PrehKeyTec

# Talking points on PrehKeyTec's Encryption Technology

- PrehKeyTec offers encryption of Cardholder Data as required by PCI DSS and recommended by Visa's PABP. Additional to being able to encrypt Cardholder Data when read by the integrated MSR on their keyboards, PrehKeyTec keyboards also do encrypt numeric entries done on the keyboards for the so called "card not present transactions". This solution uniquely secures and encrypts all financial transactions at the point of capture. The transmission of this data is as such encrypted from the point it leaves the PrehKeyTec keyboard and travels down the cable to the Host PC and beyond as required by PCI DSS req. 3.4.

- Building on the advanced technology and intelligence of our MCI keyboard series, PrehKeyTec was able to offer two different sets of security solutions based on AES and ARCFOUR encryption algorithms. Both technologies do use an above a more than required encrypted key length for advanced security.

- The AES encryption technology is built on a 256 bit key combined with an optional encrypted transaction ID to guard against the so called "man-in-the-middle" attack. It encrypts and transmits all of the data on Track 2 of financial cards which is required at the processing gateway for credit card processing. The encryption is optionally designed to transmit the first 6 digits (BIN) and last 4 Digits on Track 1 in the clear for receipt printing and routing purposes. Transmission of Cardholder Name is optional and can be adjusted as required.

- The ARCFOUR Solution is built on 2 sets of 256 bit keys per transaction. There is a set of 16000 keys, each with a length of 256 bit randomly scattered within the Firmware in the keyboards. For each transaction, a 256 bit key is randomly taken out of the Firmware, and then combined with a customer specific 256 Bit key within the keyboard to realize a double encryption per transaction. The sophisticated built of the keyboard electronic combined with the speed and simplicity of ARCFOUR allows for such complex manipulation of Financial Card Data to provide a highly secure solution. PrehKeyTec's ARCFOUR solution encrypts all Cardholder Data on financial cards (Tracks 1, 2 and 3). It can additionally be configured to encrypt other sensitive data which a customer might want to securely transmit such as passwords and Social Security Numbers.

- Using PrehKeyTec's WinProgrammer Software, a freeware written by PrehKeyTec and available on our Website for download, systems integrator and administrators can easily inject their customer unique 256 Bit keys into the keyboards. Besides letting the Integrator and Administrator inject keys for encryption into the keyboards, this software also offers the possibility to design and program the keys on the keyboards for customer specific

functionalities. It is also possible to configure Headers and Terminators for MSR transactions and keyboard credit card transactions for Card not present scenarios.

- There is basically no limit to the amount of key sequences that can be used for encryption and PrehKeyTec recommends a regular update of the customer specific key so as to keep the security of their products always at the highest level.

- Furthermore, the WinProgrammer also offers the Integrator the possibility to set LED statues for varying situations like confirming the statues of a card swipe e.g, a successful read with a GREEN Led flashed and a Bad Read with a RED LED statue. An additional buzzer within the keyboard can produce a tone effect for swipes or key pressed giving the encrypted solutions the possibility of offering audible and visual feedbacks.

- The file created by the Systems Integrator can then be logically secured against compromise and compiled into a binary file, which could be manually or remotely loaded into the keyboards. Once the created file is logically secured, only a User with knowledge of the loaded key can make changes to the file or change the security key in the keyboard.

- PrehKeyTec offers an API for easy decryption of the encryption for processing. Use of this API is highly recommended because besides reducing the Integrator's or Administrator's workload, it also uniquely minimizes code errors which might occur should the customer decide to do the decryption on their own. However, PrehKeyTec is also ready to offer the Source Code with examples for the customer to do the decryption. The customer needs to specify what programming language they will want to use for the Source Code.

- PrehKeyTec also provides an additional API which any systems Integrator can use in their software to directly communicate with the keyboards. This API can be very handy in cases where the Customer wants to be able to turn on the keyboard encryption directly from his software rather than relying on the clerk to hit a key on the keyboard to turn on encryption in order to do a "card not present transaction". The flexibility of the keyboard allows for dual purpose usage, keying of encrypted information for sensitive transactions and for standard typing when the numbers keyed do not need to be encrypted. Should a customer prefer to use the keypad only for encrypted transactions and nothing else, it is possible to program the keyboards for just that purpose.

- Because the encrypted information coming out of the keyboard can be transferred over the network to a data hosting center for decryption, the products are in a position to uniquely take the Merchant's POS Terminal out of Scope of PCI DSS and as such reduce the enormous risks and cost involved in payment processing and general handling of Cardholder Data.