Encryption and Smart Card Technology Leaders Develop Identifier-Based Encryption for Portable Formats

April 26 2005

Researchers from HP Laboratories and STMicroelectronics have collaborated with card manufacturer Incard to develop technology for the implementation of Identifier-Based Encryption (IBE) on smart cards. A demonstration of this technology will be presented on the Hewlett-Packard booth at 'Infosecurity 2005' from April 26-28, 2005, in London.

Smart cards are not only powerful and convenient; they are proven as outstanding carriers for confidential information such as private keys. By implementing IBE on a smart card, developers can create more practical and cost-effective online and offline secure business communication applications. Applications for the technology are in the areas of e-government, e- and m-commerce, wireless management of secure documents, access control, and personal-authorization tokens.

IBE has certain advantages over public-key infrastructure (PKI) security schemes. In classical PKI schemes, the public key is a randomly calculated number that has to be linked to the identity of the user by a certificate. With IBE the public key can be chosen freely and can be linked directly to the user's identity or role without the need to exchange certificates and the costly infrastructure that comes with it.

The three partners have implemented IBE on a smart card by using elliptic-curve pairing functions, which are important cryptographic primitives. IBE uses bilinear mapping on elliptic curves to obtain an

algorithm that can be used to turn a simple, well recognized identity or role into a public/private key pair. This role-based encryption allows for one party in the communication (e.g. the receiver) to dynamically change the link between the identity and the role of the user without impacting the other party (e.g. the sender).

HP Labs Bristol has one of the world's leading research groups in IBE, which has the advantage of being more easily scalable than other PKI technologies. As a result it has numerous possible applications, including smart card security.

The algorithmic calculations were developed by HP Labs and ST and implemented by Incard R&D on JsEC, an Incard smart card JavaCard 2.2.1 platform, based on ST's ST22L128 chip. JsEC decrypts an IBE message in a few seconds. Incard has already integrated a JsEC smart card into a software application to show how IBE can complement the security offering of PKI schemes in business applications and environments.

"HP Labs has been investigating IBE cryptography for some years and are impressed with its potential," said Keith Harrison, senior cryptographic researcher at HP Labs Bristol. "We are developing a number of applications, including a new HP ProtectTools security product, which would be difficult to implement with alternate forms of public-key cryptography. Working with our colleagues at STMicroelectronics on this prototype smart card solution has emphasized the complementary strengths of both research groups."

"Incard's eSecurity product 'JsEC' aims to conquer a highly specialized market that is expected to expand quickly," said Alessandro Scognamiglio, Incard's Strategic Marketing Manager. "JsEC is the right solution to guarantee secure Internet transactions and communications. It clearly and easily manages different operations such as authentications,

certifications, e-signatures, and other functions able to guarantee net and local security. Through a dynamic integration with the Windows operating system, JsEC enables the user to provide their signature and authenticate themselves simply by clicking the mouse."

"STMicroelectronics has a long history of devoting enormous efforts to its R&D to ensure that new technologies can be exploited in commercial products as quickly as possible; this cooperation between HPLabs and ST researchers is an excellent example of that tradition," said Alessandro Cremonesi, Vice President, Advanced System Technology, STMicroelectronics. "ST believes that making security implementations that are significantly cheaper, faster, more convenient, and more reliable is absolutely vital to meet the needs of the market. Additionally, this implementation by Incard, based on ST's advanced and innovative ST22 SmartJTM silicon platform, demonstrates that the 32-bit ST22 range of smart card ICs provides a perfect medium to carry any encryption algorithms."