroller Division, MDG Group, STMicroelectronics. "Seamless integration puts security at the heart of the product and frees developers to focus on maximizing added value at the application level."

ST has made design-in of its new secure element easy for customers by providing a complete ecosystem that includes an expansion board with Arduino headers, a microcontroller library, and reference implementations. These simplify attaching the STSAFE-A100 to a microcontroller such as any from the STM32 family.

The STSAFE-A100 secure element is scheduled to enter volume production in July 2016, as a 4mm x 5mm SO8N or 2mm x 3mm UFDFPN8. Please contact your ST sales office for pricing options and sample requests.

Further Technical Information:

STSAFE-A100 provides strong authentication services that help make sure only authorized IoT devices can access online services and only authorized accessories or consumables are recognized and accepted by an application. It is compliant with the USB Type-C™ device-authentication scheme and secures communications with a remote host using Transport Layer Security (TLS) handshaking.

Additional functions that further minimize any potential for security breaches include signature verification to ease secure boot and firmware upgrade, secure counters that allow usage monitoring, secure pairing with the host application processor, wrapping and unwrapping of local or remote host envelopes, and on-chip key-pair generation.

The STSAFE-A100 supports asymmetric cryptography including Elliptic Curve Cryptography (ECC) with NIST[2] or Brainpool 256-bit and 384-bit curves, and symmetric cryptography using AES-128/AES-256. The STSAFE-A100 comes with a unique serial number on each die and its operating system comprises a kernel for authentication and data management and provides strong protection against logical, fault, side-channel and physical attacks.

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.

[2] NIST: US National Institute for Standards and Technology

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

In 2015, the Company's net revenues were $6.90 billion, serving more than 100,000 customers worldwide. Further information can be found at www.st.com

For Press Information Contact:

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