

Simplify PCI Compliance with PANPADs

PPS

ERP PROVIDERS SINCE 2003

Confidence where you need it



Your Challenge the business need

You have a business to run, but the demands of today's security-conscious community seem endless. Your payment card interface is secure. You use tokenization to protect your IT infrastructure. But there is still card data on your network. Even after all your efforts you are worried that your company will be the target of the next major breach. One employee slipup and your data records could be vulnerable. You need to complete your solution to give you peace of mind. A successful business like yours needs a successful solution: smart, secure, flexible.

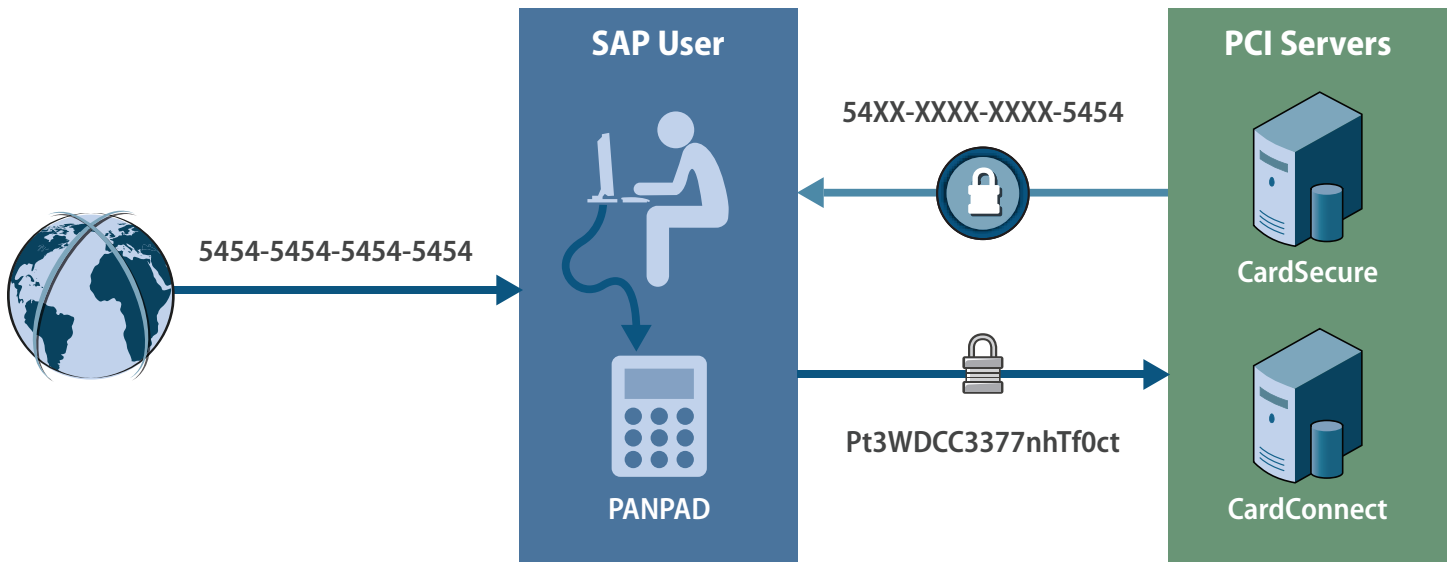
PANPADs allow card data to be encrypted at the point of entry, effectively removing all order entry and research terminals from PCI scope.

Our Solution smart. secure. flexible.

The PANPAD is a card entry device that takes your order entry workstations out of PCI scope. A number of currently available solutions use tokenization to remove most of your IT infrastructure from PCI scope, but order entry terminals have always been a concern. Payment card numbers must be typed directly into the terminals, keeping them in scope.

For most companies that process credit cards, this means that the self-assessment questionnaire (SAQ) form D is required. This form is over 250 questions and can take many man weeks to complete. A PCI certified PANPAD reduces your PCI footprint more than previously possible and provides a multitude of benefits, including the ability to

- Tokenize card data before it touches your company network
- Fill out the much shorter SAQ A or SAQ B
- Secure the entire network, when combined with other PPS offerings



Here's How

In order to securely tokenize data before it touches your system each device that receives card data must have an attached PANPAD. Each PANPAD communicates directly with your tokenization engine as illustrated

1. Customer dictates card number
2. Employee enters card number in PANPAD
3. PANPAD encrypts card and sends to CardSecure
4. CardSecure tokenizes card and returns token value
5. Employee drops token value into order form
6. Order clears and ships

For further information about tokenization review our CardSecure offering and security whitepapers. Available upon request or on our site: www.prinpay.com

Background

In 2003, the Princeton Payments Solution group was formed to address the specific needs of the ERP Community with respect to complex payment environments. CardConnect is PPS's latest card payment interface, building on over a decade of experience connecting the ERP community with the banking community. In 2004, PPS was the first company to encrypt data within an ERP system and pass the PCI audit standards with our CardSecure solution. Subsequently, responding to customer requests to remove SAP from PCI scope, and to address growing security concerns about personal information, PPS developed CardSecure's token solution. PPS clients include General Electric, Adobe, Brother, and Becton-Dickinson.

PPS Personnel

PPS staff are fully engaged with the card payment/processing security community and participate in the PCI Security Council. Their collective experience includes decades in bank operations, bank software development, and bank card technology. They enjoy personal relationships with various technical groups within the bank processing community, underpinning PPS's innovative approaches to ERP card payment issues. PPS's credentials also include advanced degrees in both business and economics. PPS staff understand your business challenges, contact us to find out more about PCI security in ERP environments.

Contact: Alex Chapman

Email: achapman@prinpay.com

Phone: +1 (203) 952-5715

www.prinpay.com