Secure Payments Framework for Hospitality

VERSION 1.0 | FEBRUARY 2013

Hotel Technology next generation™

Hotel Technology Next Generation (HTNG) is a non-profit association with a mission to foster, through collaboration and partnership, the development of next-generation systems and solutions that will enable hoteliers and their technology vendors to do business globally in the 21st century. HTNG is recognized as the leading voice of the global hotel community, articulating the technology requirements of hotel companies of all sizes to the vendor community. HTNG facilitates the development of technology models for hospitality that will foster innovation, improve the guest experience, increase the effectiveness and efficiency of hotels, and create a healthy ecosystem of technology suppliers.

Manufacturers and software providers shall not claim compliance with portions of the requirements of any HTNG specification or standard, and shall not use the HTNG name or the name of the specification or standard in any statements about their respective product(s) unless the product(s) is (are) certified as compliant to the specification or standard.

This specification has not been verified for avoidance of possible third-party proprietary rights. In implementing this specification, usual procedures to ensure the respect of possible third-party intellectual property rights should be followed. Visit http://htng.org/ip-claims to view third-party claims that have been disclosed to HTNG. HTNG offers no opinion as to whether claims listed on this site may apply to portions of this specification.

Executive Summary

The hospitality industry is a prime target for payment card data thieves. According to the Trustwave SpiderLabs Global Security Report 2011, approximately 38% of all payment card data breaches occurred within the hotel sector.

The very nature of the hotel industry makes it particularly vulnerable. Hotels are unlike industries such as retail, where payment card data is often needed only for the duration of sale. Hotels must store payment cards for weeks and months for reservation guarantees. Additionally, payment card information is often provided to the hotel through a series of unrelated parties that are outside the control or influence of the hotel. As a result, solutions that are effective for retail and other industries have significant gaps when applied to hotels' needs.

This document presents a framework of best practices and references standards that can be applied to reduce the risks and costs associated with handling payment card information for hotels. This framework was developed by a group of security experts from numerous hotel companies. The HTNG approach shifts the risk of handling payment data away from the hotel, replacing the data with "tokens." These tokens are useless to cyber thieves. This approach dramatically improves security, and is aligned with the PCI Council's best practices.

The HTNG framework builds on existing solutions from the payment industry and is consistent with approaches being pursued by most major hotel groups. However, it extends these efforts to cover gaps that are not addressed by existing commercial solutions, or indeed by even the most advanced hotel company.

The result allows hotels to complete the process of removing ALL payment card data from ALL of their systems, dramatically reducing the cost of PCI compliance. Because hotels have no obligation or reason to tell customers if a breach of useless data occurs, the cost and impact of remediation, and the effect on brand reputation, are minimized.

This framework creates new opportunities for payment solution providers to address critical industry needs by enhancing existing solutions or developing new ones. Opportunities include extending tokenization and vaulting services; providing new services to securely handle and route payment card data to and from external parties and systems (e.g. online travel agencies, central reservation systems, meeting planners); and developing secure stand-alone devices to allow hotels to safely view the actual payment card data associated with a token, when needed.

Additionally, the framework helps to educate and inform hoteliers about existing payment solutions that support elements of the framework, such as secure swipe terminals and tokenization services.

Contributors

The following companies and individuals participated in the HTNG working group that developed this document. Individuals identified with asterisks (*) had left their respective companies by the time the document was completed, and did not have an opportunity to comment on the final document.

HTNG would like to gratefully acknowledge the following:

SIGNIFICANT CONTRIBUTORS

Carlson Rezidor Hotel Group – Chip Ross

Delaware North Companies, Inc. – Brian Alessi, Yvette Vincent

Fairmont Raffles Hotels International – Paul Chin

Hilton Worldwide – Joy Millard*

Hyatt Hotels Corporation – Dave Malcom*

Kilian & Partner - Wibecke Vinke

Mandarin Oriental Hotel Group – Raju Daryanani

Marcus Hotels & Resorts – Matthew Tarasewicz

Marriott International – John Bell, Kristin Harding, Jude Sylvestre

Meliá Hotels International – Christian Palomino

Omni Hotels – David Jackson

Starwood Hotels & Resorts Worldwide, Inc. – Shamla Naidoo, Jim Weiler

ADDITIONAL PARTICIPANTS

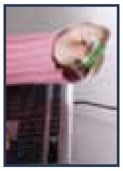
Accor – Serge Saghroune

Carlson Rezidor Hotel Group – Kathy Orner

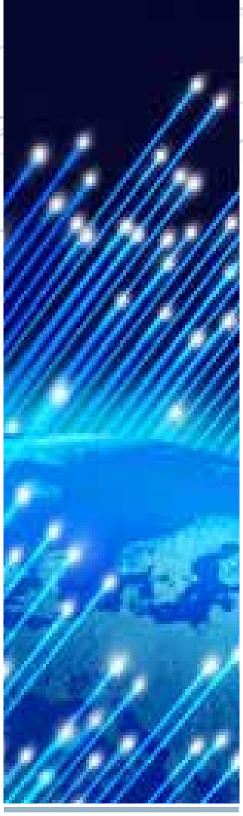
InterContinental Hotels Group – Steven Bardsley, David Billeter*

Jumeirah Group – Emad Maisari*

Wyndham Hotel Group – David Durko



Contents



Introduction

Hotel systems are vulnerable to attack for two reasons: they contain a wealth of valuable payment card data, and many hotels are small businesses with relatively weak protections in place. **Hotels are inherently harder to secure than most businesses, for three reasons:**

- Reservations, which typically include payment card data for guarantees or deposits, may traverse several different, unrelated companies between their point of origination (e.g. a travel web site) and the hotel.
- Even within a single hotel group, reservations for customers in one region routinely travel to hotels in other world geographic regions. Some elements of the payment card processing infrastructure vary in different world regions and countries.
- Payment card data may need to be retained for much longer than in traditional brick-and-mortar businesses, because the elapsed time from the provision of the payment card by the customer, until the settlement of the transaction, is often weeks, months or even longer.

Standard solutions such as encryption and tokenization, widely adopted by many other industries, have proven **challenging and less than fully effective for hotels**. Most tokenization schemes assume that the merchant controls the payment card transaction throughout its life cycle, and can therefore select a single tokenization solution and implement it consistently. If multiple world regions are involved, different solutions can be implemented in different regions, because the card transactions do not need to move between regions.

At its core, tokenization assumes that the party that converts payment card data to a token (such as a gateway) will be the same party that will need to convert it back to payment card data for subsequent use. For the reasons discussed above, **this assumption is often invalid for hotel transactions**.

Many hotel companies already implement tokenization solutions, despite their limitations. tokenization, when properly deployed, eliminates many of the risks of breaches. It also largely removes the merchant's systems from the scope of PCI requirements, by replacing sensitive payment card data with tokens. As substitutes, these tokens are worthless to a thief, but can still be used by authorized parties to process card transactions.

There are many quality tokenization-based solutions available on the market for this purpose, and they can provide a solid foundation for payment card security. **It is not the intent of this document to propose a competing approach**, because as far as these solutions go, they work well. But many of them address only a portion of the problem. None of them presently address the need of the hotel industry to be able to exchange payment information between third-party booking agents and hotels.

Security experts from numerous global hotel companies have collaborated through HTNG to create this framework for data protection. Many non-participating hotel companies have also pledged their support for this approach, which combines multiple data security best practices to create a solution tailored to the unique needs of the hotel business environment. This framework, fully implemented, will enable a hotel to **completely remove its systems from PCI scope**. It does not eliminate PCI requirements that apply to non-system aspects of payment card security, such as human factors and physical security, although it can significantly reduce the complexity of meeting these requirements by making payment card data inaccessible to hotel staff.

Importantly, the framework **extends existing payment security solutions** to meet the unique challenges of the hotel industry, **allowing them to interoperate across multiple independent entities**. The framework is relatively simple in concept and enables hotels to secure their environments in a comprehensive and unified manner. Use of the framework results in **lower costs and risks** associated with handling payment card data for hotels of all sizes.

This paper describes the key elements of the framework. It shows how payment solutions providers and hotel system software vendors can work together to secure the customer's payment information. These **partners will find new business opportunities**, and become an integral part of the entire solution, by developing additional products or services to better meet the needs of the hotel industry.

For clarity, defined terms are utilized throughout the remainder of this document. Capitalized terms are defined in the Appendix.

The Problem

Data Security Issues and Challenges in the Hotel Industry

The hotel industry presents a uniquely complex data security problem due to its multiple reservation and payment systems, involvement with assorted vendors and its retention of Customer Payment Card Data. Each part of the system presents an additional window for cybercriminals to break through. While large hotel organizations can and often do invest heavily in achieving and maintaining PCI compliance, the necessary investment is beyond the financial means of many small businesses. Smaller vendors or independent hotels may not address payment card security as a result.

The structure of hotel transactions means they will continue to be a favorite target of cyber-criminals until there is a common data security solution to which all of the organizations, systems and vendors associated with the hotel industry adhere. However, it is critical that such a solution be affordable for small and large hotel companies and vendors alike, so that there can be consistency across the hospitality industry.

PCI-DSS Is Not a Solution for the Hospitality Industry

The Payment Card Industry Data Security Standard (PCI-DSS)[1] is a set of security requirements designed to protect cardholder data during storage, processing and transmission. These requirements include configuration standards, patching, monitoring, auditing and other complex and often time-consuming practices, which are worthwhile but often beyond the core function, skill and budgets of many hotel companies. Hotels must also ensure that any third parties (called service providers) with whom cardholder data must be shared also meet PCI-DSS compliance requirements. Depending on the number of credit card transactions processed annually, extensive independent audits may be necessary in addition to the always-required self-audits. Some hotel companies use a large number of third parties, adding to the PCI-DSS compliance workload and expense.

[1/] The PCI DSS is administered and managed by the Payment Card Industry Security Standards Council (PCI SSC), an independent body created by the major payment card brands in 2006.

The Solution

The HTNG Secure Payments Framework

The HTNG Secure Payments Framework is based on the simple concept that actual Payment Card Data is not stored, processed or transmitted by any system (as defined by the PCI-DSS) within the control of the Hotel company. This essentially removes cardholder data from the Hotel Application System environment, putting those systems out of scope for PCI-DSS requirements. In other words, if no Payment Card Data is stored, processed or transmitted within a Hotel Application System, the PCI standard no longer applies to that system, thereby reducing the complexity and expense of PCI compliance.

Business Problem

Existing solutions in the marketplace can address this objective to a degree, but fail in two main areas:

- Exchange of payment information with trading partners, such as franchisees or online travel agencies.
- Exchange of payment information in transactions that use different secure-payments service providers, as may be required to service different geographic regions or for other business reasons.

Business Solution

The HTNG Secure Payments Framework **documents the best practices** shared by many commercial systems, and **introduces new concepts** capable of handling the secure *exchange* of Payment Card Data between unrelated parties. While this exchange involves systems that will necessarily fall within the scope of PCI, it can be accomplished by companies in the payments business (and whose systems will always be within PCI scope) rather than by Hotels. Fully implemented, this approach dramatically reduces the scope of the Hotel Systems that fall under PCI requirements, and more importantly, reduces Payment Card risk.

The HTNG Framework also identifies interface standards for managing Tokens and for the exchange of tokenized or untokenized Payment Card Data. While the standards may or may not be useful for exchange of Payment Card Data between systems that already exchange such data securely, they are intended to facilitate the necessary exchanges among systems that follow different tokenization approaches. Having written once to the standard, a software package will be able to quickly connect with any other system that has written to the standard. **This allows a Hotel to quickly extend its payment information security framework to a large number of online distribution partners**, for example.

Since Hotel companies generally need to capture payment information from the Customer while on property (e.g. swipe at the front desk), it is important that this solution includes the ability to capture swiped Payment Card Data in a manner that does not cause downstream systems to be reintroduced into the scope of the PCI-DSS. Tamper-resistant swipe/capture devices that immediately tokenize or encrypt the Payment Card Data have the potential to render these devices and associated data out of scope of the Hotel's PCI-DSS compliance requirements. (In the case of encryption, the decryption keys must be stored outside the control of the Hotel).

Roles for Existing Payment Solution Providers

Existing participants in the payment security ecosystem play roles in the framework. The framework makes no assumptions about which companies or types of companies provide which services or devices; any organization may participate in one or multiple roles.

Tokenization Service providers securely receive Payment Card Data; convert it into a tokenized format that can be substituted for the original Payment Card Data; and recover the original Payment Card Data when needed.

Secure Payment Terminals (capture devices) obtain Payment Card Data via card swipe (mag stripe, EMV), keypad entry, scan, NFC or other means, and send the data to the Tokenization Service, where it is converted into a Tokenized Payment Method Record that can be safely returned to the Hotel Application System. A Secure Payment Terminal must implement security sufficient to keep all other Hotel Systems out of PCI scope, through a combination of tokenization, encryption, tamper-resistant design or other means. If encryption is used, the decryption keys must be inaccessible to the Hotel.

Hosted Payment Collector services provide a secure mechanism for collecting payment information over the web, and return tokenized payment information to the user's browser.

Payment Gateways or acquirers may offer Tokenization Services, Hosted Payment Collector services, Secure Payment Terminals and/or Payment Information Proxy Services.

Hotel Application Systems, such as property management systems (PMSs), point-of-sale systems (POSs), spa/activity systems, loyalty systems and guest satisfaction systems, must never store Payment Card Data, only Tokens. Any time raw Payment Card Data travels through these systems (as for example may occur after a card swipe), it must be encrypted using a key that is not available to the Hotel. When actual Payment Card Data is required (for example to process a draft capture), the Token is transformed (outside the Hotel's environment) and sent as usable Payment Card Data to the final service provider.

Hotel Application Systems are any IT systems that are operated by or for the Hotel. Common examples of Hotel Application Systems that may use Payment Card Data include property management systems, point-of-sale systems, spa/activity systems, loyalty systems and guest satisfaction systems. A major strategy of this framework is to replace Payment Card Data that might be stored on these systems with tokenized payment information (see Tokenized Payment Method Record). Since tokenized data is not useful to others, it removes these systems as targets and takes them out of PCI concern.

Payment information that is transmitted across the Hotel network should be secured both by encryption of the message that contains the data and by using a secure transport layer. This normally requires a Secure Payment Terminal (swipe/data entry device) that encrypts the data from a swiped card or keypad entry. Based on current PCI rules, if the Hotel does not have the encryption keys required to decrypt the message that contains the Payment Card Data, then the systems through which this encrypted message passes are not considered to be in PCI scope.

Central Reservation Systems (CRSs) may be operated by a Hotel (in which case they may be treated as any other Hotel Application System), or by a third-party (another Hotel company or a third-party service provider). CRSs operated by a Hotel must never store Payment Card Data, only Tokens, if they are to remain outside of the Hotel's PCI scope. When a reservation requires the collection or distribution of Payment Card Data, it must be collected securely using one of the methods detailed in this document, and then sent directly to a Tokenization Service or through a Payment Information Proxy (PIP) Service (see below). For example, if the CRS uses a Tokenization Service that is incompatible with the Tokenization Service used by the Hotel, and if the Payment Card Data needs to be used by the Hotel, then the message with the reservation and Token should be sent through the CRS's PIP Service to be de-tokenized and routed to the Hotel's PIP Service for re-tokenization. It is also possible for the CRS to provide consolidated services, including tokenization and routing, on behalf of the Hotel, in which case the CRS would be acting as its own PIP Service, and the Hotel can use a solution which, while still adhering to the framework, can be implemented using fewer providers.

A Central Reservation System (CRS) as defined here is a common system that is shared by multiple properties. This distinguishes it from property-based hotel reservation system (for example, PMS). It is expected that a CRS would use this framework and store Tokens instead of actual Payment Card Data. At some point the CRS would need to forward the reservation, including payment information, to the Hotel. If the Hotel is using a different Tokenization Service, however, then the Hotel will not be able to use the Token created for the CRS. In this case, the CRS would send the message through its Payment Information Proxy (PIP) Service, which would extract the Token information and replace it with real payment information. The CRS's PIP Service then forwards the message with payment information to the Hotel's PIP Service. The Hotel's PIP Service replaces the payment information with the tokenized information (using the Hotel's tokenization scheme) and sends the now-safe message onward to the Hotel Application System.

Hotel Web Sites collect Payment Card Data for a Hotel, either as a part of a reservation or to support some other business transaction. HTNG has previously defined the concept of a Hosted Payment Collector System (HPCS, referred to as Hosted Payment Capture Service in some HTNG documents), which allows the collection of Payment Card Data on a Hotel Web Site using a secure third party, which provides the Hotel with a Token that can safely be stored on Hotel Application Systems for use as needed. The HPCS partner does not need to host the entire Hotel Web Site, just the pages used to collect payment information. This allows the Hotel to separate the responsibilities of hosting a Hotel Web Site from hosting those pages used to collect Payment Card Data. It can thereby remove the Hotel Web Site from the scope of PCI requirements.

Online travel agencies (OTAs) and distribution intermediaries may use their own service providers for payment information security. While implementation of the HTNG Secure Payments Framework can remove their systems from PCI scope, there is no requirement for them to implement it. Whether they do or not, when an OTA needs to send Payment Card Data to a Hotel, raw payment information is sent over a secure channel (like HTTPS), either from the OTA system or from its Payment Information Proxy (PIP) Service (see below) to the Hotel's PIP Service. The Hotel's PIP Service tokenizes the Payment Card Data in the message and forwards the revised message to the Hotel Application System.

Securing the Payment Collection Process

One of the core tenets of this Framework is the isolation of systems required to handle actual payment data from those of the Hotel, which should only handle tokenized data. There are several common occasions where Payment Card Data needs to be collected:

- When the Customer is physically present with the Payment Card
- When the Customer is interacting with staff over the phone
- When the Customer is making a self-service transaction over the Internet

The Secure Payment Terminal (SPT) is designed to address the first situation. The SPT is a device that collects the Payment Card Data via keypad and/or card swipe and immediately encrypts the Payment Card Data so it can be securely sent to the Tokenization Service (through the Payment Information Proxy). Only the Tokenization Service has the key to decrypt the Payment Card Data. This allows the data to pass securely through the Hotel Application Systems without bringing those systems or their networks into PCI-DSS scope. In the case where the Customer calls into the Hotel or a Hotel operated call center, it is possible to have the staff use the SPT to enter the Customer's payment data securely. The staff in this case still falls within PCI scope but the systems are removed.

The Framework identifies one potential alternative solution based on an Interactive Voice Response (IVR) System. When a secure IVR System is available and the phone call gets to the point where it is necessary to provide Payment Card Data, the caller is transferred to the IVR System. The IVR System collects the data, encrypts it, sends it for tokenization and then sends the tokenized data to the Hotel Application System that needs the data. The IVR then returns the caller back to the staff member if needed. This process allows the Payment Card Data to bypass the staff entirely.

The third case is for those occasions where the Customer is able to complete transactions or update their personal information through a Hotel Web Site or mobile application. In this situation the web page (or service) that collects the Payment Card Data can be provided by a secure third party called a Hosted Payment Collector service (HPCS). The Customer's browser is redirected to a page securely hosted by the HPCS to collect the Payment Card Data. The HPCS collects the Payment Card Data and sends it to the Tokenization Service, which returns the Token to the HPCS. The HPCS then redirects the browser back to the original Hotel Web Site, returning the Token.

Each of these solutions addresses the core issue of collecting the Payment Card Data in a way that isolates the Hotel Application Systems from the payment data collection process.

Potential New Service Offering for Payment Solution Providers

In addition, there is a need for existing or new participants to provide a payment service not available on the market today.

A Payment Information Proxy (PIP) Service separates the responsibilities of extracting the Payment Card Data portion of a transactional message, and the tokenization or de-tokenization of the payment information. Because the PIP abstracts these responsibilities from the underlying systems, it allows existing and legacy systems to work with Tokens even though the systems may not know anything about tokenization.

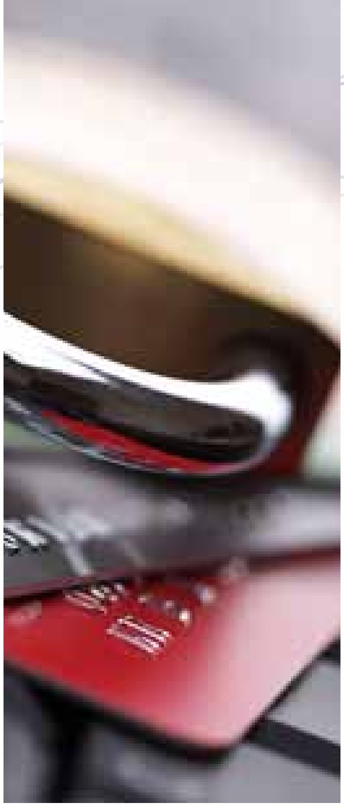
THE PIP HAS THE FOLLOWING RESPONSIBILITIES:

- Accepts business transaction messages containing Payment Card Data, and extracts the Payment Card Data.
- Securely forwards the Payment Card Data to a Tokenization Service and accepts a Tokenized Payment Method Record back from the Tokenization Service.
- Replaces the Payment Card Data in the original message with the Tokenized Payment Method Record.
- Sends the modified message forward to the target destination.
- Working in reverse, accepts messages with Tokenized Payment Method Records and replaces it with the original Payment Card Data retrieved from the Tokenization Service before forwarding the resulting message to its target destination.

THE PIP IS CONFIGURED TO BE ABLE TO:

- Reach the correct Tokenization Service for each Hotel.
- Route and deliver the messages to various Hotel and partner systems.
- Determine which targets only accept Tokenized Payment Method Records, and which are allowed to access raw Payment Card Data.

Conceptually, the PIP can be configured to support multiple Tokenization Services, allowing the exchange of Tokenized Payment Method Records between parties that use different Tokenization Services. Because the PIP must be able to handle messages with Payment Card Data, the PIP is always in PCI scope.



Tokenization

The Basis of the HTNG Secure Payments Framework

Tokenization is a process that intercepts sensitive payment information at the point of sale and substitutes the Payment Card Data with a randomly generated proxy or marker known as a “Token.” The Token can be used in all subsequent business transactions for that Hotel only and can be stored in a Hotel Application System without exposing that system to PCI compliance requirements.

Tokenization is a security solution component particularly well suited to the hotel industry. The Token allows multiple parties, and their respective systems, to process payments for hotel transactions without storing cardholder data, thereby providing greater Payment Card security and massively reducing hotel liability in the event of a security breach.

How Does Tokenization Work?

Tokenization protects the actual Payment Card number upon the first contact in a transaction process. The actual Payment Card Data is encrypted at the first encounter (e.g., point of sale, capture, web entry, arrival from third-party system) and is sent to a Tokenization Service, which operates a secure server and data store known as a “vault.” The Tokenization Service decrypts the Payment Card Data and creates a replacement Token. If the card information is first obtained through a Secure Payment Terminal, the encryption method uses “keys” that are outside the control of that device or any other Hotel Application System, meaning that the device can encrypt Payment Card Data, but the keys necessary to decrypt the data are stored securely elsewhere. The Payment Card Data is stored in the vault and the Token is returned to the Hotel (along with an authorization response, if requested). The Token can be used for a single transaction, or can be stored in the Hotel Application System for continued future use.

There are different approaches to tokenization, and the HTNG Secure Payments Framework is designed to work with any of them. Tokenization schemes work by replacing Payment Card Data with a randomly generated number or set of characters. Some tokenization schemes are "format-preserving," meaning that the resulting Tokens look like valid card numbers, and may preserve such important elements as the card type (first 1-4 digits), bank ID (first 6 digits) and/or last four digits. Format-preserving Tokens are typically easier to implement in existing systems, because fixed-length data fields need not be changed, and logic for extracting card type, bank ID, and last-four digits can often remain intact. In some cases, however, format-preserving Tokens may be marginally less secure than truly random Tokens, which can be arbitrarily long and complex.

For non-format-preserving Tokens, there is also the question of whether a particular Payment Card always generates the same Token across multiple transactions, or whether it generates a different Token each time. The advantage of generating the same Token is that the systems using the Token can then identify multiple transactions processed against the same Payment Card, since they can be identified by the consistent Token. This may be useful if a Hotel wants to, for example, track expenditures by a Customer that are independent of a Customer folio, but that utilize a credit card that the Customer has used before.

Benefits of Tokenization

FOR HOTELS

Tokenization greatly reduces a Hotel's security risk in the event of a data breach by removing Payment Card Data from Hotel Application Systems. The Tokens are worthless to criminals who may gain entry to a Hotel's system. Since the real Payment Card Data is stored outside of the Hotel's systems, the Hotel is spared significant financial investment required to maintain compliance with PCI's Data Security Standards.

Hospitality companies can save significant costs by reducing the number of systems that are in scope for PCI, potentially to zero. If format-preserving tokenization is used, this can be done with minimal changes to existing systems. A hospitality company may elect to provide some payment services to its Hotels (in which case some corporate systems will remain in PCI scope), or may outsource all services to third parties. Individual Hotels will benefit by being able to remove their systems entirely from PCI scope, by offloading the handling of sensitive data to third parties or corporate systems.

FOR HOTEL APPLICATION SYSTEM AND SERVICE PROVIDERS

Companies who provide software and hardware solutions or services to Hotels, and whose solutions involve Payment Card capture or processing, can also benefit from implementing the Secure Payments Framework. Examples of benefits include:

Expansion of Market

For example, a swipe device that works only with a proprietary tokenization scheme will meet only limited needs in hospitality, whereas one that can work with multiple schemes will have access to a much larger market.

Integration Cost

As standards are implemented by more and more hotels and third-party systems, the cost of custom interfaces can be dramatically reduced or even eliminated.

Reduced PCI Compliance Costs

Some software vendors may be able to entirely remove their systems from the scope of the PA-DSS, eliminating the costs for those systems of implementing and certifying to the PA-DSS standards.

New Product and Service Opportunities

The Framework provides opportunities for companies who already operate within PCI-secure environments (and who wish to continue to do so) to introduce new products and services to meet hotels' currently unmet needs. Examples include Payment Information Proxy (PIP) Services and a Secure Lookup Terminal.

FOR CUSTOMERS

Customers will benefit from the implementation of the Framework because their Payment Card Data will be more secure, and because it will be handled and stored by entities specializing in strong security.

FOR PAYMENT CAPTURE DEVICE MANUFACTURERS

Sale of devices meeting the PCI's standards will be accelerated by hotels' adoption of the Framework. Today, many hotels have little financial incentive to upgrade to new devices, because processing requirements are such that Hotel Application Systems would likely still remain in PCI scope.

FOR ONLINE TRAVEL AGENCIES AND DISTRIBUTION SERVICE PROVIDERS

While this Framework was designed to address PCI compliance issues faced by Hotels, it appears to be equally applicable to OTAs and distribution service companies, whose services become more valuable to hotels if they are transacted securely. In most cases the Framework can be used to remove OTA and distribution systems entirely from PCI scope, dramatically reducing compliance costs.

FOR PAYMENT SERVICE AND SECURITY PROVIDERS

While this Framework was designed to address PCI compliance issues faced by Hotels, it can be helpful in many other industries as well and may be used by providers to offer new solutions.

Business Scenarios

There are many different perspectives on the Payment Card security issue in hospitality. One of the barriers to communication has been the lack of understanding among many of the players of the issues and challenges facing hotels. This section provides narrative case examples to illustrate major facets of the problem. The cases are hypothetical, but are based on real situations encountered throughout the hotel industry, and illustrate the need for this Framework even when hotels use the best solutions available on the market today.

BUSINESS SCENARIO: Hotel Owner/Operator

A small family-owned roadside hotel is franchised from a major brand and managed by its owners. As part of the franchising agreement, the hotel gets a property management system (PMS) that is certified to the PCI Payment Application Data Security Standards (PA-DSS) to handle Payment Card Data securely. Nevertheless, credit card information is stolen from the PMS. The family has to pay fines, investigation costs and restitution for an amount greater than $200,000. Investigations conclude that the hotel failed to comply with remote access requirements of PCI, allowing a cybercriminal to get inside the PMS and steal credit card data.

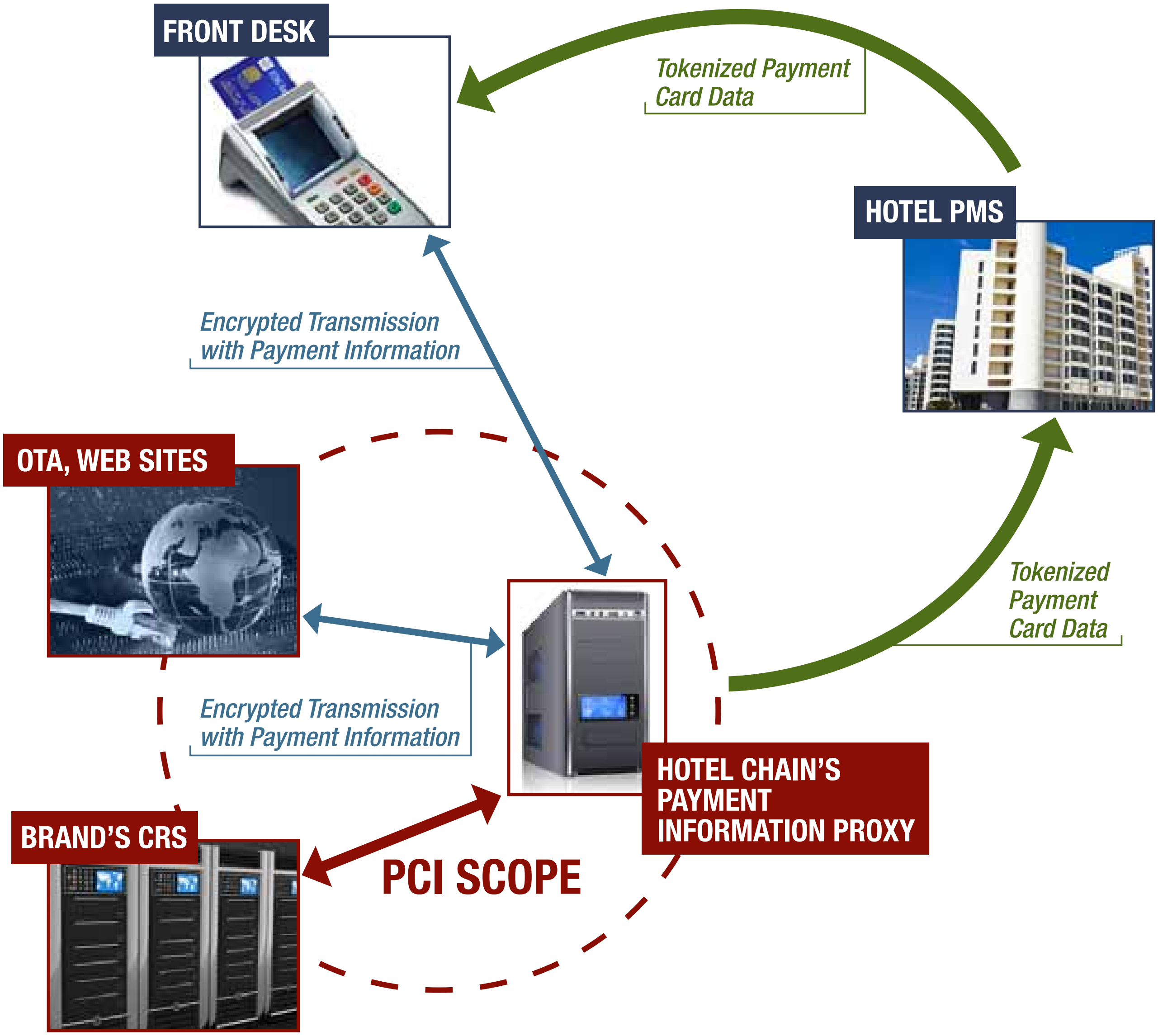
WHY EXISTING SOLUTIONS DON'T WORK:

PA-DSS certified systems handle Payment Card Data securely, but data can be extracted if the system is operated in an insecure way. Among other things, this means careful control of remote access, firewall management and monitoring, staff access credentials, physical server security, ports on network-connected devices and staff training and processes for handling of credit cards. These measures are complex and expensive. They are beyond the capabilities of most small businesses and in most cases, hotel brands are unable to help because the hotel, rather than the brand, controls the equipment, staff and network. The cybercriminal in this case took advantage of just one lapse in the hotel's management of remote access. The hotel was breached, card data was stolen and the hotel faced huge costs of the mandatory forensic investigation. The hotel may have had to notify breached customers, damaging the reputation of both the hotel and the brand.

HOW THE FRAMEWORK SOLVES THE PROBLEM:

With the proposed solution, the hotel would never have credit card data in its systems to be stolen. Transactions from credit cards swiped at the hotel using a Secure Capture Terminal do not bring the Hotel Application Systems into scope.

HOTEL OWNER/OPERATOR FRAMEWORK SOLUTION


FRONT DESK
Tokenized Payment Card Data
HOTEL PMS
Encrypted Transmission with Payment Information
OTA, WEB SITES
Tokenized Payment Card Data
Encrypted Transmission with Payment Information
HOTEL CHAIN'S PAYMENT INFORMATION PROXY
BRAND'S CRS
PCI SCOPE

BUSINESS SCENARIO:

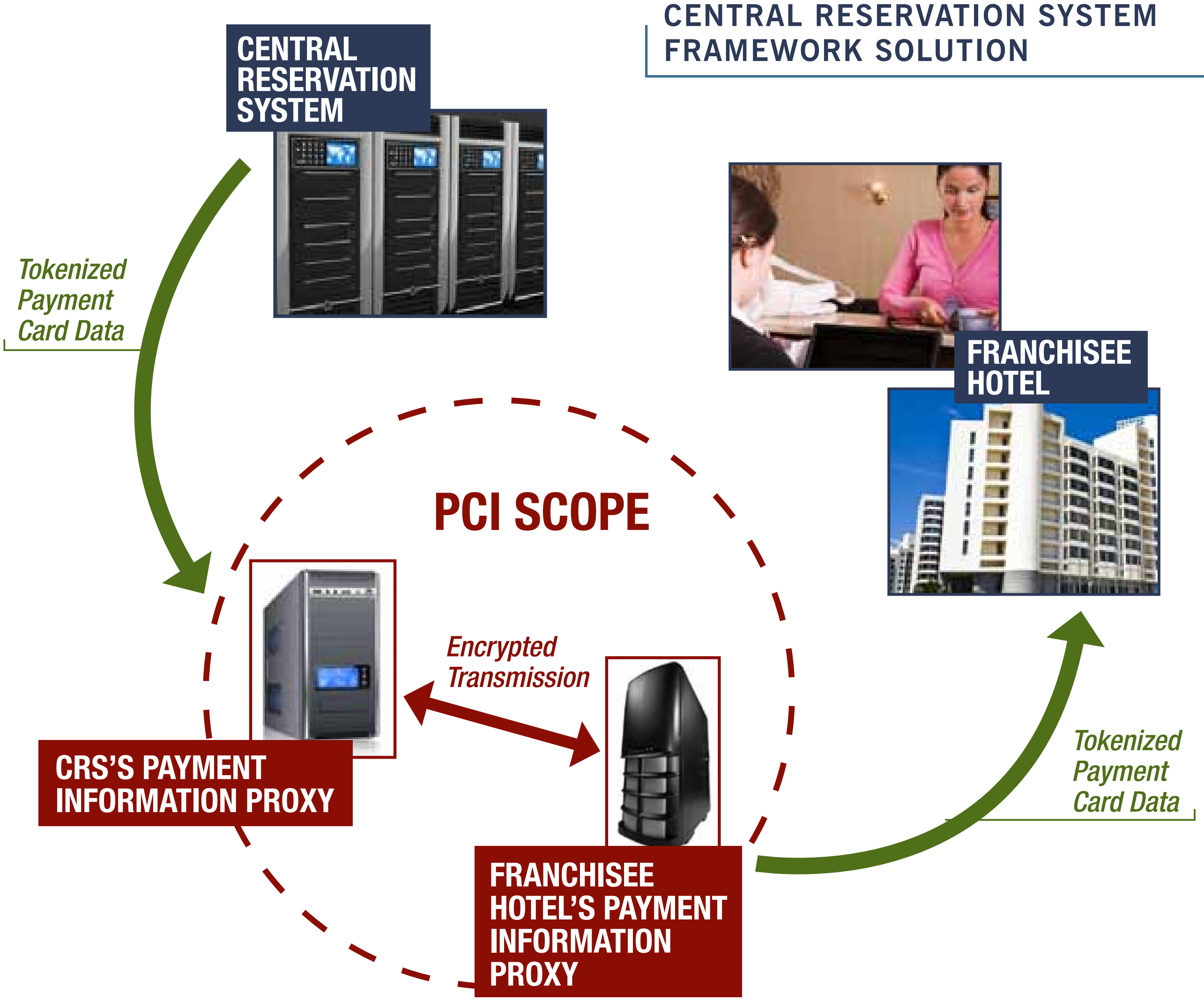
Central Reservation System

WHY EXISTING SOLUTIONS DON'T WORK:

An international hotel brand has a Central Reservation System (CRS) and Hotel Web Site, which take reservations for all the brand's hotels worldwide. Many of the hotels are franchisees, which own and operate their Property Management Systems (whether provided by the brand or acquired independently) and Payment Gateways. The Hotel Web Site and the CRS only store tokenized data.

Franchisees need to access credit card details in reservations passed down from the CRS, in order to guarantee reservations. But the Tokens used by the CRS only work with the brand's payment processing suppliers, not with the different suppliers used by the Hotel. Currently, the CRS needs to send raw payment information to the franchisee systems, bringing both systems into PCI scope.

CENTRAL RESERVATION SYSTEM FRAMEWORK SOLUTION


CENTRAL RESERVATION SYSTEM
Tokenized Payment Card Data
PCI SCOPE
Encrypted Transmission
CRS'S PAYMENT INFORMATION PROXY
FRANCHISEE HOTEL'S PAYMENT INFORMATION PROXY
FRANCHISEE HOTEL
Tokenized Payment Card Data

HOW THE FRAMEWORK SOLVES THE PROBLEM:

The CRS sends the reservation message to its own Payment Information Proxy (PIP) Service, which locates and de-tokenizes the Payment Card Data (using the CRS' Tokenization Service) and securely forwards the non-tokenized version of the message on to the Hotel's PIP Service. The Hotel's PIP then locates and re-tokenizes the Payment Card Data (using the Hotel's Tokenization Service) and forwards the (re-) tokenized message to the Hotel Application System.

Even if one of the two systems does *not* implement the Framework (and thus remains more vulnerable to a breach), the other one is protected by its PIP Service from liability in case of a breach.

A similar situation would be where a multi-brand management company needs to share Payment Card Data between two hotels that are affiliated with different brands and using those brands' tokenization schemes.

BUSINESS SCENARIO:

Global Brand

Zulu Hotels International operates 3000 hotels in 50 countries around the world. It has web sites that are tailored to 30 different language/country environments, allowing Customers from all major countries to book online. Loyalty program members store their Payment Card details in Zulu's central system (such as reservations or central Customer profile), entered through the Hotel Web Site or manually by a reservations agent. When a reservation is made, loyalty information with Payment Card is shared with the individual hotel.

Since no one Payment Gateway provider meets Zulu's needs in all of the countries in which it operates, Zulu uses multiple Payment Gateway providers to handle both prepayments made through the regionalized Hotel Web Sites, and final processing for regional hotels. Each Payment Gateway provider offers Tokenization Services, but the tokenization schemes are not compatible with each other.

WHY EXISTING SOLUTIONS DON'T WORK:

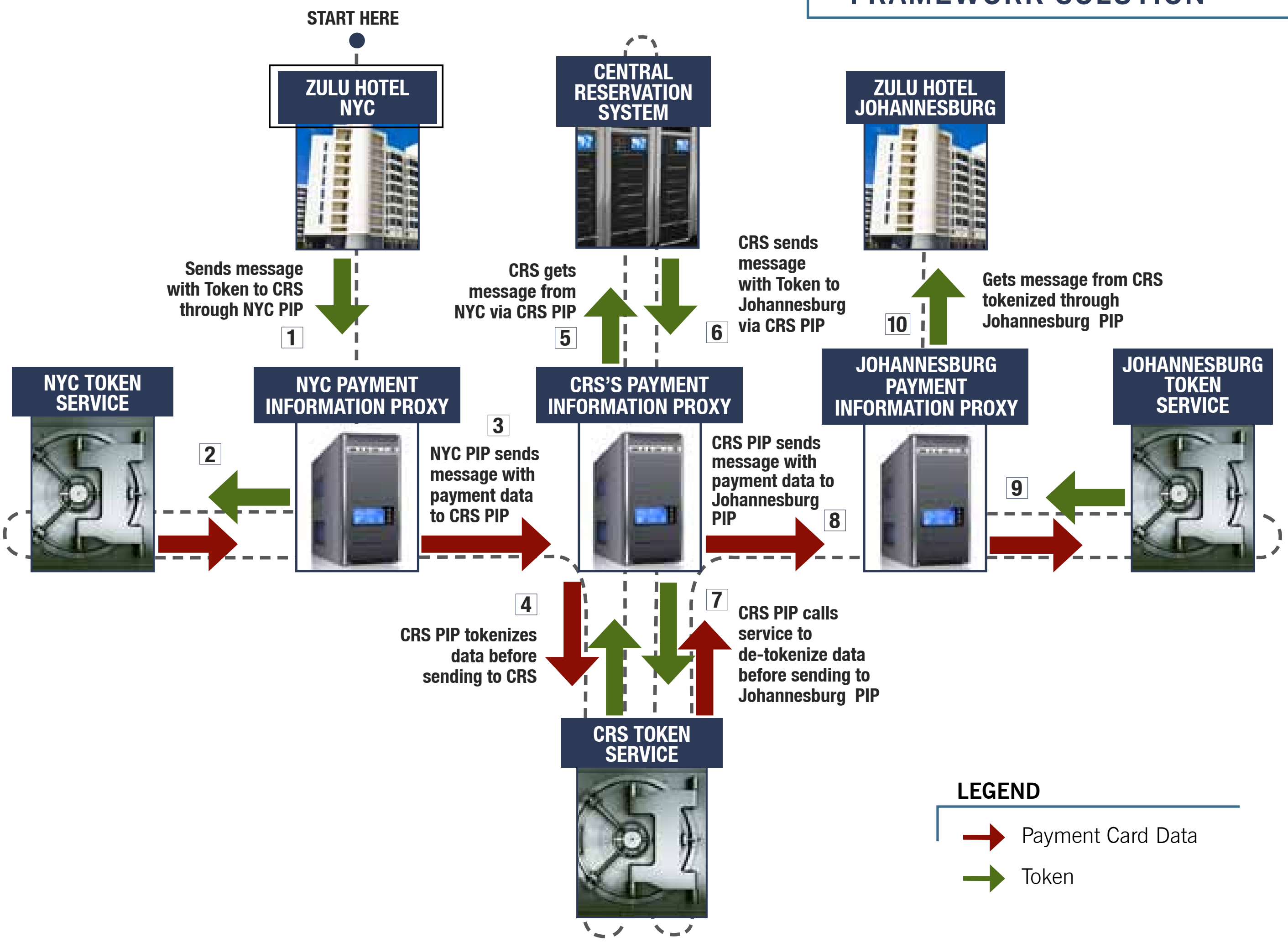
The Payment Gateways do not meet Zulu's need to exchange payment information that has been tokenized using different tokenization schemes. A Token issued by Gateway A in Africa cannot be used to process a transaction through Gateway B used by a hotel in New York. There is no option to standardize on a single tokenization approach. However, all of the brand's hotels globally need to access and use the Payment Card Data stored on the Customer profile. For example, a hotel in New York collects Customer profile information, which includes Payment Card Data that needs to be securely stored in a central profile system. A hotel in Johannesburg, South Africa needs access to this Customer profile information for a future stay.

HOW THE FRAMEWORK SOLVES THE PROBLEM:

The goal is to take tokenized payment information that originates from a system that uses one tokenization scheme and move it to a system that uses a different tokenization scheme through a central system that uses a third tokenization scheme. The hotels and the central system have each established Payment Information Proxy (PIP) and Tokenization Services, and the hotels' PIPs can communicate with the central system's PIP.

A Zulu Hotel in New York accepts a profile update from a Customer. The New York hotel tokenizes the payment information using its North American PIP and Tokenization Service. The New York hotel now needs to send the profile update to the central system. The New York hotel's PIP de-tokenizes the data and sends the transaction, now with raw Payment Card Data, to the central system's PIP. The central system's PIP receives the raw data and re-tokenizes it to be stored in the central system. Later, Johannesburg requests the profile information from the central system. The central system's PIP de-tokenizes the transaction and forwards it, now with raw Payment Card Data, securely to the Johannesburg hotel's PIP. The Johannesburg hotel's PIP tokenizes the transaction using its local Tokenization Service and forwards the tokenized data to the Johannesburg hotel's system.

GLOBAL BRAND SYSTEM FRAMEWORK SOLUTION



START HERE
ZULU HOTEL NYC
CENTRAL RESERVATION SYSTEM
ZULU HOTEL JOHANNESBURG
Sends message with Token to CRS through NYC PIP
1
CRS gets message from NYC via CRS PIP
5
6
CRS sends message with Token to Johannesburg via CRS PIP
10
Gets message from CRS tokenized through Johannesburg PIP
NYC TOKEN SERVICE
NYC PAYMENT INFORMATION PROXY
CRS'S PAYMENT INFORMATION PROXY
JOHANNESBURG PAYMENT INFORMATION PROXY
JOHANNESBURG TOKEN SERVICE
2
3
NYC PIP sends message with payment data to CRS PIP
CRS PIP sends message with payment data to Johannesburg PIP
8
9
4
CRS PIP tokenizes data before sending to CRS
7
CRS PIP calls service to de-tokenize data before sending to Johannesburg PIP
CRS TOKEN SERVICE
LEGEND
Payment Card Data
Token

BUSINESS SCENARIO:

Online Travel Agency

ABC Travel is an Online Travel Agency (OTA) specializing in custom romantic visits to the old-town areas of European cities for retired U.S. citizens. ABC combines flights, cruises, hotel, restaurants, tours and museum bookings through their online service, so the whole trip can be planned and organized before departing.

When a Customer books a hotel, ABC passes the booking to the hotel chain's CRS along with Payment Card Data in order to guarantee or prepay the reservation. The CRS passes booking information to the hotel PMS.

WHY EXISTING SOLUTIONS DON'T WORK:

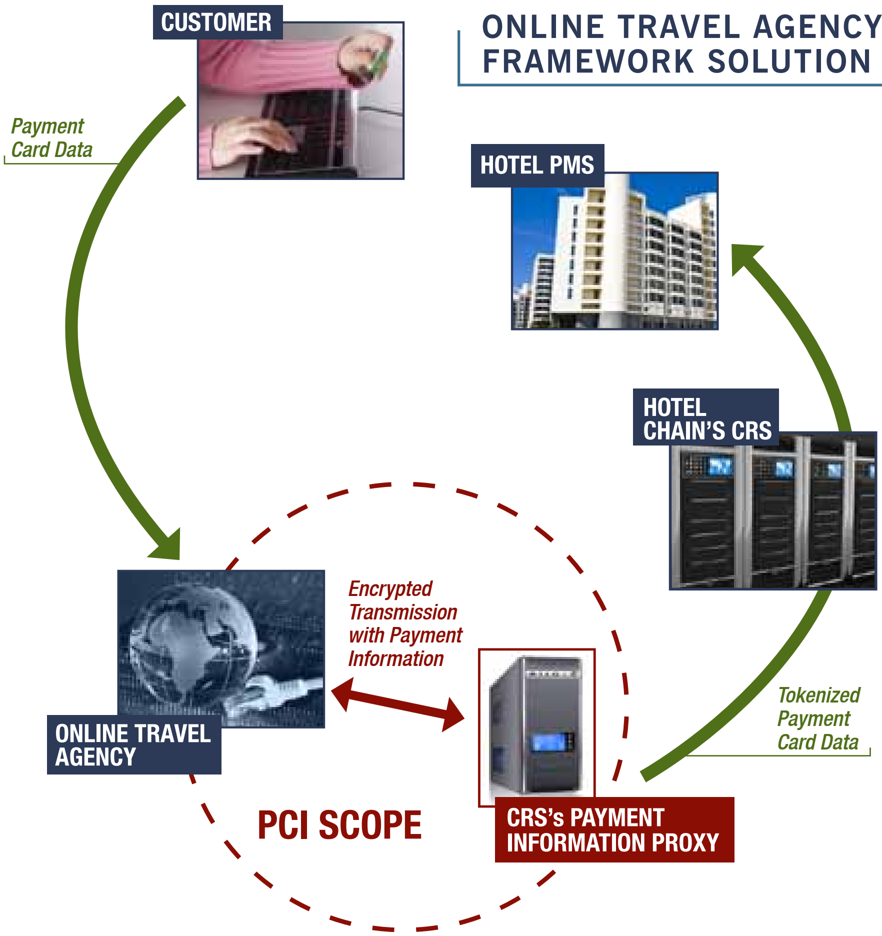
In order to guarantee or prepay hotel reservations, ABC needs to send Payment Card Data to the Hotel's CRS. But to keep the CRS out of PCI scope, the CRS cannot process, store or transmit Payment Card Data. ABC could tokenize the Payment Card Data, but then it becomes as useless to the Hotel as it does to a cybercriminal – it cannot be used for a transaction.

So ABC needs a means to securely send Payment Card Data to the Hotel, in a way that keeps the Hotel Application Systems out of scope.

HOW THE FRAMEWORK SOLVES THE PROBLEM:

When the Customer books the hotel, ABC securely sends the reservation message, including the Payment Card Data, to the Hotel's (chain) Payment Information Proxy (PIP) Service, either directly or (if it uses this Framework, through its own PIP Service). The Hotel's PIP Service facilitates tokenization of the embedded Payment Card Data using the Hotel's Tokenization Service, and sends it to the Hotel's CRS. The CRS forwards the reservation with the tokenized Payment Card Data to the Hotel's PMS. If the CRS uses a different Tokenization Service than the PMS, then this message is also de-tokenized and re-tokenized by their respective PIPs. In each case, the Hotel's CRS and PMS can remain out of PCI scope.

ONLINE TRAVEL AGENCY FRAMEWORK SOLUTION


CUSTOMER
Payment Card Data
HOTEL PMS
HOTEL CHAIN'S CRS
Encrypted Transmission with Payment Information
Tokenized Payment Card Data
ONLINE TRAVEL AGENCY
PCI SCOPE
CRS's PAYMENT INFORMATION PROXY

Messaging Standards

Since HTNG's inception, its workgroups have produced a significant number of specifications to enhance the exchange of information between systems used in the hospitality industry. Four efforts have produced materials that directly benefit the industry relating to the secure handling of credit cards, and many of them directly support aspects of the Secure Payments Framework.

PAYMENT PROCESSING

Authorization, settlement, void, reversal, etc. using Tokens: the HTNG Payment Systems & Data Security - Payment Processing Specification 2.0 handles all basic lodging transactions.

Click to Read this Specification >

EXCHANGING PAYMENT CARD DATA FOR TOKENS:

The HTNG Payment Systems & Data Security - Data Proxy Specification 1.1 supports the creation, management and use of Tokens through a Tokenization Service that is independent of the Hotel Application Systems. In the Secure Payments Framework, Hotels will not need this information because they will never touch Payment Card Data, but their service providers may find the messages useful. In addition, Hotels may find them useful during a transitional period.

Click to Read this Specification >

Links to all specifications are at www.htng.org/secure-payments-framework

HOSTED PAYMENT COLLECTOR:

The HTNG Hosted Payment Capture Systems Specification 1.0 provides the means to collect payment information from a Customer on a hosted system. This messaging specification enables products to deliver secure, hosted solutions for the capture and processing of Payment Card Data, without exposing the underlying Hotel Application Systems to PCI scope. It can be used on Hotel Web Sites, in the Central Reservation Systems, or in a contact center's Interactive Voice Response (IVR) System.

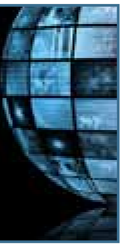
Click to Read this Specification >

WEB SERVICES FRAMEWORK (WSF):

HTNG's library of web services is most easily implemented using a common framework for message routing, reliability, security, error handling and other services not related to the message payload. The HTNG Property Web Services Specifications – Web Services Framework 2.1.1 (Part 1) provides this "plumbing" layer for connectivity. The SOAP-based WSF enables two systems to reliably exchange any XML messages (HTNG or proprietary), vastly simplifying the implementation of interfaces. The latest version also supports event subscription and notification across systems.

Click to Read this Specification >

In addition to the HTNG standards, the OpenTravel Alliance, which publishes some of the schemas on which HTNG's standards are based, already includes a data field for a masked version of the Payment Card number. Thus, a system receiving a proxy will still have access to key portions of the card number (e.g. first six digits, last four digits) that may be needed for various analytical or identifying purposes. With some tokenization schemes, these portions of the card number may be preserved, but even for those where they are not, the information can be made readily available.



Framework Assumptions and Risks

Hotel security experts who participated in the development of this Framework believe that it forms a solid underpinning for a hotel security strategy around Payment Card Data. Nevertheless, the world changes quickly, and a review of the assumptions and risks is in order.

Assumptions

1. This solution is based on today's PCI standards. While there is no current indication that it will not continue to work under future standards as well, there are certainly changes that *could* be introduced to the PCI standards that would bring elements of Hotel Application Systems back into the scope of PCI.

2. The solution assumes availability of a tamper-resistant Secure Payment Terminal that encrypts the data, and for which the Hotel has no access to the decryption key. It also assumed that the selected device has been assessed by the Hotel's Qualified Security Assessor (QSA) as sufficient for the purpose, to take the Hotel network and systems out of scope with respect to the swipe transaction. While commercially available solutions meet this need, QSAs have interpreted the PCI requirements differently, and different QSAs have been known to disagree as to whether and when specific products meet the requirements.

3. Actors identified in the Framework are not necessarily distinct companies, products or services. For example, a company that offers a Payment Gateway service may also offer a Tokenization Service. We make no assumption that any component of the Framework should be provided by any particular company or type of company. Furthermore, a Hotel brand may choose to host and offer any component service itself. In doing so, it may expose those systems and services to PCI requirements, but may still reduce risk by isolating Payment Card Data in a smaller number of systems.

4. All data is exchanged through a secure transport layer.

5. The use cases do not consider all irregularities that may arise in normal credit card processing. However, obvious principles of the Framework will normally still apply.

6. All existing interfaces through which Payment Card Data is passed are modified to support the passing of Tokenized Payment Method Records (or format-preserving Tokens) and/or a flag indicating that the data is tokenized.

7. At the time of this writing, the Framework workgroup was aware of activity by the card brands around validation levels and the EMV. It was the consensus of the workgroup that those activities do not materially affect the design of this Framework.

Risks

1. Possible changes related to EMV, Point-to-Point Encryption, tokenization, device requirements and validation for merchants who currently implement and/or have implemented these technologies.

2. There was also some discussion about whether all QSAs would consider this solution sufficient to remove Hotel Applications Systems from PCI scope. There was, however, a consensus among participants that they believed that at least their own QSAs were aligned with the broad approach, with areas of disagreement centering around the appropriateness of particular technical approaches selected by individual vendors, rather than with the principles of the Framework.

Conclusion and Call to Action

The HTNG Secure Payments Framework provides a solution to the unique data security issues confronting the hotel industry and provides many benefits to hotel owners, operators and brands.

Embracing the HTNG Secure Payments Framework as the industry standard best practice lowers costs for hotels, discourages cyber theft from hotel systems and enhances payment data security throughout the hospitality industry.

What this means to you as a reader is simple, but varies depending on your industry role:

INDEPENDENT HOTELS

If you implement this Framework entirely, you may be able to buy or maintain applications at a lower cost, because they do not have to certify compliance to the PCI's Payment Application Data Security Standards (PA-DSS). Send this document to your major system providers (PMS, CRS, POS) and to your Payment Gateway service provider, and tell them it outlines the solution you need them to embrace. Send it to any Online Travel Agencies with whom you transact significant business. The more hotels who ask for this approach, the more likely the various parties will adopt it.

FRANCHISED HOTELS

If you implement this Framework entirely, you may be able to buy or maintain applications at a lower cost, because they do not have to certify compliance to the PCI's PA-DSS. Send this document to your brand (if they haven't already endorsed it), to your major system providers (PMS, CRS, POS) and to your Payment Gateway service provider. Tell them it outlines the solution you need them to embrace. Send it to any Online Travel Agencies with whom you transact significant business. The more hotels who ask for this approach, the more likely the various parties will adopt it.

HOTEL MANAGEMENT COMPANIES

If you implement this Framework entirely, you may be able to buy or maintain applications at a lower cost, because they do not have to certify compliance to the PCI's PA-DSS. Send this document to your brands (if they haven't already endorsed it), to your major system providers (PMS, CRS, POS) and to your Payment Gateway service providers. Tell them it outlines the solution you need them to embrace. Send it to any Online Travel Agencies with whom you transact significant business. The more hotels who ask for this approach, the more likely the various parties will adopt it. Consider having these communications sent under the signature of a senior company officer.

NATIONAL AND GLOBAL BRANDS

If you implement this Framework entirely, you may be able to buy or maintain applications at a lower cost, because they do not have to certify compliance to the PCI's PA-DSS. Even if you have already implemented tokenization, you will find new opportunities in the Framework to address some remaining gaps, and the Framework will build on, not replace what you have already done. You can recognize much greater benefits from your existing investment if all your trading partners implement a complementary approach, as outlined by the Framework. Send this document to your major system providers (PMS, CRS, POS), and to your Payment Gateway service providers. Tell them it outlines the solution you need them to embrace. Send it to any Online Travel Agencies with whom you transact significant business. Send it to any franchised hotels who have systems in scope for PCI. The more hotels who ask for this approach, the more likely the various parties will adopt it. Consider having these communications sent under the signature of a senior company officer.

SECURE PAYMENT TERMINAL PROVIDERS:

You can make your product more attractive to hotels. Ensure that it meets the requirements of the PCI standards and interpretations of QSAs, to enable the capture and transmission of Payment Card Data without exposing the hotel's network or application systems to PCI scope. If you also tokenize Payment Card Data, make sure that the Tokenization Service performs the roles outlined in the Framework, and can do so through open standards with authorized third parties, as this is essential to meeting many needs of hotels. Send this document to your customers and prospects and tell them that you support this industry effort, and how your product offering fits.

KIOSK MANUFACTURERS:

You can make your product more attractive to hotels. Kiosk manufacturers can adhere to the Framework, although most kiosks today do not do so, and therefore are in PCI scope. Ensure that your kiosk meets the requirements of the PCI standards and interpretations of QSAs, and encompasses the concepts of a Secure Payment Terminal to enable the capture and transmission of Payment Card Data without exposing the hotel's network or application systems to PCI scope. If you use a Secure Payment Terminal produced by another provider, send this document to them and tell them it outlines the solution you want them to embrace.

INTERACTIVE VOICE RESPONSE (IVR) SYSTEM MANUFACTURERS:

You can solve a major problem for hotels by eliminating the exposure of telephone contact centers to Payment Card Data, both in their systems and in their call recordings. Ensure that your product allows the capture of Payment Card Data by a contact-center system (such as a Central Reservation System) without exposing that system or the agent to the card data in any form (digital, audio, etc.). Validate your system to the PCI standards, and implement tokenization by establishing standards-based or proprietary interfaces with Tokenization Services used by your customer Hotels. Send this document to your customers and prospects and tell them that you support this industry effort, and how your product offering fits.

PROPERTY MANAGEMENT SYSTEM (PMS) MANUFACTURERS:

You can make your system more valuable to hotels by reducing their PCI compliance costs dramatically. Establish interfaces with Secure Payment Terminal products to initiate the capture of Payment Card Data, with return messages coming from a Hotel's Tokenization Service in Token format. Modify your existing system and/or design new systems to work with Tokens, and document any limitations on Token formats – the fewer the limitations, the better, but legacy systems may be able to support only one or a few options without extensive customization. Use open standards particularly for Token creation and lookup, so that your product works with the widest possible choice of Payment Gateways and Tokenization Services. Send this document to your customers and prospects and tell them that you support this industry effort, and how your product offering fits.

CENTRAL RESERVATION SYSTEM (CRS) MANUFACTURERS AND SERVICE PROVIDERS:

Reduce compliance costs for yourself and for on-premise licensees by getting your system out of the scope of PCI compliance. Select and implement a Tokenization Service and Payment Information Proxy (PIP) Service, to intercept and tokenize inbound reservations that include Payment Card Data, before they enter your system. Implement Hosted Payment Collector interfaces (web or IVR based) if needed to eliminate exposure of your system to Payment Card Data from agents in call centers. Modify your existing system and/or design new systems to work with Tokens, and document any limitations on Token formats – the fewer the limitations, the better, but legacy systems may be able to support only one or a few options without extensive customization. Use open standards particularly for Token creation and lookup, so that your product works with the widest possible choice of Payment Gateways and Tokenization Services. Send this document to your customers and prospects and tell them that you support this industry effort, and how your product offering fits.

POINT-OF-SALE (POS) SYSTEM MANUFACTURERS:

You can make your system more valuable to hotels by reducing their PCI compliance costs dramatically. Establish interfaces with Secure Payment Terminal products to initiate the capture of Payment Card Data, with return messages coming from a hotel's Tokenization Service in Token format. Modify your existing system and/or design new systems to work with Tokens, and document any limitations on Token formats – the fewer the limitations, the better, but legacy systems may be able to support only one or a few options without extensive customization. Use open standards particularly for Token creation and lookup, so that your product works with the widest possible choice of Payment Gateways and Tokenization Services. Send this document to your customers and prospects and tell them that you support this industry effort, and how your product offering fits.

ACTIVITY SYSTEM MANUFACTURERS:

You can make your system more valuable to hotels by reducing their PCI compliance costs dramatically. Establish interfaces with Secure Payment Terminal products to initiate the capture of Payment Card Data, with return messages coming from a hotel's Tokenization Service in Token format. Modify your existing system and/ or design new systems to work with Tokens, and document any limitations on Token formats – the fewer the limitations, the better, but legacy systems may be able to support only one or a few options without extensive customization. Use open standards particularly for Token creation and lookup, so that your product works with the widest possible choice of Payment Gateways and Tokenization Services. Send this document to your customers and prospects and tell them that you support this industry effort, and how your product offering fits.

PAYMENT GATEWAY PROVIDERS:

You can expand your range of products and services to fill unmet needs of hotels, which will have high value because they hold the promise of eliminating Hotel Application Systems from the scope of PCI. If you have not already done so, offer a Tokenization Service. Consider adding the services outlined for a PIP Service, to receive transactional messages in various forms, cleanse them of Payment Card Data, and forward them onward. Use open standards particularly for Token creation and lookup, so that your product works with the widest possible choice of Hotel Application Systems. Send this document to your customers, prospects and partners, and tell them that you support this industry effort, and how your product offering fits.

ONLINE TRAVEL AGENCIES AND DISTRIBUTION INTERMEDIARIES

Reduce compliance costs for yourself and for on-premise licensees by getting your system out of the scope of PCI compliance. Become more attractive to hotels by eliminating the delivery of reservations with insecure Payment Card Data, which create cost and risk for hotels. Implement a Tokenization Service and Payment Information Proxy Service, to intercept and tokenize inbound reservations that include Payment Card Data, before they enter your system. Implement Hosted Payment Collector interfaces (web or IVR based) if needed to eliminate exposure of your system to Payment Card Data from agents in call centers. Modify your existing system and/ or design new systems to work with Tokens, and document any limitations on Token formats – the fewer the limitations, the better, but legacy systems may be able to support only one or a few options without extensive customization. Send this document to your hotels and tell them that you support this industry effort, and how your product offering fits.

Appendix

Terminology Cross Reference

There are multiple roles and terms defined by this Framework, and in some cases the nomenclature differs from prior HTNG Payment specifications. Below is a mapping of the many actors, roles, and definitions that overlap.

SECURE PAYMENTS FRAMEWORK		**PAYMENTS SYSTEMS & DATA SECURITY SPECIFICATION**	**HOSTED PAYMENT CAPTURE SYSTEMS SPECIFICATION**
ACTOR	**Customer**	**Guest** Definition	**Customer** Term
ACTOR	**Hotel Staff**	Front Desk, Waiter, Cashier	
ACTOR	**Hosted Payment Collector System**		**Hosted Payment (Capture) System** Role
ACTOR	**Hotel**	**Merchant, Service Establishment** Definition	
ACTOR	**Hotel Systems**	**Business Logic System** Role	
ACTOR	**Payment Service**	**Payment Processing System** Role	
ACTOR	**Secure Payment Terminal**	**PED** Definition	
ACTOR	**Tokenization Service**	**Payment Gateway** Definition	
DEFINITION	**Hotel Web Site**		**Hotel Web Site** Role
DEFINITION	**Payment Card**	**Card**	
DEFINITION	**Payment Card Data**	**Cardholder Data** Definition	

Actors

Actors fulfill roles participating in the business functions of an organization. Actors may be human or a system and may initiate an action or participate in a business process. Human roles are played by people. A single person may be the actor in several different roles.

- **Customer:** someone who is purchasing product(s) and/or service(s) from a Hotel. May also include an agent acting on the Customer's behalf.
- **Hosted Payment Collector:** a system, typically hosted by the Tokenization Service, designed to collect Payment Card Data without going through any Hotel Application System.
- **Hotel:** an individual property, or an enterprise that owns, manages or franchises one or more properties.
- **Hotel Application Systems:** Hotel Systems (see below) that process hotel transactions, rather than systems that are specifically part of the payment process. The Framework is designed to remove these application systems from PCI scope.
- **Hotel Staff:** a staff member employed by the Hotel or the Hotel's agent, who interacts with the Customer in the context of a Payment Card transaction; the person that enters the reservation and payment data into the system on behalf of the Hotel.
- **Hotel System:** any system within the Hotel that deals with Payment Card processing, storage or transmission in any form, whether encrypted, tokenized or otherwise. Examples include Secure Payment Terminals, PMS, POS, Spa, Sales & Catering, CRES, Hotel Web Site and IVR Systems.
- **Interactive Voice Response (IVR) System:** a module, typically part of a telephone system, that allows a caller to enter information, via keypad or voice commands.
- **Meeting Planner:** a person or company that is making reservations on behalf of a group of individuals.
- **Payment Capture System:** any system that captures or collects Payment Card Data, including but not limited to Secure Payment Terminals and Hosted Payment Capture Systems.
- **Payment Information Proxy (PIP) Service:** extracts, then swaps Payment Card and/or Token data from a message, then routes and sends the modified message forward to its destination.
- **Payment Service:** a party that can authorize and settle Payment Card transactions.
- **Secure Payment Terminal:** a PCI/PTS/P2PE-approved device that allows Payment Card Data to be collected while keeping the Hotel Application System out of PCI scope. Depending on the particular application, may support one or more of card swipe, keypad or other methods of entry.
- **Secure Lookup Terminal** – a device designed to enable designated Hotel Staff access to actual cardholder data without requiring the Hotel Staff to have access to encryption keys or tokenization and de-tokenization processes. This device, provided to the Hotel by a service provider, needs to be implemented using a PCI/PTS/P2PE-approved method or otherwise properly segmented from Hotel Application Systems. Hotel Staff using the Secure Lookup Terminal fall within PCI-DSS scope. See the Securely Accessing Raw Payment Card Data use case below.
- **Tokenization Service:** A party that can accept and securely store Payment Card Data and return a tokenized representation of that data, and return the Payment Card Data when presented with the Token.

Definitions

- **Hotel Web Site:** The web presence for the Hotel that can be used to make reservations and/or to create and update Customer profile information.
- **Payment Card:** Any physical credit or debit card, or electronic representation thereof, that is processed through the electronic payment industry network.
- **Payment Card Data**: The information on a Payment Card that is required for the processing of a transaction.
- **Payment Gateway:** A service that may offer one or more payment-related services to Hotels, typically including translation of payment transactions from Hotel Systems to acquiring bankcard processors. Payment Gateways may also provide Tokenization Services and Payment Information Proxy (PIP) Services, and may offer other services as well.
- **Secure Data Repository:** Acts as an information vault that securely stores, for later retrieval, Payment Card Data that has been received via fax, e-mail, upload of spreadsheets, or similar means. This service might be provided by the Tokenization Service providers.
- **Token:** In common vernacular, "Token" refers to the substitute data that replaces the Payment Card account number (PAN); in this framework, it refers to a structured data record (Tokenized Payment Method Record) that includes the substitute data and also certain other contextual information.
- **Tokenized Payment Method Record:** a Token issued by a Tokenization Service, representing specific Payment Card Data, together with ancillary information such as the Payment Card issuer, card type and permissible portions of Payment Card Data (e.g. first six, last four digits).

Abbreviations and Acronyms

CRS	Central Reservation System
EMV	Europay, MasterCard and Visa
HPCS	Hosted Payment Collector Service
IVR	Interactive Voice Response
NFC	Near Field Communication
OTA	Online Travel Agency
PAN	Payment Card Account Number
PA-DSS	Payment Application Data Security Standard
PCI-DSS	Payment Card Industry Data Security Standard
PCI	Payment Card Industry
P2PE	Point-to-Point Encryption
PMS	Property Management System
POS	Point of Sale
PTS	PIC Transaction Security
PIP	Payment Information Proxy
QSA	Qualified Security Assessor
SOAP	Simple Object Access Protocol
XML	Extensible Markup Language
WSF	Web Services Framework

Use Cases and Sequence Diagrams

A complete list of use cases, and the intended processing methodologies for each, follows. To assist the reader, Figure A depicts all of the actors relevant to the Framework in a single diagram. The detailed use cases then refer to the numbered boxes on the diagram.

🟥 Red boxes indicate systems within PCI scope, which would typically be operated by a service provider (e.g. gateway) or by a Hotel brand that wishes to stage its own secure environment.

🟩 The green box in the upper left encompasses Hotel Application Systems that can be operated outside of PCI scope, plus Secure Payment Terminals which, while within PCI scope, do not expose the Hotel Application Systems to PCI scope.

🟥 Third-party partners (box #5) may utilize the framework in the same manner as Hotels, or may remain within scope (hence they are shown with a dotted red border).

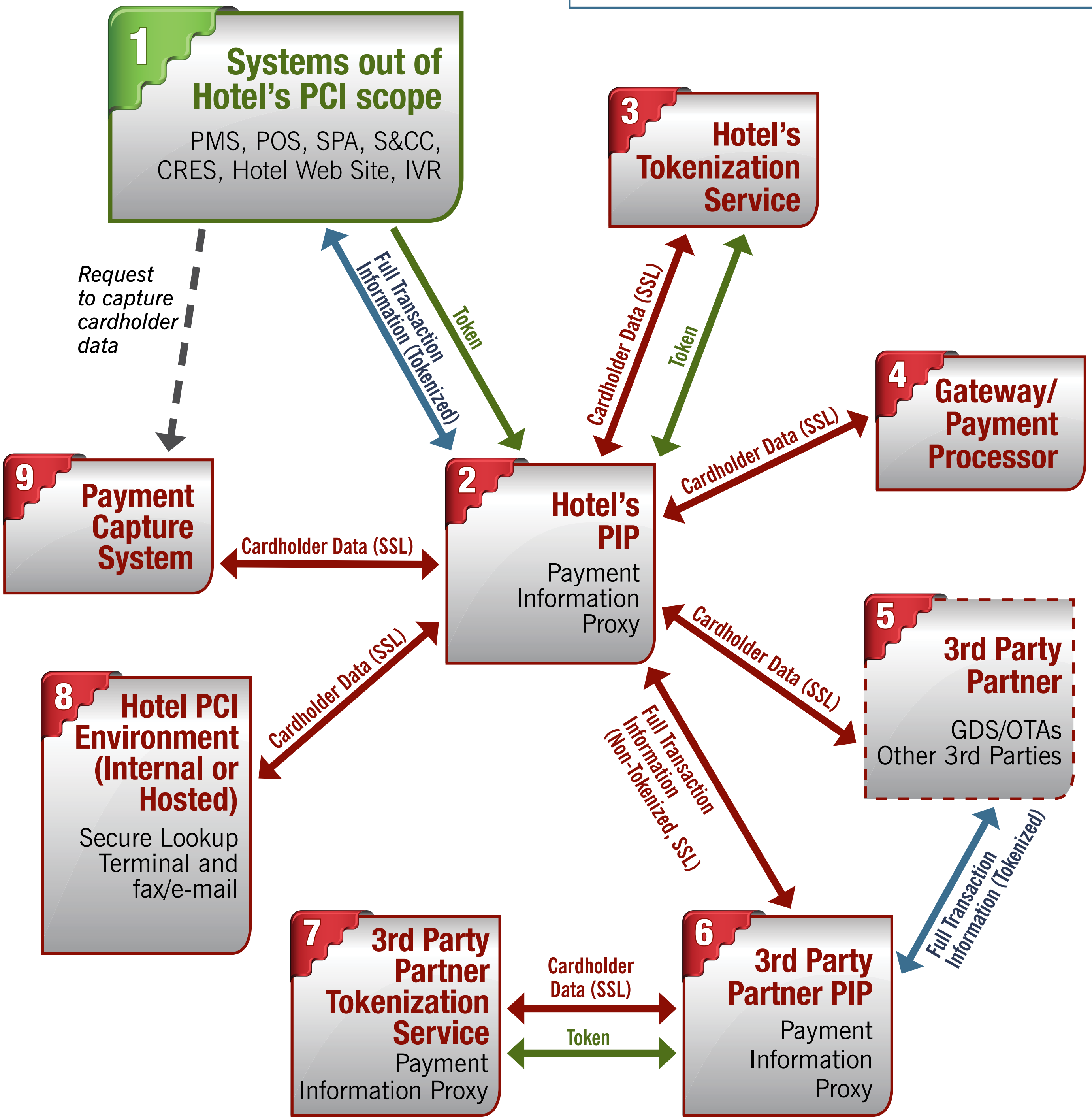
In the real world, a single service provider or Hotel brand may combine several of the actors into a single service (for example, actors #2, 3, 4, 8 and 9, or any subset, could be offered as a single service). In this case, the flow of information between actors may occur internally within a single system or ecosystem of cooperating systems, and need not exactly follow this diagram.

While Figure A captures what may be the most common implementation of the framework, it should be noted that variations exist that are equally valid. One common variation would be that Hotel Systems (actor #1) could communicate directly with the Tokenization Service (actor #3), rather than routing messages through the Payment Information Proxy (PIP) Service. This could make sense, for example, if the Hotel used different providers for tokenization vs. its PIP, and wished to avoid transaction costs that might be assessed by the PIP for performing what is essentially just a routing function.

HTNG standard messages are referenced throughout this section.

Links to all specifications are at www.htng.org/secure-payments-framework

FIGURE A
SEQUENCE DIAGRAM


1
Systems out of Hotel's PCI scope
PMS, POS, SPA, S&CC, CRES, Hotel Web Site, IVR
3
Hotel's Tokenization Service
Request to capture cardholder data
Full Transaction Information (Tokenized)
Token
Cardholder Data (SSL)
Token
4
Gateway/ Payment Processor
Cardholder Data (SSL)
9
Payment Capture System
Cardholder Data (SSL)
2
Hotel's PIP
Payment Information Proxy
Cardholder Data (SSL)
5
3rd Party Partner
GDS/OTAs
Other 3rd Parties
8
Hotel PCI Environment (Internal or Hosted)
Secure Lookup Terminal and fax/e-mail
Cardholder Data (SSL)
Full Transaction Information (Non-Tokenized, SSL)
Full Transaction Information (Tokenized)
7
3rd Party Partner Tokenization Service
Payment Information Proxy
Cardholder Data (SSL)
Token
6
3rd Party Partner PIP
Payment Information Proxy

LEGEND

→ Red arrows indicate the flow of (raw) Payment Card Data, typically over a secure connection.

→ Green arrows indicate the flow of tokenized Payment Card Data.

→ Blue arrows indicate transactional messages (e.g. reservations) that include tokenized Payment Card Data.

USE CASE:

Collecting Payment Card Data

Customer, or Hotel Staff acting on behalf of Customer, enters Payment Card Data for use by Hotel Application Systems. For example, this typically occurs when a Customer checks in, pays their bill, guarantees a future reservation or updates Payment Card Data in their profile. This may occur either by physical swipe or manual entry.

One way to keep Hotel Staff and call recording systems out of PCI scope would be to direct callers to an IVR System (see "Collecting Payment Data Over Voice Channels" use case below).

Another way to keep hotel contact-center staff and Hotel Systems out of PCI scope would be to direct Customers using a web browser to a Hosted Payment Collector System (see "Collecting Payment Data through the Web" use case below).

Remember: Usable card data may never touch the Hotel Application Systems – it must be protected, even at the point of swipe.

ACTORS AND PARTICIPANTS

- 1 Hotel Systems
- 3 Hotel Tokenization Service
- 9 Payment Capture System
- 2 Hotel PIP
- 4 Gateway/ Payment Processor
- Customer
- Hotel Staff

Preconditions and Assumptions

Customer wishes to use a Payment Card for which no corresponding Tokenized Payment Method Record is on file in the Hotel Application System.

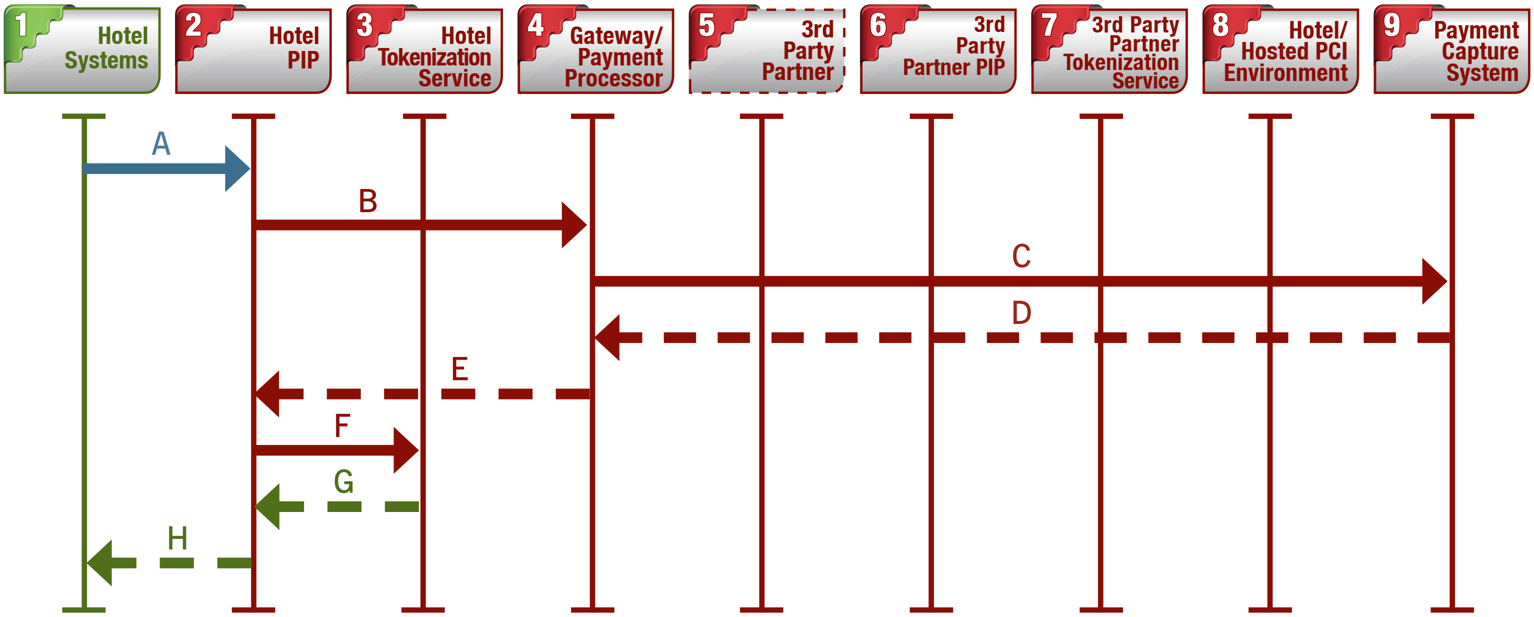
Process

A	Hotel System sends a request to the PIP to collect Payment Card Data from a specific Secure Payment Terminal	1 Hotel Systems	to	2 Hotel PIP
B	PIP sends a request to the Gateway/Payment Processor to collect Payment Card Data from the Secure Payment Terminal	2 Hotel PIP	to	4 Gateway/ Payment Processor
C	Gateway/Payment Processor sends a request to Secure Payment Terminal to collect Payment Card Data	4 Gateway/ Payment Processor	to	9 Payment Capture System
D	After the Customer or Hotel Staff member enters the Payment Card Data into the Secure Payment Terminal, the captured Payment Card Data is sent to the Gateway/Payment Processor	9 Payment Capture System	to	4 Gateway/ Payment Processor
E	The Gateway/Payment Processor sends the Payment Card Data to the Hotel PIP	4 Gateway/ Payment Processor	to	2 Hotel PIP
F	Hotel PIP sends Payment Card Data to Hotel's Tokenization Service	2 Hotel PIP	to	3 Hotel Tokenization Service
G	Hotel's Tokenization Service sends Tokenized Payment Method Record to Hotel PIP	3 Hotel Tokenization Service	to	2 Hotel PIP
H	The Hotel PIP sends the Tokenized Payment Method Record to the Hotel System	2 Hotel PIP	to	1 Hotel Systems

Postconditions

The Hotel Application System has a Token that can be used in place of a Payment Card (which would have brought the Hotel Application System into PCI scope).

COLLECTING PAYMENT CARD DATA MESSAGE FLOW DIAGRAM


1 Hotel Systems
2 Hotel PIP
3 Hotel Tokenization Service
4 Gateway/ Payment Processor
5 3rd Party Partner
6 3rd Party Partner PIP
7 3rd Party Partner Tokenization Service
8 Hotel/ Hosted PCI Environment
9 Payment Capture System
A
B
C
D
E
F
G
H

LEGEND

- → Red arrows indicate the flow of transactional message containing Payment Card Data, typically over a secure connection.
- → Green arrows indicate the flow of transactional message containing tokenized Payment Card Data.
- → Blue arrows indicate transactional messages that do not contain Payment Card Data.
- — Solid line represents a request
- - - Dotted line represents a response

RELEVANT HTNG MESSAGES

A-E)	Not yet defined*
F)	HTNG_PaymentCardProxyRQ
G)	HTNG_PaymentCardProxyRS
H)	Not yet defined*

*May be addressed by future HTNG efforts

USE CASE:

Settling and Reversing Transactions

A Hotel has a Token stored in its PMS and needs to settle or reverse a transaction to the associated Payment Card. The Token needs to be turned into Payment Card Data in order to process the transaction. The Hotel Application Systems, PIP and Tokenization Services all interact to provide the Payment Card Data to the Payment Gateway without the Hotel System ever needing to touch the Payment Card Data.

ACTORS AND PARTICIPANTS

1 Hotel Systems

2 Hotel PIP

3 Hotel Tokenization Service

4 Gateway/ Payment Processor

Preconditions and Assumptions

Tokenized Payment Method Record is stored in Hotel Application System.

Process

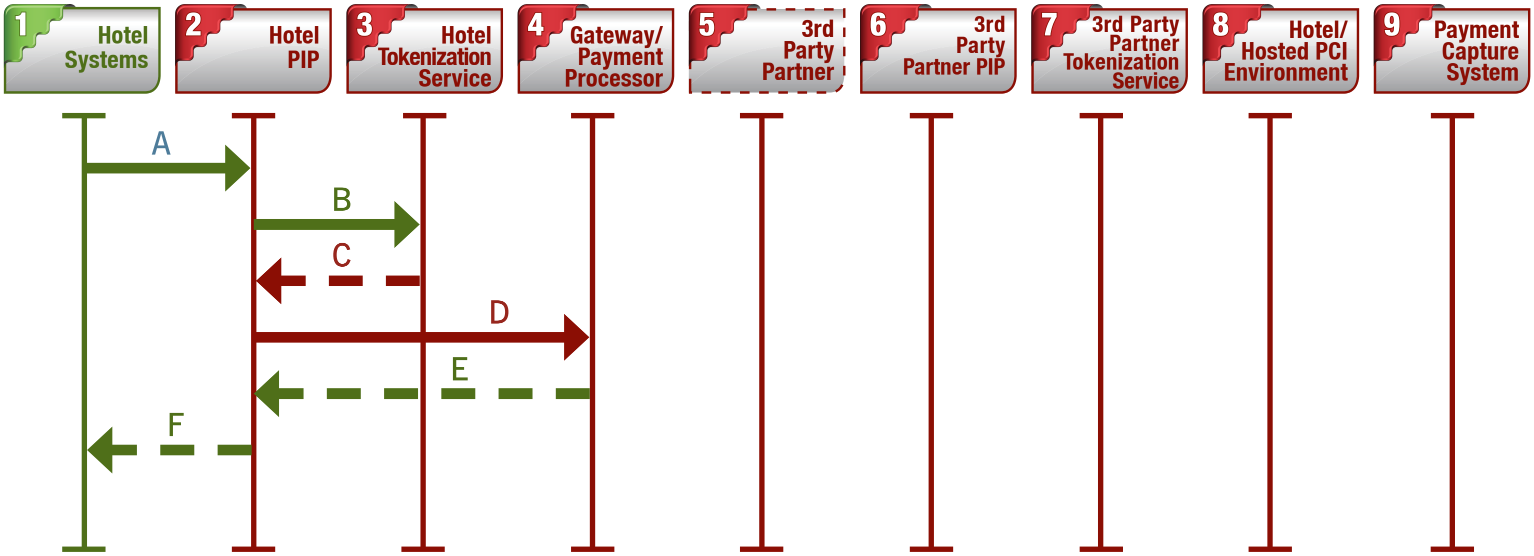
A	Hotel Application System sends Tokenized Payment Method Record to the PIP	1 Hotel Systems	to	2 Hotel PIP
B	PIP sends Tokenized Payment Method Record to Hotel's Tokenization Service	2 Hotel PIP	to	3 Hotel Tokenization Service
C	Tokenization Service de-tokenizes and returns Payment Card Data to PIP	3 Hotel Tokenization Service	to	2 Hotel PIP

D	PIP securely sends Payment Card Data to Payment Service/Gateway to process payment	2 Hotel PIP	to	4 Gateway/ Payment Processor
E	Payment Service/Gateway returns transaction result to PIP	4 Gateway/ Payment Processor	to	2 Hotel PIP
F	PIP returns transaction result to Hotel Application System	2 Hotel PIP	to	1 Hotel Systems

Postconditions

The Hotel will have the funds in process.

SETTLING AND REVERSING TRANSACTIONS MESSAGE FLOW DIAGRAM



1 Hotel Systems
2 Hotel PIP
3 Hotel Tokenization Service
4 Gateway/ Payment Processor
5 3rd Party Partner
6 3rd Party Partner PIP
7 3rd Party Partner Tokenization Service
8 Hotel/ Hosted PCI Environment
9 Payment Capture System
A
B
C
D
E
F

RELEVANT HTNG MESSAGES

A) HTNG_PaymentCardProcessingRQ
B) HTNG_PaymentCardRQ
C) HTNG_PaymentCardRS
D) HTNG_PaymentCardProcessingRQ
E) HTNG_PaymentCardProcessingRS
F) HTNG_PaymentCardProcessingRS

USE CASE:

Securely Accessing Raw Payment Card Data

There are various situations where a Hotel may need to retrieve the full Payment Card Data from a Token, for example to research a dispute, to process an offline card-not-present transaction or for a concierge to guarantee theater tickets on a Customer's behalf, using the card they presented at check-in. In each case, the assumption is that a Secure Lookup Terminal is used to input a Token and display the underlying card data.

The Secure Lookup Terminal is designed to support the lookup process without bringing the Hotel Application Systems into PCI scope. From a best practices standpoint, Hotel Staff should not have access to Payment Card Data. This can be accomplished by outsourcing the lookup process to the Tokenization Service provider or another third party. For example, the Hotel Staff member that has a Token and needs Payment Card Data calls the service provider, where a person looks up the Token, obtains the card number and completes the transaction on behalf of the Hotel Staff member. Offering this service is an incremental business opportunity for Tokenization Service providers, and the Hotel is relieved of the burden of compliance with respect to the Secure Lookup Terminal.

Depending on the needs and service levels being provided by the Hotel, it may or may not be feasible to outsource the lookup process, but in any case, the use of the Secure Lookup Terminal within the Framework can keep this process from bringing all Hotel Application Systems into PCI scope.

ACTORS AND PARTICIPANTS

- 2 Hotel PIP
- 3 Hotel Tokenization Service
- 8 Hotel/ Hosted PCI Environment
- Hotel Staff

Preconditions and Assumptions

The Hotel Staff has a Tokenized Payment Method Record and authorized access to a Secure Lookup Terminal.

Process

A The Hotel Staff enters the identifier of the Tokenized Payment Record Method into the Secure Lookup Terminal

8 Hotel/ Hosted PCI Environment to 2 Hotel PIP

B PIP sends Token to Hotel's Tokenization Service

2 Hotel PIP to 3 Hotel Tokenization Service

C Tokenization Service de-tokenizes and returns Payment Card Data to PIP

3 Hotel Tokenization Service to 2 Hotel PIP

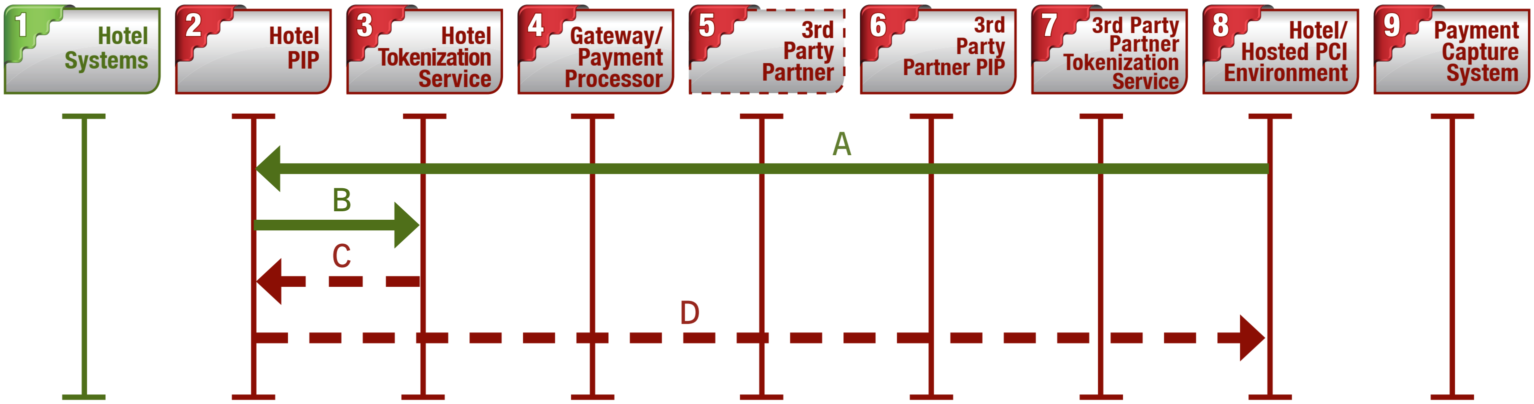
D The Hotel PIP sends the Payment Card Data to the Secure Lookup Terminal to display the corresponding Payment Card Data

2 Hotel PIP to 8 Hotel/ Hosted PCI Environment

Postconditions

Hotel Staff now has the full Payment Card Data.

SECURELY ACCESSING RAW PAYMENT CARD DATA MESSAGE FLOW DIAGRAM


1 Hotel Systems
2 Hotel PIP
3 Hotel Tokenization Service
4 Gateway/ Payment Processor
5 3rd Party Partner
6 3rd Party Partner PIP
7 3rd Party Partner Tokenization Service
8 Hotel/ Hosted PCI Environment
9 Payment Capture System
A
B
C
D

RELEVANT HTNG MESSAGES

A) HTNG_PaymentCardRQ

B) HTNG_PaymentCardRQ

C) HTNG_PaymentCardRS

D) HTNG_PaymentCardRS

USE CASE:

Collecting Payment Data through the Web

There are four basic business scenarios concerning web collection of payment information. Each scenario applies to individual transactions and potentially also to batch transactions:

- Customer enters Payment Card Data for reservation(s) pre-payment via the web, where payment is processed by the reservation system.
- Customer enters Payment Card Data via a web or other web-based self-service interface into Hotel Application System and updates their system profile, independent of any particular reservation.
- Customer enters Payment Card Data for reservation(s) pre-payment via the web, where Payment Card Data is stored in the reservation system for payment processing by another system.
- Customer enters Payment Card Data via the web at time of reservation(s) for guarantee purposes. The Payment Card Data is only stored and not processed. However, the card may be charged at a later date (and potentially by a different entity) if the Customer is a no-show.

ACTORS AND PARTICIPANTS

Customer

1 Hotel Systems

2 Hotel PIP

3 Hotel Tokenization Service

9 Payment Capture System

Preconditions and Assumptions

- Customer has selected a product on the Hotel Web Site for which Payment Card Data is required.
- Customer wishes to use a Payment Card for which no corresponding Tokenized Payment Method Record is on file in the Hotel Application System.

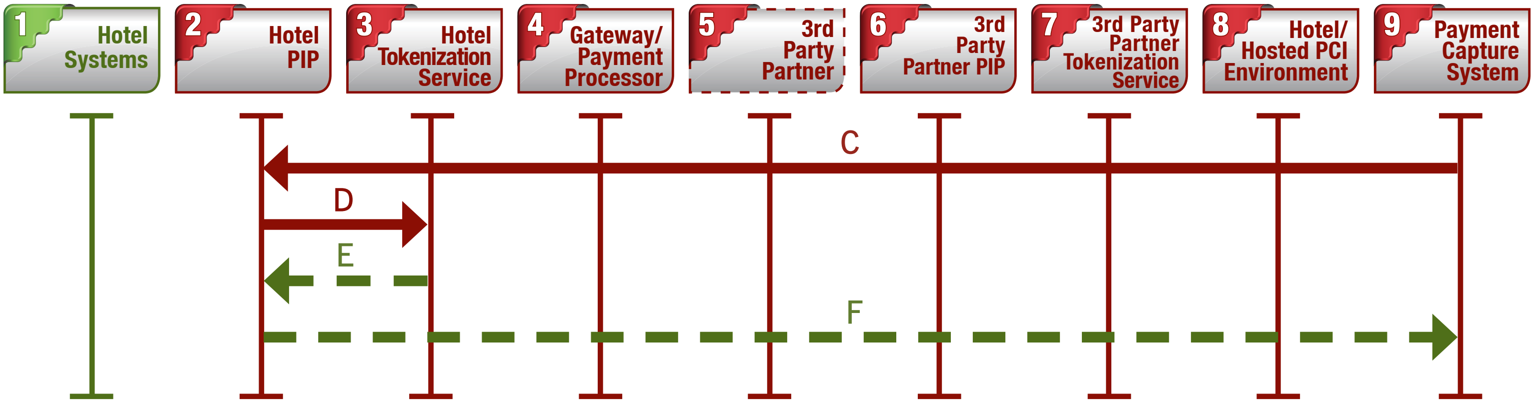
Process

A	Hotel Web Site redirects to Hosted Payment Collector web page	1 Hotel Systems	to	9 Payment Capture System
B	Customer enters Payment Card Data into their web browser	Customer	to	9 Payment Capture System
C	Hosted Payment Collector webpage securely sends Payment Card Data to the Hotel PIP	9 Payment Capture System	to	2 Hotel PIP
D	Hotel PIP sends Payment Card Data to Hotel Tokenization Service	2 Hotel PIP	to	3 Hotel Tokenization Service
E	Hotel's Tokenization Service returns token to Hotel's PIP	3 Hotel Tokenization Service	to	2 Hotel PIP
F	Hotel PIP returns Tokenized Payment Method Record to Hosted Payment Collector	2 Hotel PIP	to	9 Payment Capture Systems
G	Hosted Payment Collector webpage redirects Customer back to Hotel Web Site, returning Token for Hotel Web Site's use	9 Payment Capture Systems	to	1 Hotel Systems

Postconditions

Hotel Web Site has a Token that can be used in place of a Payment Card

COLLECTING PAYMENT DATA THROUGH THE WEB MESSAGE FLOW DIAGRAM



1 Hotel Systems
2 Hotel PIP
3 Hotel Tokenization Service
4 Gateway/ Payment Processor
5 3rd Party Partner
6 3rd Party Partner PIP
7 3rd Party Partner Tokenization Service
8 Hotel/ Hosted PCI Environment
9 Payment Capture System
C
D
E
F

RELEVANT HTNG MESSAGES

A) Not applicable	C) HTNG_PaymentCardProxyRQ	E) HTNG_PaymentCardProxyRS
B) Not applicable	D) HTNG_PaymentCardProxyRQ	F) HTNG_PaymentCardProxyRS

USE CASE:

Collecting Payment Data Over Voice Channels

A Customer calls a Hotel's contact center and needs to provide Payment Card Data, for example to guarantee a reservation or update a profile.

Traditional operating methods for larger contact centers expose the Hotel company to the full scope of PCI requirements because the systems and agents have access to Payment Card Data. Furthermore, most contact centers maintain recordings of telephone conversations that may include Payment Card Data.

To remove the agents and recordings from PCI scope, an Interactive Voice Response (IVR) System can be used to capture and tokenize Payment Card Data in a private "conversation" between the Customer and the IVR System; the agent is not a party to the conversation and therefore has no exposure to Payment Card Data. The IVR System itself will fall within PCI scope, but can be a Hosted Payment Collector operated by the Hotel's PIP or other third party with access to the Tokenization Service.

When an agent needs to ask a Customer for Payment Card Data, they transfer control of the call to the IVR System after instructing the Customer that they will need to speak or enter their Payment Card Data directly into the IVR System. While the Customer is entering the Payment Card Data, the agent is blocked from listening. Once the Customer has finished entering the Payment Card Data, the conversation between the Customer and the agent resumes.

ACTORS AND PARTICIPANTS

Customer

1 Hotel Systems

2 Hotel PIP

3 Hotel Tokenization Service

9 Payment Capture System

Preconditions and Assumptions

Customer is on the telephone with an agent in a contact center that has an IVR System.

Process

A Hotel Application System initiates a request to the IVR Hosted Payment Collector to collect Payment Card Data for a particular transaction

1 Hotel Systems to 9 Payment Capture System

B IVR Hosted Payment Collector requests the Customer to enter or speak their Payment Card Data

Customer ↔ 9 Payment Capture System

C IVR Hosted Payment Collector captures the Payment Card Data and sends it to the Hotel PIP

9 Payment Capture System to 2 Hotel PIP

D Hotel PIP sends Payment Card Data to Tokenization Service

2 Hotel PIP to 3 Hotel Tokenization Service

E Tokenization Service returns Tokenized Payment Method Record to Hotel PIP

3 Hotel Tokenization Service to 2 Hotel PIP

F Hotel PIP sends Tokenized Payment Method Record to IVR Hosted Payment Collector

2 Hotel PIP to 9 Payment Capture System

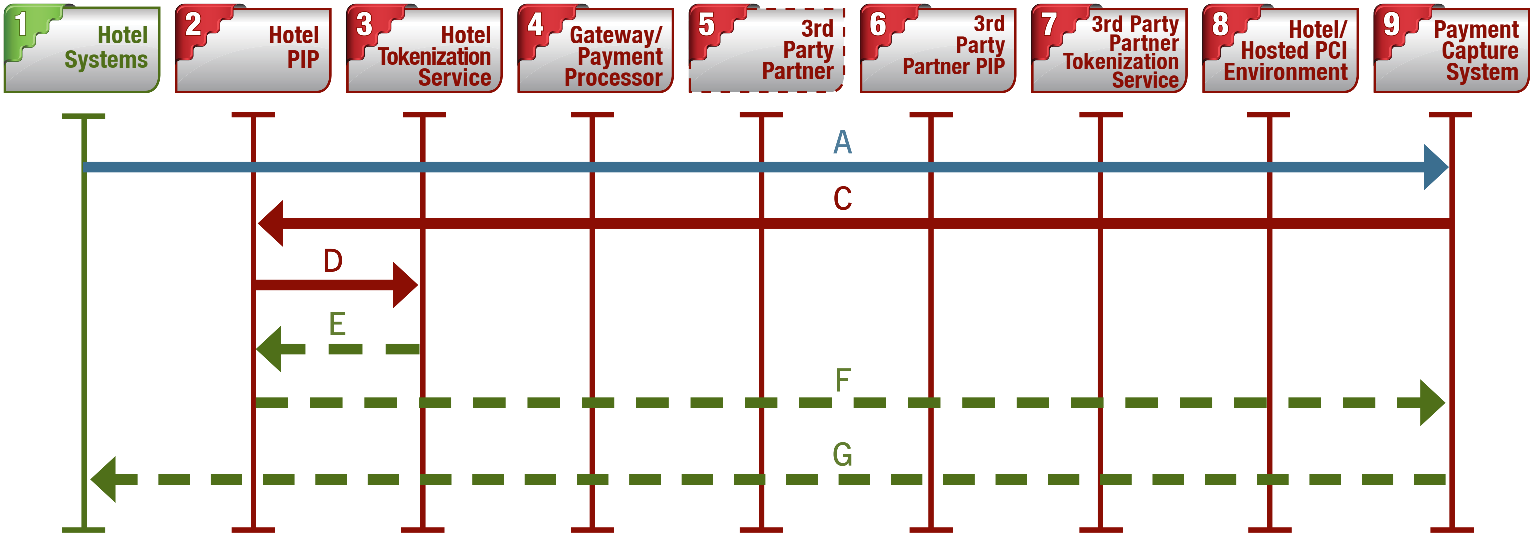
G IVR Hosted Payment Collector returns Tokenized Payment Method Record and transaction identifier to Hotel Application System

9 Payment Capture System to 1 Hotel Systems

Postconditions

The Hotel Application System has a Tokenized Payment Method Record that can be used in place of a Payment Card.

COLLECTING PAYMENT DATA OVER VOICE CHANNELS MESSAGE FLOW DIAGRAM


1 Hotel Systems
2 Hotel PIP
3 Hotel Tokenization Service
4 Gateway/ Payment Processor
5 3rd Party Partner
6 3rd Party Partner PIP
7 3rd Party Partner Tokenization Service
8 Hotel/ Hosted PCI Environment
9 Payment Capture System
A
C
D
E
F
G

RELEVANT HTNG MESSAGES

A) Not yet defined*

B) Not applicable

C) HTNG_PaymentCardProxyRQ

D) HTNG_PaymentCardProxyRQ

E) HTNG_PaymentCardProxyRS

F) HTNG_PaymentCardProxyRS

G) Not yet defined*

*May be addressed by future HTNG efforts.

USE CASE:

Exchanging Payment Information

A third party (such as an Online Travel Agent) sends a transactional message (such as a reservation) to a Hotel Application System, where the message includes Payment Card Data. The third party may have tokenized the Payment Card Data, but if it has, the Hotel will not typically be able to use the third party's Tokens to process transactions due to differences in tokenization scheme or tokenization provider.

In order for the receiving Hotel Application System to remain outside of PCI scope, the incoming message is intercepted by the Hotel's PIP and the Payment Card Data is identified, extracted, tokenized using the Hotel's Tokenization Service and replaced; the message is then forwarded to the intended receiving Hotel Application System.

This process also works in reverse. If a Hotel Application System needs to send a transactional message containing Payment Card Data, it sends a message with a Tokenized Payment Method Record to the Hotel's PIP, which calls the Hotel's Tokenization Service to obtain actual Payment Card Data. The Hotel's PIP then substitutes the Payment Card Data for the Token and securely forwards the message to the intended recipient.

If the third party also uses tokenization and a PIP (as we have assumed in the diagrams below), then the third party sends the transaction using the reverse process. In this case, the sensitive portions of the transaction are entirely handled by secure entities within PCI scope, and not by the Hotel or the third party.

ACTORS AND PARTICIPANTS

1 Hotel Systems

2 Hotel PIP

3 Hotel Tokenization Service

5 3rd Party Partner

6 3rd Party PIP

7 3rd Party Tokenization Service

Preconditions and Assumptions

- Third-Party System needs to securely send the Payment Card Data to a Hotel Application System.
- Third-Party System has the endpoint (e.g. IP address) that the Hotel has designated to receive messages.
- Hotel's endpoint is managed by a PIP Service and uses a Tokenization Service.
- Third-Party System is using a Tokenization Service and a PIP.

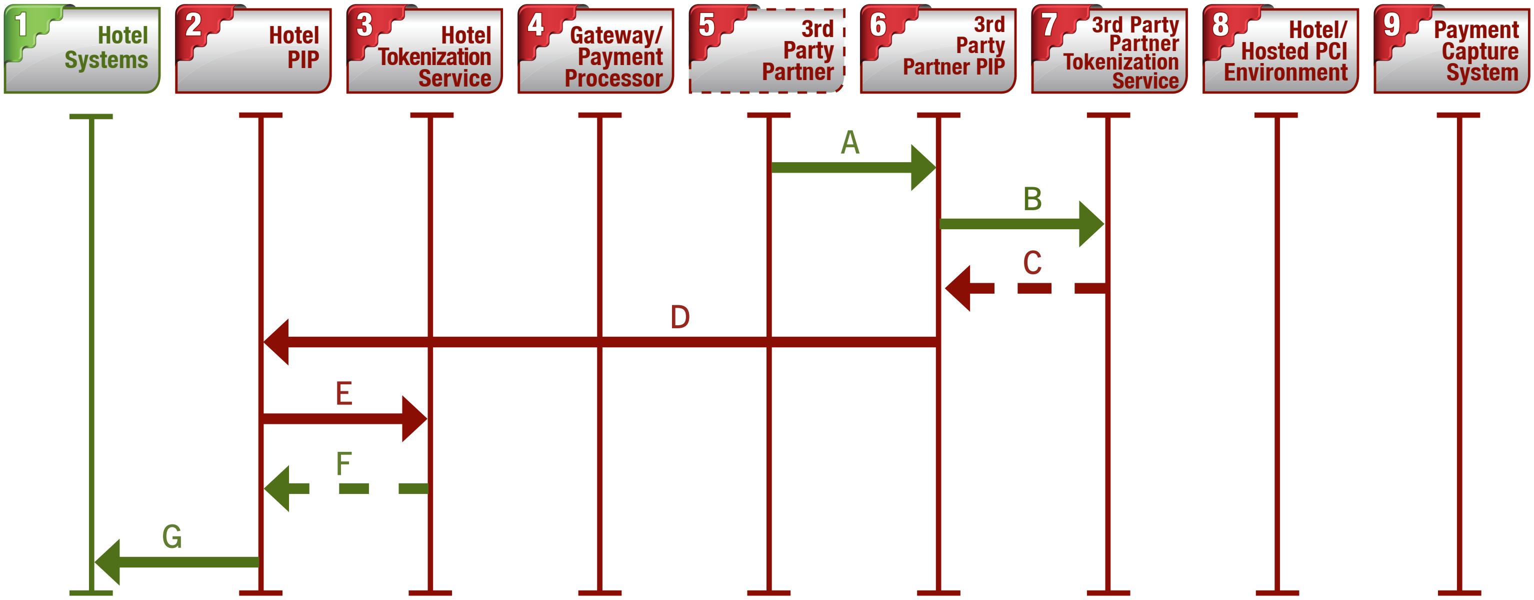
Process

A	Third-Party Partner sends transaction with Tokenized Payment Method Record to Third-Party Partner PIP	5 3rd Party Partner	to	6 3rd Party PIP
B	Third-Party Partner PIP extracts Tokenized Payment Method Record from transaction message, and sends it to Third-Party Tokenization Service	6 3rd Party PIP	to	7 3rd Party Tokenization Service
C	Third-Party Tokenization Service de-tokenizes and send encrypted Payment Card Data to Third-Party PIP via secure transport	7 3rd Party Tokenization Service	to	6 3rd Party PIP
D	Third-Party Partner PIP replaces Tokenized Payment Method Record with Payment Card Data in transaction message, and sends message to Hotel PIP via secure transport	6 3rd Party PIP	to	2 Hotel PIP
E	Hotel PIP extracts Payment Card Data from transaction message and sends it to Hotel's Tokenization Service via secure transport	2 Hotel PIP	to	3 Hotel Tokenization Service
F	Hotel Tokenization Service sends Tokenized Payment Method Record to Hotel PIP via secure transport	3 Hotel Tokenization Service	to	2 Hotel PIP
G	Hotel PIP replaces Payment Card Data in transaction message with Tokenized Payment Method Record and sends it to Hotel Application System	2 Hotel PIP	to	1 Hotel Systems

Postconditions

- The Hotel Application System now has a Tokenized Payment Method Record that it is able to use for transactional purposes

EXCHANGING PAYMENT INFORMATION MESSAGE FLOW DIAGRAM



1 Hotel Systems
2 Hotel PIP
3 Hotel Tokenization Service
4 Gateway/ Payment Processor
5 3rd Party Partner
6 3rd Party Partner PIP
7 3rd Party Partner Tokenization Service
8 Hotel/ Hosted PCI Environment
9 Payment Capture System
A
B
C
D
E
F
G

RELEVANT HTNG MESSAGES

A) Arbitrary message agreed by trading partners

B) HTNG_PaymentCardRQ

C) HTNG_PaymentCardRS

D) HTNG_PaymentProcessingRQ

E) HTNG_PaymentCardProxyRQ

F) HTNG_PaymentCardProxyRS

G) Arbitrary message agreed by trading partners

USE CASE:

Handling Unstructured Payment Card Data Sent by Customers

In this use case, the Customer sends Payment Card Data intended for the Hotel, via means such as fax, e-mail or electronic messages sent in a format that the receiving Hotel Application System cannot accept without manual intervention (e.g. re-keying) or pre-processing.

One situation where this may occur is when a Meeting Planner manages a list of attendees in a spreadsheet (for example) that includes the payment information for each attendee. This spreadsheet is then e-mailed or faxed to the property or uploaded through a web application. This Meeting Planner role may be played by someone like a Little League coach making arrangements for a travel team, or a bride making arrangements for a wedding, rather than a professional Meeting Planner.

Systems that store, process or transmit Payment Card Data fall within the scope of PCI requirements. If a Hotel accepts Payment Card Data via fax, e-mail or similar means, then these systems fall within the scope of PCI.

The simplest way for the Hotel to avoid PCI-DSS requirements on these systems is to engage a third party to intercept and to use the Hotel's PIP and Tokenization Services to tokenize the Payment Card Data and send it to the Hotel environment. Solutions exist to perform this function with e-mail and other electronic documents. For faxes, optical character recognition may find some card data, but human review may be necessary as well.

This is analogous to the automated process performed by a Payment Information Proxy (PIP), and is a new potential service offering for a PIP system provider or other third party.

Paper and postal mail are not explicitly addressed here, because paper-based transactions are not handled by Hotel Systems; the objective of this Framework is to get systems out of scope. It can, however, be handled either by forwarding it to a secure central facility for handling, or by handling the Payment Card entry in a secure fashion as described in other use cases.

Process

- Receive information into Secure Data repository
- Manual entry of info through Secure Payment Terminal – see "Collecting Payment Card Data" use case
- Securely maintain archives of original documents (if needed)