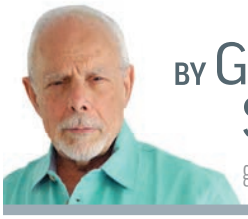
EMV GOES ECC



BY GIDEON SAMID
gideon@bitmint.com

THIS CRYPTIC HEADLINE is quite telling, and it deserves proper attention from the payment community. Payment people know that EMV replaced magnetic-stripe technology, and that it sometimes takes uncomfortably long seconds to get the transaction approved. But few appreciate its big, innovative step in e-commerce.

Instead of repeated exposure of payment card content, the EMV card engages its authenticator in a dialogue, a conversation that leads to the authentication. This dialogue is based on dramatic cryptographic advances introduced almost 50 years ago. Shows you how long it takes to get science to the storefront.

For thousands of years, cryptography worked as follows: Transmitter and recipient shared a secret key used to encrypt the communicated secret and to decrypt it. It was applied in war and espionage, won battles, and shaped history. Alas, when payment went digital late in the last century, this mode became impractical. A customer spotting a new store on the Web has no shared key with this merchant. No shared key, no secure payment.

Fortunately, in the 1970s, three innovators at the Massachusetts Institute of Technology (Rivest, Shamir, Adleman) made a radical proposal: Use one key to encrypt a message and a different key to decrypt it. Why is this so revolutionary? It allows the merchant to send the customer its encryption key so the customer can use it to encrypt his payment information and send it over. The merchant will then decrypt it with its decryption key.

Without possession of the decryption key, eavesdroppers can't compromise the payment information. This simple two-keys approach opened the door to e-commerce as we know it today.

For this idea to work, two conditions must be met. First, it should be impossible to decrypt the message with the encryption key, which is in the public domain. Second, it should be impossible to deduce the secret decryption key from the public encryption key in time to harm the parties.

The first condition is mathematically secured. The second condition is mathematically suggested—but not guaranteed. A faster-than-expected computer and/or a smarter-than-expected mathematician could compromise all e-commerce transactions and jeopardize online trade.

For decades, that MIT method, known as RSA, has been used to generate pairs of public and private keys such that the latter can't be extractable from the former. It has apparently held up so far. The method is harder to compromise when larger keys are used, so we keep the keys growing, and plan to keep doing so. This requires changes to the standard, but we have no choice.

Technology, though, keeps moving. Some dark clouds are gathering from the corners of technology where quantum computers are being built. It has been shown that these new computers will crack RSA, rendering it useless. The proposed solution is called Elliptic Curve Cryptography (ECC), a different mathematical construct in which the private key, we hope, cannot be easily deduced from the public key.

The math behind ECC is more complicated and has a better chance to withstand a quantum-computing attack, while using smaller, more convenient keys. But the change from RSA to ECC is quite involved and will require a great deal of planning and design.

Society is maintained through payments, so a collapse of the underlying cryptography would be a social disaster. How long will RSA stand up? Would ECC hold up for long?

Trying to outrun the quantum predator is not sustainable. Payment requires a new vision. We at BitMint are proud to take part in the search for a more secure, sustainable payment climate. As EMV goes ECC, we go DCC: Durability – Consensus – Courage. DT