Simplify

Nothing to Find, Nothing to Steal.

The recent spate of high-profile data breaches has businesses across the country reviewing their payments security infrastructure, and with good reason. Growing your business while protecting sensitive cardholder data is within reach, using flexible and scalable solutions designed to support mid- to large-scale businesses.

Simplify is a secure software application that resides within a Simplify payment terminal. It isolates sensitive cardholder data from your payment system by securely encrypting it at the start and during the payment authorization process. Simplify interfaces with your POS/ PMS System and our gateway, triggering the creation of a token in place of the payment card number to create more secure payment processing.

During the course of a transaction, card data is vulnerable in three scenarios – when it's "in transit", "in use", and when it's "at rest". Implementing an encryption process embedded in a Simplify payment terminal reduces risk throughout the entire payment cycle, from the moment a payment card is accepted. Encrypted data is decrypted at Elavon's secure data center. Sensitive cardholder data is removed from your system, allowing you to utilize a unique token rather than your customers' account data. Tokens have no value to hackers, thereby reducing the risks inherent with holding customer's card data for subsequent charges.

Encryption & Tokenization protect your payment data and your brand

Simplify is a key component of safe-t, our integrated, layered approach to security. Along with EMV, Encryption, and Tokenization, our powerful security solutions help you reach your growth goals while keeping your payment data safe.

safe-t
SECURITY SOLUTIONS

Elavon

Scalable Solutions Let You Focus on Service

TAKING A BITE OUT OF PCI

Simplify insulates the payment eco-system from any PCI sensitive data. Encryption occurs at card entry; and can only be decrypted at our secure site. Simplify follows PCI DSS guidelines concerning non-retention of prohibited card data.

READY FOR EMV?

EMV cards are already displacing traditional magnetic stripe cards in the United States as the region catches up with other parts of the world. This is driving an imperative for businesses – especially those servicing international customers - to utilize flexible payment acceptance models that accommodate chip and magnetic stripe cards as well as NFC/contactless payment methods. The addition of EMV-enabled equipment allows your staff to securely process chip cards and innovative payment solutions of tomorrow, such as mobile wallets, while continuing to support legacy magnetic stripe cards during the EMV migration.

BENEFIT FROM AN INTEGRATED APPROACH TO SECURITY

Your business can take immediate advantage of a seamless, secured end-to-end process that leverages Elavon's security features:

- Our terminals drive the authorization process, facilitating the transmission of encrypted sensitive data to reduce risk exposure the moment a customer's card is swiped or inserted.
- Our gateway deploys tokenization for immediate and subsequent payment transactions. Sensitive card data is not resident on the POS or PMS workstation, greatly reducing the impact of a security breach and lessening your PCI compliance burden.

WHY ELAVON?

When it comes to your customers' security, rely on an expert. Backed by U.S. Bank, Elavon offers 20 years of global payment processing and gateway experience. Our knowledgeable team of security professionals can guide you in making wise investments in data protection.

WHY SIMPLIFY?

Security – Remove card holder account numbers from your processing environment

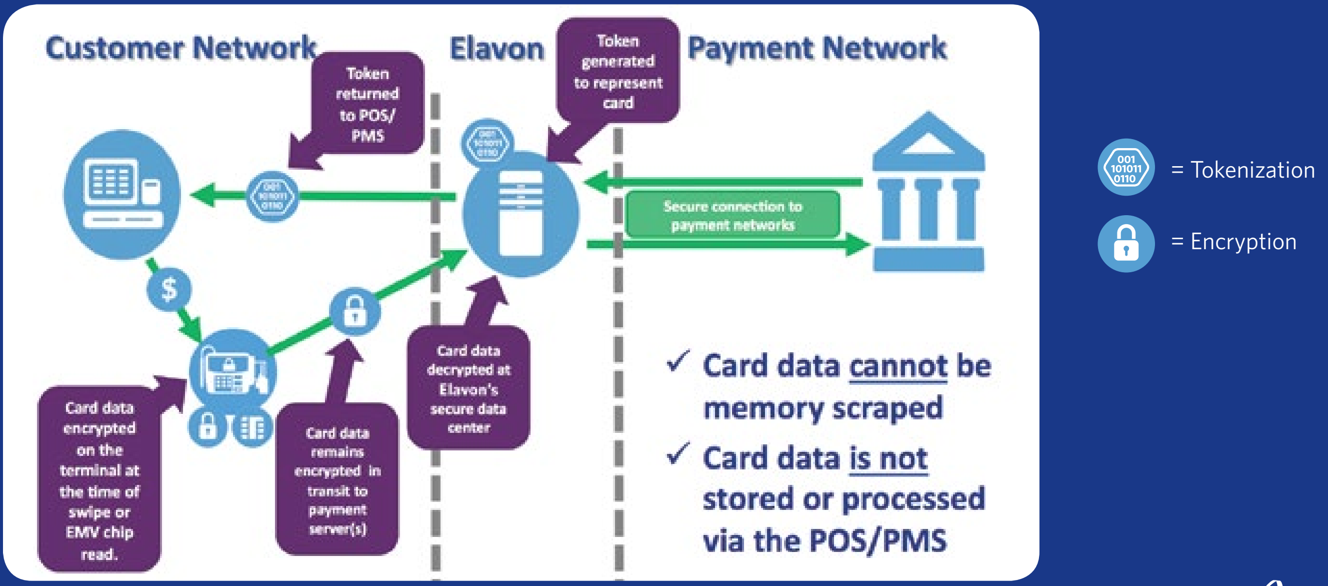
Future Proof – Add EMV to your processing environment in less time and with less expense than creating/certifying your own code

Flexibility –

- Remains compatible with existing solutions
- Use a variety of terminals without coding to a terminal directly
- Support for all payment types (Magnetic Stripe cards, EMV cards, Contactless)

Reduce Complexity –

- Eliminates EMV certification between customer and card brands
- Reduce time and effort of PCI compliance
- Eases the integration involved with adding encryption and tokenization



Customer Network
Elavon
Payment Network
Token returned to POS/ PMS
Token generated to represent card
001 101011 0110
Secure connection to payment networks
$
Card data encrypted on the terminal at the time of swipe or EMV chip read.
Card data remains encrypted in transit to payment server(s)
Card data decrypted at Elavon's secure data center
✓ Card data cannot be memory scraped
✓ Card data is not stored or processed via the POS/PMS
= Tokenization
= Encryption