Payment Processing for Retail Petroleum/Convenience

December 31, 2014

Version 1.1

Abstract

This white paper describes some of the unique challenges and requirements for payment card processing in a retail petroleum/convenience environment.

Contributors

Linda Toth, Conexxus
Sue Chan, W Capra
Bob Slimmer, BP
Sharon Scace, WEX
Alan Thiemann, Conexxus Counsel
Brian Russell, VeriFone
Dan Fritsche, Coalfire
James Shepard, Phillips 66
Steven Bowles, Wayne

Revision History

Revision Date	Revision Number	Revision Editor(s)	Revision Changes
December 31, 2014	1.1	Linda Toth, Conexxus	Removed "Draft" Watermark
September 23, 2014	1.0	Linda Toth, Conexxus	Incorporated Feedback Release Version
August 25, 2014	Draft 0.6	Linda Toth, Conexxus	Incorporated Feedback
August 16, 2014	Draft 0.5	Linda Toth, Conexxus	Incorporated Feedback
August 12, 2014	Draft 0.4	Linda Toth, Conexxus	Incorporated Feedback
August 5, 2014	Draft 0.3	Linda Toth, Conexxus	Incorporated Committee Feedback
August 4, 2014	Draft 0.2	Linda Toth, Conexxus	Incorporated Committee Feedback
July 22, 2014	Draft 0.1	Linda Toth, Conexxus	Initial Version

Copyright Statement

Disclaimers

Conexxus makes no warranty, express or implied, about, nor does it assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product, or process described in these materials. Although Conexxus uses reasonable best efforts to ensure this work product is free of any third party intellectual property rights (IPR) encumbrances, it cannot guarantee that such IPR does not exist now or in the future.

Introduction

Driven partially by needed functionality for pay-at-the-pump transactions, as well as the acceptance of a variety of cards (both payment and other), the retail petroleum/convenience sector faces several challenges and requirements that are unique to the industry. This white paper describes some of these challenges and requirements.

Paying for Fuel at the Dispenser

Paying for fuel at the dispenser typically begins with the consumer swiping a payment card, which triggers a pre-authorization request message to the payment host. The request may contain a specific fixed dollar amount (e.g., $50) or a token amount (e.g., $1), which indicates to the host to use a preconfigured limit (e.g., $75). Limits may vary by card type, local jurisdiction, and other factors.

If the transaction is authorized, the host responds to the request with a pre-authorization amount and places a hold on funds for that pre-authorization amount. The fuel dispenser transaction limit is determined by card type, local fueling restrictions, and the returned pre-authorization amount. The dispenser is then authorized up to the transaction limit amount and the customer may begin fueling. Once fueling is finished, the actual amount of the sale is transmitted in a completion message to the host. The host releases the unused amount of the original pre-authorization and finalizes the sale in the actual amount.

The actual time to release reserved funds rests with the host and card processors (i.e., is outside the control of the site). This is a particularly sensitive issue with debit card users because the funds originally reserved in the pre-authorization are unavailable for other use until the host releases the unused amount.

Other retail sectors (e.g., hotels, car rentals) may also use a pre-authorization and completion message pair. These transactions, however, are for typically much higher dollar purchases. In addition, they typically involve longer periods of time between the pre-authorization and the completion (e.g., days).

Most retail petroleum/convenience sites require some form of partial approval of a transaction for bank cards, debit cards, and gift cards. For example, if the pre-authorization request is for $75, but only $20 in funds is available, the authorization may return partial approval for $20. This allows the consumer to purchase up to $20

rather than being completely denied any fuel because the request to pre-authorize $75 failed.

Card Types

Retail petroleum/convenience sites typically accept, via a Point of Sale (POS) or equivalent (i.e. Electronic Payment Server (EPS)), one or more of the following card types described below. These cards fall into two broad categories:

1. Those processed with little or no POS/EPS logic required; and
2. Those whose processing requires the POS/EPS to positively identify the card for purposes of performing "card based" business logic required by the issuer of the card.

The second category of cards require special considerations, in particular when implementing point-to-point encryption solutions (encryption at swipe) to protect sensitive cardholder data, rather than allowing data to be transmitted in the clear (as cleartext).

The following three "bank" card types require little POS/EPS processing logic. Other than the ability to rule out that these cards fall into one of the categories requiring business logic, these bank cards can be processed with standard prompts such as "Process as Debit?" and "Enter PIN". Typically, standard ISO Bank/Issuer Identification Number (BIN/IIN) ranges (limited to the first six digits of the account number) and a debit prompt allow the POS/EPS to process these cards and that processing differs little from a standard retail environment.

Bank Cards: These cards include those issued by American Express, Discover, JCB, MasterCard and Visa. They may have prompting (e.g., Zip Code or CVV2) requirements. These cards must follow rules related to protecting sensitive cardholder data.

Debit Cards: These bank cards generally require the use of a PIN, which requires the customer to enter the PIN on an approved secure PIN-entry device.

Dual Use Cards: These bank cards may be used as credit or debit and therefore require extra prompting and logic.

The following cards fall into the category requiring "card based" POS/EPS logic to process, and are largely what make retail petroleum card processing unique. In general, the data required by the POS/EPS to process these cards at the site falls outside the normal allowable first 6/last 4 positions (F6L4) recognized by the PCI SSC and the PCI DSS standard as non-sensitive data. Industry standard encryption methods, performed

at the card swipe, render card data required by the POS/EPS to process the cards unreadable and irrecoverable within the merchant environment. Accordingly, the challenge facing retailers in the retail petroleum channel is how to encrypt card data at the point of swipe while still allowing the necessary local "card based" business logic, which may require the exposure of additional digits of the Primary Account Number (PAN), to process the cards.

Fleet Cards: This card type can be either bank cards (e.g., MasterCard Fleet, Visa Fleet) or third party cards (e.g. WEX, Voyager, Fuelman, FleetOne). These cards are issued to customers that maintain fleets of vehicles, enabling the petro retailer to offer special promotions (e.g., fuel purchase discounts), to simplify billing, and to enable the issuer/host to provide data collection services. Data embedded in the card's magnetic stripe (i.e., PAN, discretionary track data) indicates requirements for fleet data prompting (e.g., odometer, driver id, vehicle id) and/or purchase restrictions (i.e., what types of products and/or fuel may be purchased). The POS/EPS requires access to those embedded track data items to generate appropriate prompting and to restrict product purchases as required by the fleet issuer. The challenge is to provide encryption solutions that secure cardholder data according to standards, while ensuring that the prompting and product restriction codes are available to the business logic in the POS/EPS.

Co-Branded Cards: These bank or third-party cards are issued in conjunction with a petroleum retailer. Petroleum retailers require their systems to have the ability to identify co-brand cards so that the sites can offer discounts or other benefits to customers holding the co-branded cards. Some of these cards cannot be identified as a co-branded card simply by using the first six digits of the card. Therefore, typical encryption methods (e.g., exposing only the first 6/last 4 digits of the PAN) may prevent a site from exploiting co-branded card features and benefits.

Loyalty Cards: These cards contain membership information for a loyalty program, which allows the customer to earn or redeem rewards. Sites may be able to accept one or more loyalty cards. When accepting multiple loyalty cards, special business logic in the POS/EPS is required.

Hybrid Cards: These cards have loyalty and payment features in the same card. Because the account number for loyalty is the same as the account number for payment, these cards may require following the card issuer's rules to protect sensitive cardholder data. Protecting a dual use account number may render data required by the POS/EPS

to process the loyalty portion unreadable and therefore may create data usage problems for a loyalty program.

Access Cards: These cards enable dispenser functionality (e.g., Fueling Station Attendant, Diagnostic Mode). Because data from these cards is typically returned in the clear, care must be taken to ensure there is no overlap with other card types, which may cause a conflict in encryption requirements.

Two Card Solutions: These solutions require a card pair to achieve functionality (e.g., Driver and Vehicle Card Pairs, Membership and Payment Card Pairs). Each card is treated as a unique/separate encrypted card swipe. The POS or equivalent will hold the business logic required to process the cards together. For driver/vehicle card pairs, typically one of the cards will not have traditional account data and may require additional/different processing rules. These cards may require following one or both card issuer's rules to protect sensitive cardholder data.

Local Cards: These cards are authorized locally (e.g., at the site, the POS, or other retailer network), as opposed to the main credit and debit processing networks. These cards may require following the card issuer's rules to protect sensitive cardholder data.

Conclusion

In summary, there are many unique challenges with card-based payment methods for the retail petroleum/convenience sector. These challenges are driven in part by pay-at-the-pump and the significant diversity in payment card types. Conexxus is committed to ensuring that retail and financial service industry standards (e.g., X9, ISO TC68) take into account these unique requirements. Visit us on the web at www.conexxus.org for additional information.