11 July 2006

Keeping secrets safe in the future

EUREKA Strategic Initiative MEDEA+ A304CryptoSoC project has developed a data encryption system embedded on a microchip that is not only set to revolutionise the protection of information passed through the Internet, but will also give Europe back the control over its security systems. MEDEA + is EUREKA's largest industry-driven Cluster, a pan-European programme for advanced cooperative R&D in microelectronics, seeking to ensure global competitiveness.

The Internet has grown to be a universal medium for conducting business transactions. This phenomenon has also seen a parallel growth in the hi-jacking of information transferred over the web. The vulnerability of commercial software used to provide encryption and keep information confidential has given rise to a new generation of encryption and security systems embedded directly in the hardware components – the microchips. However, a serious limitation of such systems has been the need to define specific uses or applications, with very specific operating systems. This makes them costly and uncompetitive in comparison to software protection systems. That is, until the MEDEA+ cryptographic system on a chip (CryptoSoC) project created a system-on-chip (SOC) device architecture entirely under the control of European companies.

MEDEA+ focuses on enabling technologies, aiming to make Europe a leader in system innovation on silicon, turning its microelectronics sector into a world-class industry. The eight partners belonging to the MEDEA+ CryptoSoC project have broken ground in defining a new way of designing chips. Patrick Le Quéré, the project leader at Bull, a leader in the field of Internet security, explains; "We have defined a new single architecture rather than dedicated security chip, to fit all applications, as all applications have different types of chips. New chips can now be designed for a type of application quickly and easily".

Applications include electronic servers on the web, high-speed data networks, and USB data protection keys for personal computers. These encrypt all the information stored on a personal computer. It can then only be read when the personal security key is plugged in.

Bull has been successful in using the project results. "Thanks to EUREKA and the MEDEA+ project, we have been able to put a new generation of data security products on the market very quickly", says Le Quéré. The partners, including STMicroelectronics, Sagem, CEA-LIST, two small and medium enterprises and two Italian universities, are hoping to launch a new project that will lead towards the standardisation of their architecture.

Currently, European companies are reliant on using predominantly American information security technologies that lead the global market. The standardisation and hence availability of a flexible structure that could be used to design any sort of high security chip, card or application quickly and easily, would give Europe its independence and position it as the market leader.

For further information about EUREKA Clusters visit:
http://www.eureka.be/inaction/strategicInitiatives.do