SREDKey: Bringing Security to Card Not Present Transactions

80137507-001

Rev. B

3/2/2018

http://www.idtechproducts.com

10721 Walker Street, Cypress, CA 90630, USA Voice: (714) 761-6368 Fax: (714) 761-8880

Executive Summary

Card Not Present transactions pose special challenges that are not easily met by traditional credit card readers and PIN pads. PCI-compliant handling of these transactions essentially requires the use of a dedicated device that can encrypt keyed-in data in real time. But most credit card readers (even those that have a keypad) are not capable of complying with Card Not Present requirements. The SREDKey™ keypad by ID TECH is a PCI-PTS certified Secure Reading and Exchange of Data (SRED) device that allows businesses to participate in phone and mail order transactions, and other Card Not Present situations; yet the device also has a physical magstripe slot, which can optionally be used for pickup-in-store, hotel check-in, and other scenarios in which the original order needs to be phoned in (for pre-authorization) but final settlement involves a physical card.

Card Not Present: A Special Challenge

In the majority of retail businesses, credit card transactions involve a customer presenting a physical card, in person. But this is not the norm for all business types. In Mail-Order/Telephone-Order (MOTO) businesses, and call-ahead businesses (where services or merchandise must be reserved in advance with a credit card number) – including car rental, hotel reservations, airline ticketing, mail-in bill payment, and other common scenarios – a physical credit card might never be presented, in person, by the customer.

Card Not Present scenarios present a special challenge, in that Payment Card Industry (PCI) rules forbid businesses from storing or transmitting credit card data. Under PCI rules, neither the Primary Account Number (PAN) nor any accompanying sensitive data (such as the three-digit CVV code on the back of the card) can be stored or transmitted in the clear. PCI rules, in fact, require that merchants render PANs and other sensitive data *unreadable* and *unrecoverable* through one of the following methods:

- One-way hashes based on strong cryptography (hash must be of the entire PAN)
- Truncation (hashing cannot be used to replace the truncated segment of PAN)
- Index tokens and pads (pads must be securely stored)
- Strong cryptography with associated key-management processes and procedures

Even the mere act of manually typing a card number into an onscreen form (using an ordinary PC and keyboard, or a purpose-built POS system running on Android or Windows) places the merchant in "PCI scope," because manual key entry using a conventional keyboard can expose cardholder data to surreptitious logging or monitoring by malware. (For PCI purposes, a regular PC constitutes an untrusted execution environment.) Even if data entered into a computer is not saved to disk, it may be cached in data buffers and/or logs (creating a vulnerability).

To reduce security vulnerabilities (and stay within PCI rules regarding the handling of sensitive cardholder data), card data needs to be encrypted at the point of entry—and remain encrypted throughout the transaction process, until it reaches an appropriate party (such as a remote gateway, or online payment processor that normally processes the merchant's transactions) who can decrypt the data in a properly controlled setting, at the time of need. In this type of setup, the merchant is part of an "end-to-end encryption" scenario, where the data never exists in clear text form (except upon reaching a trusted recipient).

To achieve end-to-end encryption with a keypad-based manual entry device, the data must be encrypted as it is entered, at a hardware level. Since ordinary PCs and tablets aren't set up to do this, it essentially means a purpose-built device is required. The SREDKey™ keypad by ID TECH is such a device.

Secure Reading and Exchange of Data

ID TECH's SREDKey™ is unique among handheld key-entry payment devices in that it meets PCI's exacting standards for SRED (Secure Reading and Exchange of Data) products. No other device in this class meets these standards.

PCI's requirements around SRED go well beyond mere encryption of data at the time of entry. The requirements govern secure manufacture (including the provisioning of data encryption keys, by a certified Key Injection Facility, before the device enters service), self-check logic that must execute periodically (i.e., daily) when the device is in service, authentication-based upgrading of firmware, and documented procedures for secure decommissioning of devices when they've reached end-of-life. In addition, SRED devices include anti-tamper features, so that if, for example, a stolen device is ever disassembled (in an attempt to gain access to electronic components), the device will automatically "zero out" its encryption keys and enter a state in which it is permanently disabled.

All of this is in addition to normal DUKPT (derived unique key per transaction) security measures, whereby transaction data is never encrypted with the same key more than once. (A new key is derived, and used once, for each transaction; then the key is discarded.) Moreover, although

SREDKey™ supports industry-standard Triple DES encryption and also AES encryption, it contains no decryption logic whatsoever. Thus, it is impossible to make the device decrypt sensitive cardholder data once it has been encrypted.

P2PE

Companies that require the ultimate protection against data breaches inevitably end up looking at a full PCI-validated P2PE (Point-to-Point Encryption) solution. But the cost of independently certifying such a solution is prohibitive for many (indeed, most) businesses. That's where Philadelphia-based FreedomPay comes into play. As a provider of PCI-validated P2PE payment solutions, FreedomPay provides a best-in-class P2PE solution for companies that might not otherwise be able to justify the expense of a one-off PCI Validated system. Merchants who utilize the FreedomPay Commerce Platform can choose from a variety of pre-approved card readers, then leverage FreedomPay's PaaS (Platform as a Service), FreeWay, to route payments electronically to their back end of choice, without worrying about "on premise" storage of cardholder data, or interception of cardholder data "in flight" (since all data is encrypted).

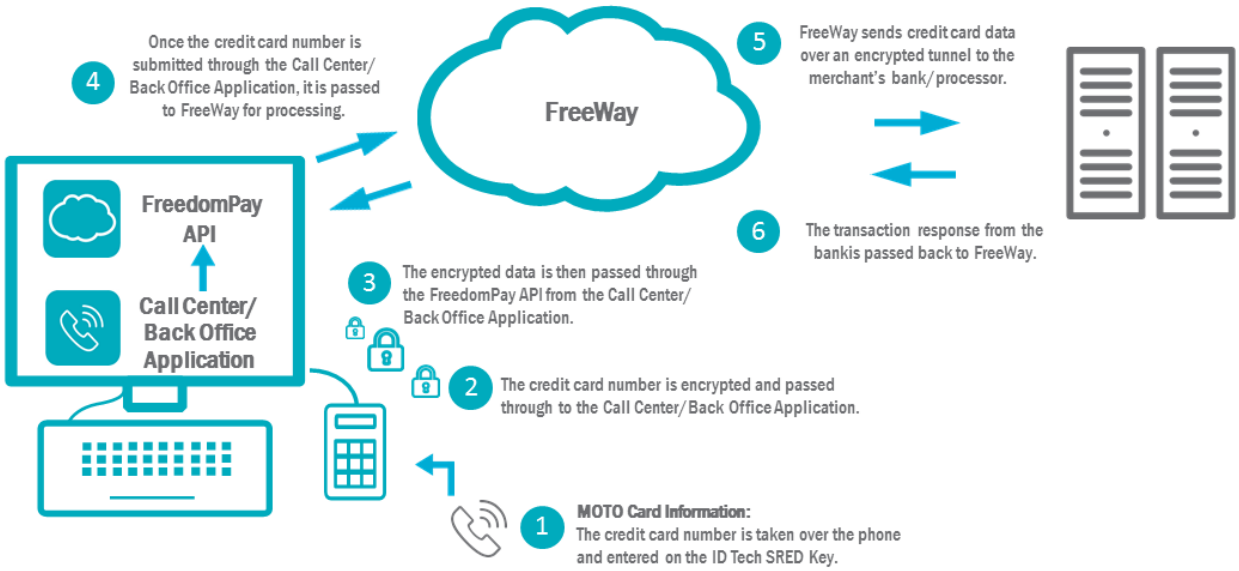
"All of FreedomPay's solutions are PCI-validated P2PE," explains company president Chris Kronenthal, "and ID TECH's SREDKey™ is our go-to device when it comes to any scenario involving back-office order-intake or Card Not Present transactions, which are still quite common in ticket sales, college admissions, health care, lodging, rentals, and storage—not to mention businesses that might have a limited retail presence backed by a much larger online experience." In many of these sorts of enterprises, customers might call ahead to reserve an item, then pay in person with a credit card, "which is where SREDKey™ really shines," says Kronenthal, "because you can use the device's manual key-entry mode to get pre-authorization, then run a card physically, using SREDKey's MSR slot, when the customer arrives in person to pay."

SREDKey™ Data Entry Modes

ID TECH's SREDKey™ supports six standard data-entry modes, including:

- Card Number, plus Expiration Date
- Card Number, Expiration Date, and ZIP Code
- Card Number, Expiration Date, and Security Code (CVV)
- Card Number, Expiration Date, Street Number of Address, ZIP Code
- Card Number, Expiration Date, Security Code, ZIP Code
- Card Number, Expiration Date, Security Code, Street Number, ZIP Code

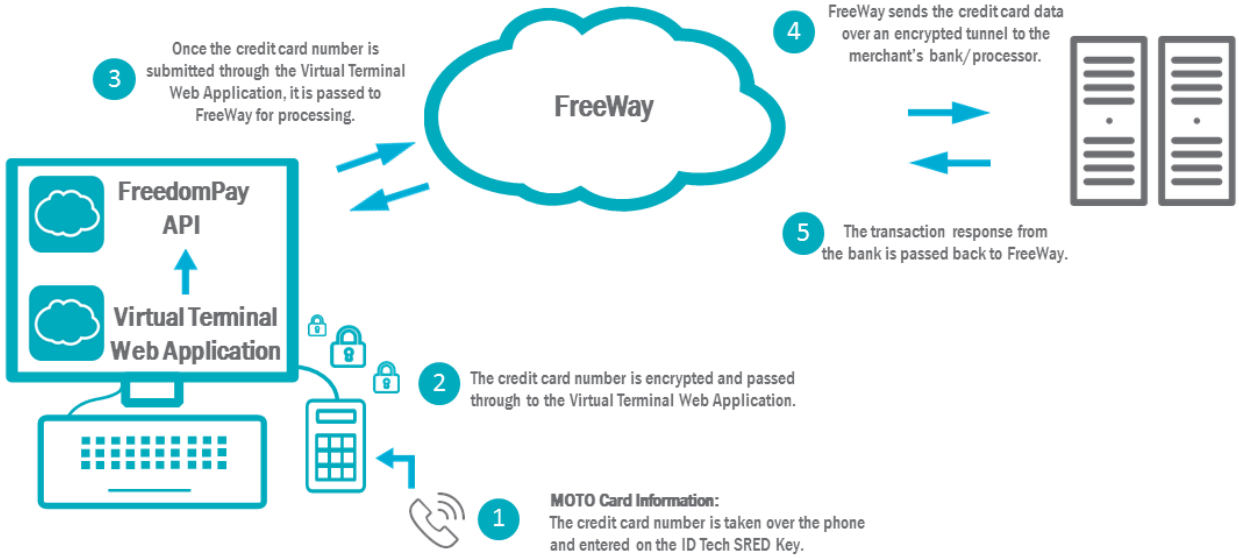
Call Center Application Data Flow



Key Points:

- PCI Validated Point-to-Point Encryption (P2PE) removes workstations, application and supporting network from PCI DSS scope.
- All payment data is entered using the IDTech SREDKey and encrypted within the SRED module. Standard keyboard input is disabled.

Virtual Terminal Data Flow



SREDKey data captured by a call center (top diagram) can be sent to FreedomPay's cloud-based processing platform, then forwarded to the merchant's bank for clearing. From the moment of capture, sensitive cardholder data is encrypted. When used in a Virtual Terminal environment (lower diagram), SREDKey can keep the merchant out of PCI scope, since keystrokes are not captured in the clear but are encrypted at the moment of key entry, before reaching the merchant's computer. (Source: FreedomPay)

The most common use case for merchants who process on FreedomPay's Commerce Platform is within the lodging industry. Since FreedomPay can offer P2PE with over 200 POS/PMS integrations, solving for the entire payments ecosystem of a hotel/resort, there are thousands of SREDKey devices deployed in Las Vegas and across the US to solve for over-the-phone credit card payments. Hotels and casinos utilize PMS (property management systems) that record and manage both Card Present and Card Not Present transactions; by utilizing the P2PE FreedomPay/SREDKey integration, merchants can securely book reservations over the phone to be settled at the front desk upon checkout.

Higher education is another Card Not Present "industry" served by FreedomPay in which SREDKey plays a critical role. "At this point, we serve over fifty percent of the Division One schools," FreedomPay's Chris Kronenthal notes. "It's incredible how many Ivy League tuition offices we're in, not to mention alumni offices that rely on being able to capture orders over the phone as well as in person."

Some retail businesses want to add phone-in/in-store-pickup capability, but quickly learn that MOTO (mail-order/telephone-order) is not as easy as simply hooking a PIN-pad up to a PC. "If you try to bring a non-validated device into your system," FreedomPay's Chris Kronenthal points out, "you can find yourself facing a full PCI-DSS 3.2 Level 1 security audit, if the device you're adding isn't [PCI] Validated. Whereas if you're bringing in SREDKey, you can remain out of scope for PCI, which will greatly simplify any audit." (Note: Regular yearly on-site security audits are required by PCI and card brands, for Level 1 businesses; and fresh audits must be conducted whenever the system changes.)

The Ultimate High-Security Industry: Health Care

Few industries are subject to as many security restrictions and statutory requirements as Health Care. In the U.S., HIPAA laws specify stringent requirements for the protection of patient data (in storage, as well as in transit), and most health care enterprises qualify as Level 1 businesses for PCI security, which means yearly on-site audits as well as quarterly audits of computer networks and data transmission systems.

Southern California based TrustCommerce—a payment solutions provider well known for its emphasis on security—serves customers in diverse industries, including non-profit, municipality, insurance, transportation, education, and retail. It's also among the most experienced of all gateways when it comes to the health care industry. In health care, TrustCommerce solutions integrate with Interactive Voice Response (IVR) systems, online payments, front and back office, mobile payments, kiosks, e-statements/billing services, and patient portals.

For Card Not Present scenarios, TrustCommerce offers ID TECH's SREDKey™, because, according to Preisdent of Technical Operations Chris Gowins: "It's durable, it's easy to use, it's secure—it's the best device of its kind out there."

For large call centers like mail service pharmacies or customers adding MOTO (Mail Order/Telephone Order) to an existing, conventional "Card Present" solution, SREDKey™ is relatively easy to integrate—not just at system design time, but at audit time. According to Gowins, Qualified Security Assessors "are definitely more comfortable when they see, during an audit, that a new addition to the system is a PCI-validated SRED device." Devices that are *not* PCI-listed as SRED-qualified are potentially subject to detailed physical examination to determine intrusion resistance and security characteristics. "With SREDKey, there's no question as to its security," Gowins points out. "It's already validated. It's PCI-listed."

But What About EMV?

Most card readers (including most of those manufactured by ID TECH) incorporate a chip-card bezel, for EMV transactions. ID TECH's SREDKey™, on the other hand, has a magstripe slot—but no EMV slot. "The point of the chip on a chip card is to prove that the card was physically present," explains ID TECH Product Manager Vince Steffano. "With Card Not Present transactions, it's a given that no card is present, hence the EMV slot is superfluous. To keep costs down, we eliminate it. But there are still situations where a transaction that was pre-authorized as Card Not Present goes to settlement with a card present, and for that we offer the MSR capability."

Lack of EMV capability normally means the merchant is liable for chargebacks in the event of fraud. But as TrustCommerce's Chris Gowins points out: "That turns out to be a non-issue for many of our healthcare customers. I mean, if someone has a surgical procedure at a hospital and they want to put the co-pay on their credit card, it's not likely they're using a stolen card."

FreedomPay's Chris Kronenthal echoes that sentiment. "In higher education, and many other places where we see SREDKey™ used, there's just not a fraud problem, because cardholders tend to provide lots of identifying information up front."

"EMV is about validating the card," says TrustCommerce's Chris Gowins, "whereas encryption protects cardholder information so that it is not sent in the clear exposing the cardholder to identity theft and fraudulent transactions. SREDKey™ encrypts transaction data from the point of entry, securing and safeguarding customer data—for both cardholders and merchants."

Ergonomic Design

Ergonomic design is an important factor in SREDKey's success, especially in high-volume call centers. To ensure that users are able to enter keystroke data quickly yet positively, SREDKey™ is precisely weighted and sits on non-skid rubber feet to maximize stability and eliminate slippage. Also, unlike conventional credit-card PIN pads (which are telephone-like in key layout), the numeric keys on SREDKey™ are arranged "calculator style," with 7, 8, and 9 on the top row of keys—a layout that's familiar to bookkeepers, spreadsheet users, and data-entry professionals. As a safeguard against accidental mis-entry of credit card data, the device automatically runs a Luhn checksum on PAN (primary account number) data and will flag as incorrect any credit card number that has been entered with (for example) two digits flipped, or a digit missing.

Conclusion

ID TECH's SREDKey™ allows merchants to conduct Card Not Present transactions with total security, in compliance with all applicable PCI requirements. As a PCI-validated SRED (Secure Reading and Exchange of Data) device, SREDKey™ meets the industry's highest standards for encryption-enabled payment devices, and incorporates anti-tamper features not found in lesser devices. SREDKey's ergonomic design, ruggedness, compact form factor, and driverless USB compatibility (with power supplied solely by the USB connection), combined with the unit's low Total Cost of Ownership and ease of use, make SREDKey™ a unique solution for merchants in telemarketing, health care, higher education, hospitality, and other industries where Card Not Present transactions are often the norm rather than the exception.

For More Information

For more information on SREDKey™, be sure to visit http://idtechproducts.com.

For a full list of P2PE validated solution providers certified with ID TECH's SREDKey™, see the PCI's listing of Validated P2PE solutions at: https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions.