Title: ECQV Implicit Certificates and the Cryptographic Suite for Embedded Systems (Suite E)

Presenter: Greg Zaverucha, Certicom Research, Research In Motion

Emerging technology space: Embedded systems, constrained devices

Class of cryptographic requirements: Lightweight PKI and efficient public key algorithms

Embedded systems on constrained wireless devices have strict computation, power and bandwidth constraints. As these systems become more prevalent they are likely to interface with other networked devices like smartphones, tablets, personal computers and be incorporated in larger home, industrial, and vehicular automation systems.

The central component in a public-key infrastructure (PKI) is a certificate scheme. An increasingly popular choice for constrained environments is the ECQV implicit certificate scheme. In the smart energy sector, ECQV has been deployed in over 20 million certified devices today, and is expected to reach 100 million over the next three years. Standardization activities involving ECQV have also increased, and now include: ZigBee Smart Energy 1.0 (smart grid), ISA SP100.11a (industrial automation), IEEE 1609.2 (vehicular networking), ANSI X9.123 (financial industry), SECG SEC 4 (general purpose), and NFC Forum (near field communication, where ECQV has been proposed for inclusion).

The Cryptographic Suite for Embedded Systems (Suite E) combines ECQV with a set of standard symmetric key and elliptic curve public-key primitives to form a complete cryptographic suite providing 128-bit security. Suite E requires only modest resources, having small code space, as well as low computational and low bandwidth costs, making Suite E both lightweight and energy efficient. Additionally, Suite E algorithms were chosen as a group to minimize overall system costs in mass production by selecting easily embeddable algorithms. In addition to ECQV, Suite E includes the ECMQV key agreement protocol, and profiles the ECPV signature scheme, a scheme with message recovery producing compact signed messages. An IETF Internet Draft document specifying Suite E is available online at http://tools.ietf.org/html/draft-campagna-suitee-01.