

# Credit Card Processing with LUKE and SHELBY

Educational Guide



## Disclaimer

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Digital Payment Technologies Corporation.

No patent liability is assumed with respect to the use of the information contained herein. Neither is any liability assumed for damages resulting from the use of the information contained herein.

The Digital brandmark is a Service Mark of Digital Payment Technologies Corporation. © Copyright 2010 Digital Payment Technologies™ Corporation. All rights reserved.



## Contents

Introduction	7
Processing Environment	7
Processing Methods	9
Reconciling Credit Card Data	14
Supported Merchant Processors	14
About Digital Payment Technologies	15



**Increase revenues and compliance by providing more payment options.**

## Introduction

Parking operators can greatly increase revenues as well as compliance at parking facilities by providing more payment options to parkers. Positive results are especially evident when one of these payment options is credit card payment.

Both the LUKE and SHELBY pay stations, manufactured by Digital Payment Technologies (DPT), have the option to accept credit cards as a form of payment and process these transactions either in real-time or via a batch method. This document explains the processing environment, the differences between batch and real-time processing, associated fees for different methods of processing, the method for reconciliation with bank statements, and the merchant processors currently supported on DPT equipment.

## Processing Environment

The LUKE and SHELBY have an optional credit card reader used for accepting credit card transactions. Information from the credit card and the associated transaction is then either stored on the pay station for future batch processing or processed in real-time via a merchant processor through DPT's Enterprise Management System (EMS).

## Application Service Provider Hosted Environment

EMS is a system operated by DPT to process payments on behalf of pay station clients. For large clients, this environment may be set up and configured in the client's data center. EMS servers assist in the management and operation of a client's fleet of pay stations, and process consumer credit card payments. EMS servers have been specifically designed to remove all sensitive card data after the post-authorization message (sale transaction) is concluded.

EMS components include:

- **Application Server:** to handle the interaction between pay stations and EMS database as well as to serve the Web pages that comprise EMS graphical user interface. All communications with this server

are protected by 128-bit SSL (Secure Socket Layer) encryption. User access is restricted by user name, password, and module access control lists.

- **Database Server:** to handle all corresponding information from the pay stations. The database can include account and configuration information for pay stations, transaction information, and credit card data consisting of only the card type, last four digits of the card number, and the digital signature. No Track 2 or Primary Account Number (PAN) data is stored or logged.

Additional elements of the EMS environment include:

- A dedicated EMS Server (i.e. a server that is not shared with other businesses or applications).
- EMS Server is hosted by an internationally recognized and award-winning data center.
- The system availability is 99.99 percent.
- The power source is backed up by a diesel generator-assisted uninterruptible power supply (UPS).
- The storage media are mirrored and hot-swappable.
- EMS Server access is restricted to authorized DPT employees only.
- Employee access is controlled and tracked.

### Storage and Communication Protocols

The intent of these systems is to manage the processing of the payment, but not to store any sensitive information. The only data that remains after a successful credit card transaction is:

- Card type
- Last four digits of the PAN
- Digital signature of the PAN

All encrypted data including PAN and Track 2 is removed after final authorization of a transaction.

All data stored on the pay station, BOSS Data Key, BackOffice Support System (BOSS), and EMS is encrypted with 2048-bit encryption. All data transferred between the pay station, EMS Server, and the processor's server is done using SSL (SSL is a security technology commonly used to secure e-commerce transactions through 128-bit data encryption). Additionally, any encryption schemes in place by the Internet Service Provider (via Wi-Fi, CDMA, or GSM/GPRS technologies) further encrypt the data transmission.

EMS Server also provides another layer of data security with the use of the nCipher card. This card provides hardware-based, cryptographic operations such as random number generation, key generation, digital signatures, and key archive and recovery.

**All encrypted data is removed after final authorization of a transaction.**

**All DPT equipment has been designed to meet or exceed PCI standards.**

The pay stations initiate all communications with EMS and do not accept incoming requests to establish a connection (i.e. the pay stations are part of a “push” system). Information only flows out from the pay stations. Hence, it is impossible for an unauthorized entity to connect to a pay station. In addition, the SSL certificates installed on EMS Server are signed by Comodo, which is a WebTrust Compliant Certification Authority.

## Compliance with Payment Card Industry (PCI) Standards

The PCI Data Security Standard is the credit card industry's set of stringent regulations and policies that govern the processing, transmission, and storage of credit card data. All DPT equipment has been designed to meet or exceed these standards.

DPT first received official compliance as a Level 1 Service Provider in April 2007 for the processing of credit card data through EMS after completing an audit by a qualified security assessor (QSA). DPT completed its third annual audit in May 2009. DPT's products received official validation under PCI's Payment Application Data Security Standard (PA-DSS), a sub-set of PCI, in December 2007 and its latest major software release was validated in May 2009. DPT products meet PCI standards for both real-time and batch processing methods.

DPT's current status under the PCI and PA-DSS standards may be found by reviewing the updated lists maintained on Visa's Web site ([http://usa.visa.com/merchants/risk\\_management/cisp.html](http://usa.visa.com/merchants/risk_management/cisp.html)).

To learn more about PCI standards, please phone DPT at 888-687-6822 to obtain a copy of the white paper entitled *PCI Data Security and the Parking Industry*.

## Processing Methods

There are two methods for processing credit card data—batch (offline) and real-time (online).

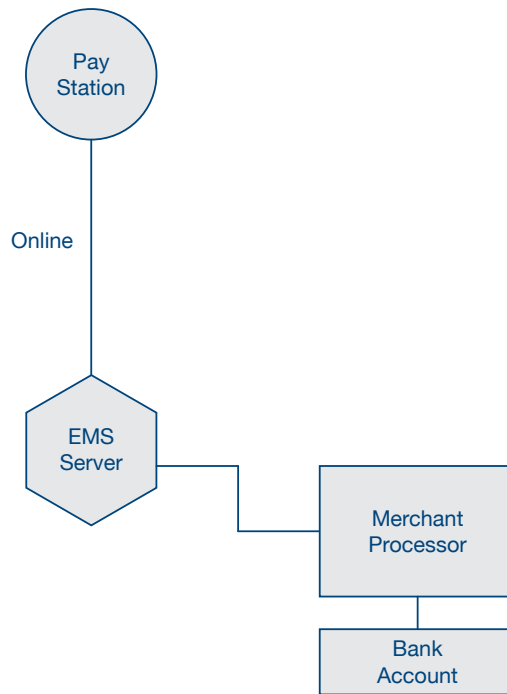
### 1. Real-Time Processing (Online)

Real-time credit card processing enables parkers to obtain an instant approval or declination of their transactions, all within a matter of a few seconds (typically four to five). This method of processing also provides parking operators the following benefits:

- Elimination of bad credit card debt
- Faster deposit of money into the bank
- Lower transaction fees paid to the merchant bank processing the transaction

To facilitate real-time credit card processing, all pay stations must be connected to the Internet either through Ethernet, Wi-Fi, or cellular (GSM/GPRS/CDMA) network. Operators must also subscribe to the DPT Real-Time Credit Card Processing service to support this capability. A typical real-time credit card transaction is as follows:

1. Credit card information is swiped at the pay station.
2. Credit card data is encrypted via 2048-bit RSA encryption and communicated to EMS Server using additional 128-bit SSL encryption through an Ethernet, Wi-Fi or cellular network.
3. EMS Server receives the transaction and securely connects to the merchant processor selected by the parking operator.
4. Merchant processor either authorizes or declines the transaction.
5. Parkers with a declined card will be notified at the pay station with the message “Card Declined.”
6. Parkers with an accepted transaction will be notified at the pay station with the message “Authorized” and will receive a printed receipt with the authorization number of the transaction.
7. At the end of the day, the merchant processor will settle all transactions and deposit the funds into the parking operator’s bank account.



In the event that the communication network is unexpectedly disrupted, LUKE and SHELBY pay stations running version 6.2.0 or higher will store the transaction and then automatically forward it for processing

when communication is re-established. In software versions prior to 6.2.0, transactions occurring when communications are disrupted are batch processed manually (see Batch Processing Method).

An outline of the hardware and fee requirements associated with real-time processing can be found in the following table:

Equipment	Hardware	Cost
LUKE or SHELBY Pay Station	Ethernet	Cabling, switch, and router hardware costs. Connectivity costs are minimal as several pay stations can be serviced by a single connection running through a router; however, costs to bring cabling to each pay station can be high.
	Cellular Modem	Modem costs and monthly data plan fees based on volume of transactions. Unlimited accounts are recommended, which are typically around \$40 per month per pay station.
	Wi-Fi Bridge	Bridge and Network costs vary depending on the size of the area covered. While up-front costs can be high, there can be significant long-term savings over cellular.
EMS Service Subscription	None	Monthly EMS subscription fee along with a monthly real-time processing fee per pay station.
BOSS Computer	Internet Connection	One-time license and setup fee
Merchant Processor	None	Per transaction fee. Fees vary by processor, but are typically about \$0.20 per real-time transaction. If required to use a gateway processor to connect to the merchant processor, additional charges will apply; however, charges can be minimal based on large transaction volumes.

## 2. Batch Processing (Offline)

**Costs can be higher with increased bad card debt and transaction fees.**

Batch processing of credit card transactions is required to complete the settlement process when the pay station operates in a stand-alone environment, with no communication device connecting the pay station to EMS. This method of processing also provides parking operators the following benefits:

- Elimination of pay station communication equipment costs
- Elimination of real-time credit card processing service fees
- Elimination of communication network costs

However, the costs can be higher in the long-term with increased bad card debt and more expensive transaction fees.

To demonstrate the true cost comparison between batch and real-time processing using a single pay station, consider the following example:

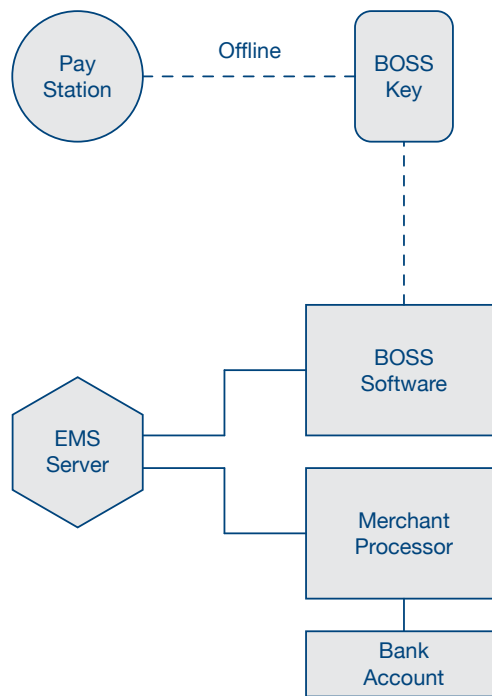
Batch Variables	
Credit card transactions per month per pay station	200
Average parking transaction per day	\$5.00
Cards used that are lost, stolen or have insufficient funds	10%
Extra processing charge per batch transaction	\$0.10
Labor cost to collect transactions per month	\$25.00
Total Batch Costs – $10\% \times (200 \times \$5) + (\$0.10 \times 200) + \$25 = \$145$	

Real-Time Variables	
Cellular fees for real-time processing per month	\$40.00
Average EMS real-time service cost per month	\$50.00
Total Real-Time Costs – $\$40 + \$50 = \$90$	

Over multiple pay stations, this example demonstrates that the true cost of batch processing is much higher than real-time processing.

The typical batch processing method using the LUKE or SHELBY is as follows:

1. Credit card is swiped at the pay station.
2. Credit card data is encrypted and stored.
3. Parker receives a ticket for a paid transaction.
4. On a regular schedule, the parking operator manually downloads all transactions from each pay station onto the BOSS Data Key.
5. BOSS Data Key is connected to the BOSS computer in the head office and all transactions are downloaded.
6. Credit card transactions are sent from the BOSS computer through the Internet to EMS.
7. Once EMS receives the transactions, it connects to the merchant processor selected by the parking operator.
8. Merchant processor authorizes or declines each transaction.
9. After a user specified number of retries, revenues associated with the rejected cards will be lost, but the rejected card numbers will be stored on the bad card list. The list can be manually loaded onto the pay station to prevent future purchases using those cards.
10. BOSS will then be notified of the authorized transactions for reporting purposes.
11. At the end of the day, the merchant processor will settle all transactions and deposit funds into the parking operator's bank account.



An outline of the hardware and fee requirements associated with batch processing can be found in the table below:

Equipment	Hardware	Cost
LUKE or SHELBY Pay Station	None	None
BOSS Computer	Internet Connection	One-time license and setup fee
Merchant Processor	None	Per transaction fee. Fees vary by processor, but they are typically about \$0.30 per batch transaction. Requirement to go through a gateway processor to reach a merchant processor will add additional charges, but charges can be minimal based on large transaction volumes

**Both processing methods should be considered before deciding which to use.**

Aside from the financial charges, batch processing transactions can also be confusing to clients if parking was purchased over several days and then batched one week later, resulting in a single charge for all transactions. In this case, all of the charges will appear to have occurred at the same time. This situation can result in an increase in customer complaints. Based on these issues, a careful examination of the pros and cons and the long-term financial impact of both processing methods should be considered before deciding which method to use.

## Reconciling Credit Card Data

Reconciling credit card data from the pay station with bank account statements is accomplished by generating reports through EMS. All credit card transaction information is stored in EMS for both batch and real-time processing environments. The information for each transaction includes transaction date and time, the pay station where payment was accepted, the rate selected, the type of credit card used, the total charge, and the authorization number for the transaction. EMS also records the date and time of each stage of the credit card transaction process as it's completed.

When transactions are sent to merchant processors, they are first pre-authorized to confirm that the card is valid and the transaction will be accepted. The pre-authorization is confirmed with an authorization number that is printed on the parker's receipt. The actual deposit into the parking operator's bank account will occur as a separate event known as the settlement process. Depending on the merchant processor, the settlement process can occur a few seconds after the pre-authorization or it can occur at the end of the day. In some cases, the parking operator can specify the time of day settlement occurs.

To reconcile pay station credit card transactions with bank statements, a report can be generated in EMS based on the settlement date in order to generate daily deposit totals. This set of totals can then be compared directly with the parking operator's bank deposit statement.

## Supported Merchant Processors

DPT has developed direct integrations with several merchant processors, and one gateway processor, to facilitate credit card processing. Each merchant processor must be reviewed separately to determine the best one to meet a parking operator's needs as they all differ in terms of contract requirements, fees, and service levels. Gateway processors are typically more expensive than directly supported processors, but they have the advantage of enabling the LUKE and SHELBY pay stations to access a greater number of merchant processors that may be better suited to a client's unique needs.

The currently supported merchant processors are listed in the following table:

Supported Credit Card Processors	
Canada	Moneris Paymentech
U.S.A.	Alliance Data Systems First Data EFSNet Paymentech First Data Nashville Link2Gov First Horizon

**Processors must be reviewed to determine which one best meets a client's needs.**

## About Digital Payment Technologies

Digital Payment Technologies (DPT) is an innovative leader in the design, manufacture, and distribution of electronic multi-space parking meters, parking management software, and online services for the multi-billion-dollar parking industry. The company's products provide complete financial tracking, control, and reporting for parking revenue collected by municipalities, universities, parking management companies, and national parks, from customer payment through to bank deposit.

### Digital Payment Technologies

330 – 4260 Still Creek Drive  
Burnaby, B.C.  
V5C 6C6

888.687.6822 | [digitalpaytech.com](http://digitalpaytech.com)