STMicroelectronics Boosts Consumer Data Security

Posted Janine E. Mooney, Editor October 20, 2011

The cost of protecting confidentiality and secret information stored on PCs and laptops - and the costs that a commercial enterprise or Government department may have to pay when a laptop containing sensitive information is lost or stolen - will be dramatically reduced by a unique new device announced by STMicroelectronics. Called HardCache-SL3/PC, the new device is a single-chip data encryption engine that is the first in the world to include a cryptographic module certified to the United States NIST[1] (National Institute of Standards and Technology) FIPS 140-2 Level 3 standard, the most rigorous security standard anywhere in the world for non-military applications.

FIPS (Federal Information Processing Standard) 140-2 is a U.S. Government standard that specifies requirements for cryptographic modules. Initially developed for use by US Government departments and agencies, FIPS 140-2 is fast becoming a de facto standard, both nationally and internationally, and is the model for the International Security Standard ISO 19790 currently being developed. The growing importance of these standards is due to the increasing damage individuals and businesses suffer as a result of the loss and disclosure of sensitive and confidential information. In addition, a proliferation of new laws around the world require enhanced security and privacy while raising the legal and financial stakes for enterprises that fail to meet the standards.

“HardCache-SL3/PC sets a new reference level for the industry by providing a solution certified by NIST for its highest non-military level of security, that is accessible to a broader audience, thanks to its affordable cost,” said Francesco Brianti,Vice President Open Market Business Unit. “ST has a long history of providing best-in-class security solutions to our customers, illustrated by our strong positions in the supply of Trusted Platform Modules, Smart Cards and secure features in Set-Top Box systems. We are now able to bring this depth of expertise to the secure computer market with the world’s first FIPS 140-2 Level 3 certified encryption chip.”

Until now, the cost of complying with Level 3 was so high that very few computer and data storage manufacturers could afford it. As a result, most “secure computers” employed software solutions that could not go beyond Level 2 but worse, also slowed the performance of the computer. The HardCache-SL3/PC eliminates these problems because the hard-wired encryption engine embedded within the chip performs all of the encryption and decryption algorithms that are needed each time the system retrieves data stored from the memory to the central processor with no impact to performance.

The HardCache-SL3/PC is fully supported by software drivers and a development kit to lower the cost of developing new secure applications.

Please contact your ST sales office for pricing options and sample requests, or visit the following URL to order from distributors:
http://www.st.com/internet/com/ordering/buy_from_distributors.jsp [1]

Source URL (retrieved on *07/29/2014 - 5:41am*):
http://www.wirelessdesignmag.com/product-releases/2011/10/stmicroelectronics-boosts-consumer-data-security

Links:
[1] http://www.st.com/internet/com/ordering/buy_from_distributors.jsp