On-Guard Point-to-Point Encryption (P2PE)

A powerful security solution helping merchants fortify their payment infrastructure and protect their brand image

- Encrypt all sensitive cardholder data at the point of swipe, insertion, or tap
- Reduce PCI DSS audit scope by removing sensitive cardholder data from the payment environment
- Save time and money by simplifying the PCI DSS certification process and eliminating the financial burden resulting from a data breach
- Enable seamless integration with legacy systems using a non-intrusive format preserving encryption
- Supported in SRED for all Ingenico PCI PTS approved smart terminals
- Protect your brand image by using a proven solution that powers 75% of PCI P2PE validated P2PE solutions in the U.S. and 60% abroad

ingenico

AXIUM

On-Guard can help merchants reduce their PCI DSS scope and decrease their vulnerability to cybercriminal attacks, while protecting their brand – and their bottom line.

TETRA

Decrease Vulnerability to Cybercriminal Attacks

With On-Guard, sensitive card data are encrypted at the point of entry and remains protected until decrypted at a secure end point so that it's never legible to cybercriminals. With point-to-point encryption from the terminal to the payment host, captured data has no value.

Reduce PCI Audit Scope

Merchants are seeking ways to simplify and limit the scope of PCI security audits by reducing the touchpoints where cardholder data interacts with their systems. On-Guard encrypts sensitive cardholder data so that it is never exposed to the merchant's point of sale (POS) and back office systems, helping to decrease their PCI scope, increase the chance of audit success, and reduce the cost of maintaining compliance.

Deliver Enhanced Security

On-Guard provides an enhanced level of security with unique keys per terminal and transaction. The encryption occurs in the terminal's Secure Reading and Exchange of Data (SRED) module, which is a prerequisite for developing a PCI P2PE validated P2PE solution.

Upgrade Path to Advanced Security

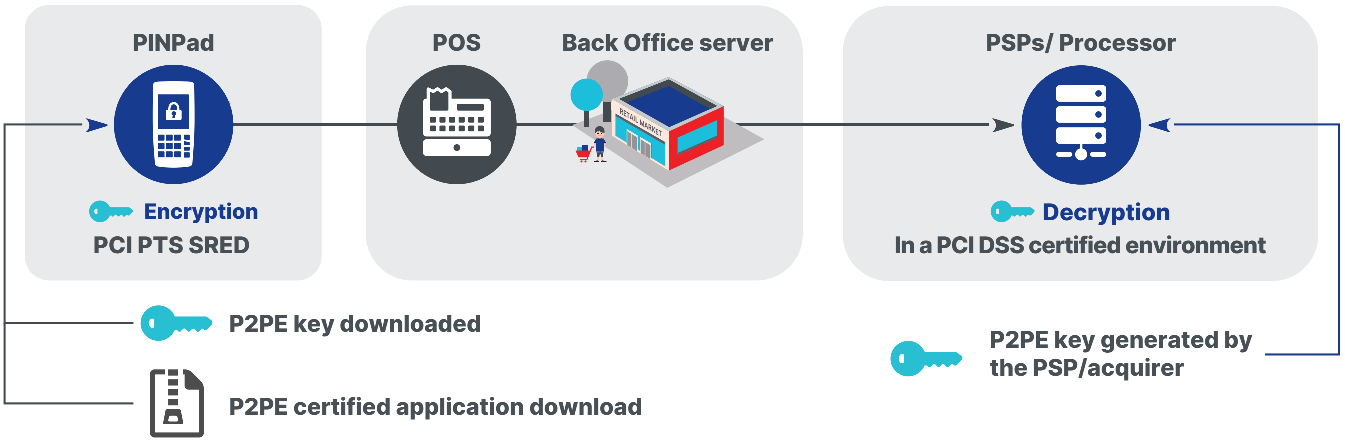
On-Guard encompasses an option for advanced security with Standard Data Encryption (SDE), offering full PAN encryption that is ANSI X9.24-3 compliant DUKPT encryption using either 3DES or AES cryptography. On-Guard SDE works directly with all FIPS or PCI approved HSMs.

Minimize Impact to Legacy Systems

Integration with legacy systems is simplified through the use of NIST-reviewed format preserving encryption. By combining industry-standard DUKPT/3DES encryption with format preserving encryption (FPE), integration with legacy systems is simplified. Modifying the POS or back-office systems for a new format is no longer necessary.

Simplify Integration

To simplify interoperability, the On-Guard decryption system is built using modern XML and web services interfaces. This creates a robust, flexible design that allows processors, gateways, token service providers, and merchants to seamlessly integrate and deploy On-Guard P2PE within their existing environments. On-Guard decryption is supported in industry-leading hardware security modules (HSM).


PINPad
Encryption
PCI PTS SRED
POS
Back Office server
RETAIL MARKET
PSPs/ Processor
Decryption
In a PCI DSS certified environment
P2PE key downloaded
P2PE key generated by the PSP/acquirer
P2PE certified application download

Encryption Point

- Algorithm reviewed by NIST and ASC X9
- PCI PTS approved terminal
- Encryption in SRED module

Decryption Point

- On-Guard decryption application (needed for FPE decryption) runs on standard server hardware
- Supported in Industry-leading HSMs
- Payment and Decryption Service delivered from a PCI DSS certified environment

USA-CAN_DATASHEET_OnGuardP2PE_ING_230406. All rights reserved. This document is not binding and the specifications above can be modified without prior consent. ©2023

www.ingenico.com

ingenico