Agilysys

rGuest® pay

rGUEST® PAY GATEWAY:
A Solution Review

TABLE OF CONTENTS

INTRODUCTION

Merchants today navigate an evolving payments landscape riddled with technology challenges, false statements about security and an increasing regularity of data theft. rGuest® Pay Gateway addresses these challenges, offering the hospitality industry's first, PCI-validated, point-to-point encrypted (P2PE) payment gateway that meets the security needs of merchants everywhere.

The Payment Card Industry (PCI) Security Standards Council develops the standards by which payments are securely processed. The P2PE standard, the PCI Council's newest standard, meticulously defines the rigorous requirements a payment solution provider must adhere to, enabling merchants to securely process payments and keep their network environment out of scope for traditional PCI security assessments.

There are many providers who claim to leverage secure technology for payment transactions and claim to offer PCI scope reduction; however, many of these providers have limits to the amount of security their solutions actually provide. Some, for instance, do not provide 100% hardware-based encryption – something that disqualifies the solution from ever being PCI-Validated. Only when the solution is clearly listed on the PCI Council's site as a certified provider can merchants have confidence that their data is processed via the most advanced technology and security. This significantly reduces the merchant's risk of data breach and the costly burden of PCI assessments. If the provider is not listed on the PCI Council's site, merchants are at greater risk.

The Agilysys rGuest® Pay Gateway P2PE solution – powered by FreedomPay™ – is PCI- and P2PE-certified. rGuest Pay leverages the only gateway solution in North America that is P2PE PCI-validated and also supports EMV, tokenization and a Payment Information Proxy for e-commerce transactions. This solution easily integrates into several of today's Point-of-Sale (POS) systems, property management systems and payment processors. With the coveted PCI validation, merchants employing rGuest Pay have the opportunity to reduce their scope of PCI compliance requirements and can conduct business with the confidence that no unencrypted cardholder data flows through their systems.

This document explores the merchant benefits of PCI-Validated P2PE, the process by which the underlying FreedomPay solution earned PCI validation, and the valuable advantages of the rGuest Pay Gateway platform.

AGILYSYS' RGUEST PAY GATEWAY P2PE SOLUTION – POWERED BY FREEDOMPAY™ – IS FULLY VALIDATED BY THE PCI COUNCIL.

PCI Security Standards Council
PARTICIPATING ORGANIZATION™

WHY P2PE?

Merchants face an increasing number of challenges related to payments: ensuring security, maintaining compliance, managing costs and keeping pace with an ever-changing payments technology landscape, to name just a few. Emerging standards, like the 2015 switch to EMV and digital wallet products from Apple®, Google®, PayPal® and even Starbucks®, have disrupted the payment landscape and sent merchants scrambling for solutions.

The stakes are high. For many merchants, a growing threat of cyber crime and malware has placed security at the top of the priority list. In today's hospitality environment, preventing a data breach and keeping guest data secure is a need that cannot be ignored. To complicate matters, the solution marketplace is rife with misinformation and biased opinions.

The PCI Council has created and published a standard against which to validate payment solutions. In doing so, the payments industry has established a very clear, incontrovertible technology standard that, when followed, secures a merchant's payment processing and infrastructure. With PCI-validated P2PE, transactions are entirely encrypted before they even enter the merchant's environment, essentially removing cardholder data from the merchant's POS and network.

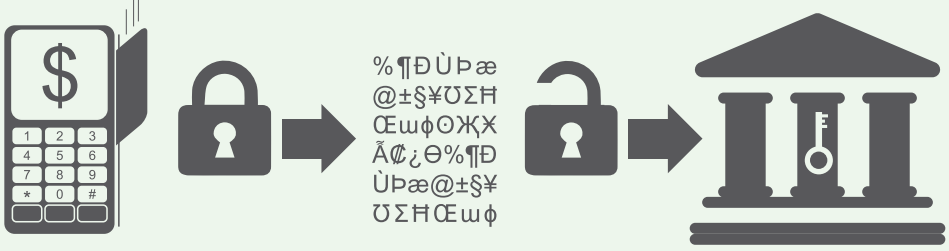
Point-to-point encryption (P2PE) delivers two critically important benefits to merchants:

- P2PE offers the greatest possible security for guest payment information, thus protecting merchants from damaging data breaches.
- Payment solutions featuring PCI-validated P2PE allow merchants to greatly reduce their PCI DSS compliance burden.

rGuest Pay Gateway, powered by FreedomPay's P2PE solution, earned PCI P2PE validation in 2014. It offers merchants unparalleled payment security and functionality and further protects that investment with EMV support. This foresight is setting the pace for the entire payments industry. Moreover, merchants who use rGuest Pay Gateway benefit from a reduced annual assessment report that requires only 19 quick controls instead of the standard 284 documentation requirements.

How P2PE encryption works:

1. Data is entered into the payment terminal.
2. Before the data is stored/transmitted, it is transformed into unreadable code.
3. Only with a special key does the data become readable once again.



PCI P2PE STANDARDS

In 2012 and 2013, the PCI Security Standards Council released the PCI P2PE Standard: a set of controls aimed at providing clarity and definition around point-to-point encryption.

$225,000+

[1]AVERAGE ANNUAL COSTS OF A PCI AUDIT

$3.5MM+

[2]AVERAGE COST OF A DATA BREACH

[1]PCI DSS Trends 2010 QSA Insights Report. Ponemon Institute Research Report. March 2010

[2]2014 Cost of a Data Breach Study: Global Analysis. Ponemon Institute Research Report. May 2014.

There are three core principles underlying PCI-Validated solutions:

- Hardware to hardware encryption and decryption with a POI (point-of-interaction) device that has SRED (Secure Reading and Exchange of Data) listed as a function and enabled.
- Certified to have a validated, secure distribution channel. This means the entire chain of custody of the POI devices follow strict controls regarding shipping, receiving, tamper-evident packaging and installation.
- P2PE Instruction Manual (PIM) that guides the merchant on POI device use, storage, return for repairs and regular PCI reporting.

Merchants who implement PCI-Validated P2PE solutions that adhere to the secure principles gain an important advantage: a reduction in the scope of their PCI assessments.

As stated on the PCI Security Standards Council's FAQ web page:

> "Only Council-listed solutions are recognized as meeting the requirements necessary for merchants to reduce the scope of their cardholder data environment (CDE) through use of a P2PE solution."
> - PCI Security Standards Council

To earn validation, P2PE solution providers must ensure their solutions satisfy all requirements of the P2PE standard. As a requirement for the P2PE solution assessment, the solution provider must supply the P2PE assessor with all required documentation, software, access to facilities and access to third-party service providers used in connection with the P2PE solution.

The PCI P2PE standard encompasses nearly 1,000 individual controls governing encryption and decryption methodologies, software applications, device management and operations related to distribution and cryptographic key injection facilities.

To summarize the onerous P2PE assessment process, solutions must be able to account for:

- Encryption Device Management: Secure Cryptographic Devices (SCDs) provide tamper resistance and detection, as well as response features to help prevent successful attacks involving penetration, monitoring, manipulation, modification or substitution of the devices to recover protected data.
- Application Security: The application must not transmit or store clear-text primary account numbers (PANs) or sensitive authentication data (SAD) outside the device, and must only use communication methods included in the scope of the PCI-approved POI device evaluation.
- Encryption Environment: The solution provider must maintain inventory control and monitoring procedures to accurately track POI devices in their possession and provide related instructions to merchants (P2PE Instruction Manual).
- Decryption Environment Device Management: Documented procedures must exist and be demonstrably in use to ensure the security and integrity of decryption devices as they are placed into service, initialized, deployed, used and decommissioned.
- P2PE Cryptographic Key Operations: Key management, cryptographic algorithms and cryptographic key lengths must be consistent with international and/or regional standards. Key components must be protected at all times during transmission, conveyance and movement between locations.

Agilysys partners with FreedomPay™, Ingenico™ and ScanSource™ to deliver all facets of the P2PE solution. Ingenico Group's best-in-class hardware and ScanSource's secure distribution and key injection capabilities are meticulously vetted as part of FreedomPay's complete PCI P2PE assessment process.

"ONLY COUNCIL-LISTED SOLUTIONS ARE RECOGNIZED AS MEETING THE REQUIREMENTS NECESSARY FOR MERCHANTS TO REDUCE THE SCOPE OF THEIR CARDHOLDER DATA ENVIRONMENT (CDE) THROUGH USE OF A P2PE SOLUTION."

— PCI SECURITY STANDARDS COUNCIL RESPONSE TO FAQ 1162

BUYER BEWARE

Many vendors in the payments industry claim to offer P2PE, usually bundled with a POS system and/or payment terminal and/or payment gateway. However, merchants must be cautious about false claims and misstatements. Any P2PE solution that does not adhere to the stated PCI requirements and is not listed by the PCI Security Council as validated P2PE will not exclude the merchant's POS and supporting network from compliance requirements.

It is incumbent on merchants to work with their Qualified Security Assessor (QSA) on vetting fact from fiction. There are a number of vendors making claims that simply cannot hold up to the explicit facts as stated by the PCI Council. Only PCI-Validated P2PE solutions have been thoroughly audited and evaluated, delivering the highly preferred benefits of security assurance and true scope reduction.

PCI DSS SCOPE REDUCTION

PCI compliance validation has grown to become a burdensome and costly process for large and small merchants alike. Its complexity is evident in the PCI DSS Self-Assessment Questionnaire (SAQ). The SAQ is a validation tool intended to assist merchants and service providers who are permitted by the payment brands to self-evaluate their compliance with PCI DSS. With 284 individual, complex controls to document and maintain, PCI DSS compliance has historically required merchants to invest significant time and resources each year.

Employing a PCI-Validated P2PE solution offers merchants significant reductions in scope for PCI DSS compliance. Because all clear-text cardholder data are removed from the merchant's POS and network environment, that infrastructure is no longer subject to an extensive PCI compliance documentation process.

Merchants who employ a PCI-validated P2PE solution will notice a reduction in the documentation necessary as well as a reduction in the underlying costs of maintaining a less secure environment. At only 19 questions, SAQ P2PE-HW is a substantially shorter compliance document available only to merchants who process cardholder data via approved payment terminals as part of a Council-listed P2PE solution.

To be eligible for the SAQ P2PE-HW, merchants must confirm that they:

- Exclusively use a PCI P2PE solution listed on the PCI SSC's List of Validated P2PE Solutions.
- Do not store, process or transmit any cardholder data on any system or electronic media (for example, on computers, portable disk or audio recordings) outside the payment terminal used as part of the Council-listed P2PE solution.
- Do not store any cardholder data in electronic format. This includes verification that there is no legacy storage of cardholder data from other payment devices or systems.
- Have implemented all controls in the P2PE Instruction Manual (PIM) provided by the P2PE Solution Provider.

With substantially fewer requirements to complete, largely related to the proper maintenance and implementation of the P2PE payment terminal, SAQ P2PE-HW removes the core elements of the merchant environment from scope: the POS, operating system and network. As an added benefit, penetration tests and vulnerability scans are no longer required. This enables POS devices and operating systems that would otherwise fall out of compliance to remain in use because the P2PE payment terminal circumvents that infrastructure, and no cardholder data flows through legacy systems.

"OFFICIAL PCI VALIDATION FOR A P2PE SOLUTION MEANS THAT MERCHANTS CAN SIGNIFICANTLY REDUCE THEIR SCOPE FOR PCI DSS VALIDATION AND OBTAIN THIRD- PARTY ASSURANCE THAT NO CARDHOLDER DATA PASSES THROUGH THEIR NETWORK ENVIRONMENT IN AN UNENCRYPTED STATE."

— MATT GETZELMAN, NATIONAL PCI PRACTICE DIRECTOR, COALFIRE SYSTEMS, INC.

P2PE PAYMENT TERMINALS

Core to the PCI-validated P2PE solution is the "Secure Reading and Exchange of Data" (SRED) module, designed to encrypt data at the Point-of-Interaction. The SRED module applies the security and cryptographic protection of PIN data to the reading of card data presented by magnetic stripe, EMV, contactless/NFC and manual entry.

As Rob Martin, Vice President of Security Solutions for Ingenico Group explains,

> "In order for P2PE to be in the SRED module, the encryption key management and encryption of the cardholder data must be done in the device's security processor. This and other P2PE program aspects must be in firmware, as opposed to being in the application. The firmware is reviewed and certified as meeting the SRED requirements by a PCI approved laboratory."

The rGuest Pay solution leverages SRED-enabled terminals from Ingencio Group, offering merchants flexibility to roll out a variety of compliant devices. All Ingenico devices provide support with traditional magnetic stripe payments in addition to alternative and emerging payment methodologies such as EMV and NFC.

Partnering with Ingenico, Agilysys offers a diverse portfolio of payment devices to meet the specific needs of hospitality businesses. rGuest Pay supports a wide variety of PCI P2PE payment device options for every use-case, including countertop, pay-at-table, EMV, mobile tablet and signature capture scenarios.

THE PAYMENT INFORMATION PROXY (PIP)

In complex enterprises common to the hospitality industry, even the security offered through SRED-compliant payment terminals and validated P2PE may still be insufficient to secure all of a merchant's payment channels. Cardholder data collected via e-commerce interfaces from online travel agents must also be protected.

rGuest Pay Gateway's Payment Information Proxy (PIP) secures these e-commerce transactions. Based on the HTNG Secure Payments Framework, the PIP intercepts e-commerce messages containing card data and replaces the sensitive data with a unique token. Therefore, merchants' systems remain secured and infrastructures remain out of PCI scope.

How the Payment Information Proxy (PIP) Works:

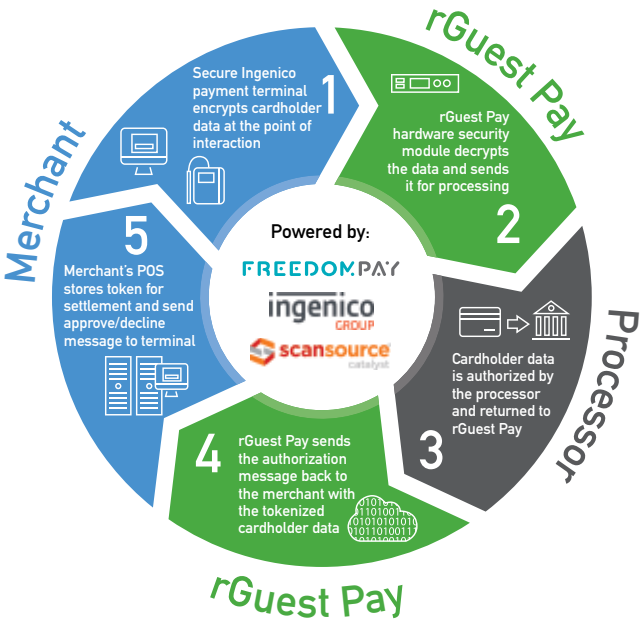
1. Guest enters card data into a 3rd-Party OTA website.
2. OTA sends request not to PMS, but rather to the rGuest PIP
3. PIP extracts card data from message and replaces it with a token.
4. Sanitized message is forwarded to your PMS

ONLY A PCI-VALIDATED, P2PE PAYMENT TERMINAL CIRCUMVENTS THE POINT-OF-SALE SYSTEM AND NETWORK.

CONCLUSION

rGuest Pay Gateway is purpose-built for the complex merchant environments prevalent throughout the hospitality industry. With unparalleled security as a core requirement, rGuest Pay offers official PCI-P2PE validation, allowing Agilysys to offer PCI cost and scope reduction that other providers cannot. And by layering tokenization and the Payments Information Proxy atop our strong P2PE platform, merchants are assured to be protected across all business channels. Additionally, rGuest Pay delivers robust connectivity to all major U.S. credit card processors. It also supports a wide variety of PCI P2PE payment devices.

As the payment landscape shifts to include EMV and NFC transactions, rGuest Pay enables merchants to stay ahead of the game. Using North America's first fully-functional PCI-Validated P2PE platform with EMV and NFC-ready terminals, rGuest Pay sets the standard for merchants to deliver an enhanced guest experience based on security, functionality and superior technological intelligence.



About Coalfire

Coalfire is the global technology leader in cyber risk management and compliance services for enterprises and government organizations. Coalfire's professionals are renowned for their technical expertise and unbiased assessments and recommendations. Coalfire's approach builds on successful, long-term relationships with clients to achieve multiple compliance objectives tied to a long-term strategy to prevent security breaches and data theft.

About Ingenico Group

Ingenico Group is the global leader in seamless payment, providing smart, trusted and secure solutions to empower commerce across all channels, in-store, online and mobile. With the world's largest payment acceptance network, Ingenico delivers secure payment solutions with a local, national and international scope. Ingenico is the trusted world-class partner for financial institutions and retailers, from small merchants to several of the world's best known global brands. Their solutions enable merchants to simplify payment and deliver their brand promise.

BY IDENTIFYING THE IMPORTANT DIFFERENCES IN TODAY'S PAYMENT GATEWAY OFFERINGS A MERCHANT CAN MAKE THE MOST INFORMED DECISION AND SECURE ALL CARDHOLDER DATA.

About FreedomPay

FreedomPay is the engine inside the world's expanding and interconnected ecosystem of commerce. FreedomPay makes payments smarter, simpler and more secure. The FreedomPay Commerce Platform is a multi-patented solution portfolio designed to enable companies to embrace current trends and accelerate innovation. The platform seamlessly bridges the gap across in-store, web and mobile by interconnecting POS systems, transaction processors, incentive engines and other disparate systems to a cutting edge payment gateway. The FreedomPay Commerce Platform P2PE solution provides merchants complete payment data security, including EMV and NFC compliance, in accordance with the coveted certification from the PCI Security Standards Council.

WITH UNPARALLELED SECURITY AS A CORE REQUIREMENT, RGUEST PAY OFFERS OFFICIAL PCI-P2PE VALIDATION, ALLOWING AGILYSYS TO OFFER PCI COST AND SCOPE REDUCTION THAT OTHER PROVIDERS CANNOT.

Agilysys

ABOUT AGILYSYS

Agilysys is a leading developer and marketer of software-enabled solutions and services to the hospitality industry. The company specializes in next-generation point-of-sale, property management, inventory and procurement, workforce management, analytics, document management and mobile and wireless solutions. These solutions are designed to streamline operations, improve efficiency, increase guest recruitment and wallet share, enhance the guest experience and maximize revenue potential. Agilysys operates extensively throughout North America, Europe and Asia, with corporate services located in Alpharetta, GA, and offices in Singapore, Hong Kong and Malaysia. For more information, visit www.agilysys.com.