

Benefits of Integrated Credit Card Processing Within Microsoft Dynamics® GP

White Paper



May 2011

Copyright

Copyright © 2011 k-eCommerce. All rights reserved.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of k-eCommerce. Notwithstanding the foregoing, the licensee of the software with which this document was provided may make a reasonable number of copies of this document solely for internal use.

Trademarks

k-eCommerce® and eSource® are registered trademarks of k-eCommerce. The names of actual companies and products mentioned herein may be trademarks or registered marks - in the United States and/or other countries - of their respective owners. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

Intellectual property

k-eCommerce may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. The furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property except as expressly provided in any written license agreement from k-eCommerce.

Warranty disclaimer

k-eCommerce disclaims any warranty regarding the sample code contained in this documentation, including the warranties of merchantability and fitness for a particular purpose.

Limitation of liability

The content of this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by k-eCommerce. k-eCommerce assumes no responsibility or liability for any errors or inaccuracies that may appear in this manual. Neither k-eCommerce nor anyone else who has been involved in the creation, production or delivery of this documentation shall be liable for any indirect, incidental, special, exemplary or consequential damages, including but not limited to any loss of anticipated profit or benefits, resulting from the use of this documentation or sample code.

License agreement

Use of this product is covered by a license agreement provided with the software product. If you have any questions, please call k-eCommerce at 734-928-6000 or 734-928-6020.

Table of Contents

Abstract	1
Problem Statement	1
Solution	1
Credit Card Payment Process	2
Merchant Accounts	2
Payment Gateways	2
How do Credit Card Payments Work.....	2
PCI Compliance – What is it and Why is it Important	3
k-eCommerce Credit Card Extension	4
Background	4
Integration Points	4
k-eCommerce Credit Card Extension Data Flow	5
Conclusion	6
Glossary	7

Abstract

This white paper intends to educate readers who are considering accepting credit cards for their business while also explaining the process of credit card transactions and industry security requirements that have been established. This white paper will also provide information about credit card payment applications and the benefit of connecting them with back-office enterprise resource planning (ERP) systems to gain greater efficiency and insight in one convenient location without the need to go out to a payment gateway to process credit cards.

Problem Statement

Organizations that want to accept credit card payments from customers who are also using or plan to use an Enterprise Resource Planning system like Microsoft Dynamics® GP and need a built-in credit card payment solution that is PA-DSS certified and removes the need to go out to a payment gateway to process credit cards.

Solution

Credit Card Extension is a credit card processing application that can integrate into an Enterprise Resource Planning system like Microsoft Dynamics® GP and also adhere to security standards passed by the Payment Card Industry Security Standards Council (PCI-SSC). It provides credit card processing, transaction management and tracking in the Microsoft Dynamics® GP Sales Order Processing and Receivable Management modules. Transaction types such as authorization, post-authorization, sale, void, and credit are provided through the Sales Payment Entry, the Receivable Transaction Entry and the Cash Receipts Entry windows.

Features

The main features Credit Card Extension provides users of Microsoft Dynamics® GP with are as follows:

- Provides all credit card transaction types through Sales Payment Entry Window, Cash Receipt Window, and Receivable Transaction Entry Window
- Offers availability to post-authorize or credit throughout either Sales Payment Entry or Cash Receipt Entry
- Defaults credit card transaction type automatically based on sales document type and transaction history
- Provides encrypted storage and retrieval of multiple credit cards for each customer; and
- Provides batch mode processing of credit card transactions.

Credit Card Payment Process and Involved Entities

Merchant Accounts

Companies that accept credit card payments from customers will need to setup merchant accounts. These accounts are setup through banks and financial institutions and allow payments to be accepted and received from customers. This basically serves as a way of connecting a customer's bank account with the credit card processing network.

Payment Gateways

Companies that conduct business online will need payment gateways that enable them to accept online payments via credit card and ACH/eCheck.

Fees

There are costs that are associated with accepting payments online. Fees typically associated with payment gateways include discount rates, which are commissions taken from your customer's payment, and can range from two to six percent of the sale.

How do Credit Card Payments Process

1. The merchant submits a credit card transaction to the credit card Gateway on behalf of a customer.
2. Payment gateway receives the transaction and passes it via a secure connection to the merchant's bank processor.
3. The merchant bank's processor submits the transaction to the credit card network (a system of financial entities that communicate to manage the processing, clearing, and settlement of credit card transactions).
4. The credit card network routes the transaction to the customer's credit card issuing bank.
5. The customer's credit card issuing bank approves or declines the transaction based on the customer's available funds and passes the transaction results back to the credit card network.
6. The credit card network relays the transaction results to the merchant bank's processor.
7. The merchant bank's processor relays the transaction results to credit card gateway.
8. The customer's credit card issuing bank sends the appropriate funds for the transaction to the credit card network, which passes the funds to the merchant's bank. The bank then deposits the funds into the merchant's bank account. This step is known as the settlement process and typically the transaction funds are deposited into your primary bank account in two to four business days.



PCI Compliance

Properly securing credit card accounts and transaction information has become crucial for all companies that process or transmit credit card transactions. This is why Visa and other major credit card companies have formed the Payment Card Industry Security Standards Council (PCI SSC) with the goal in mind of protecting consumers, merchants and service providers.

To meet PCI DSS Compliance, companies need to meet 12 requirements that include building and maintaining a secure network, protecting cardholder data, maintaining a vulnerability management program, implementing strong access control measures, regularly monitoring and testing networks, and maintaining an information security policy.

Once a company is PCI Compliant, it makes it easier to gain customer trust and assurance that your site is safe. In addition, it also helps companies in the long-run avoid hefty fines that can run up to \$500,000 for not being PCI Compliant. Being PCI Compliant is beneficial and will help avoid:

1. Customer loss
2. Financial liabilities (fees and fines)
3. Reputation loss
4. Lose merchant account
5. Potential lawsuits

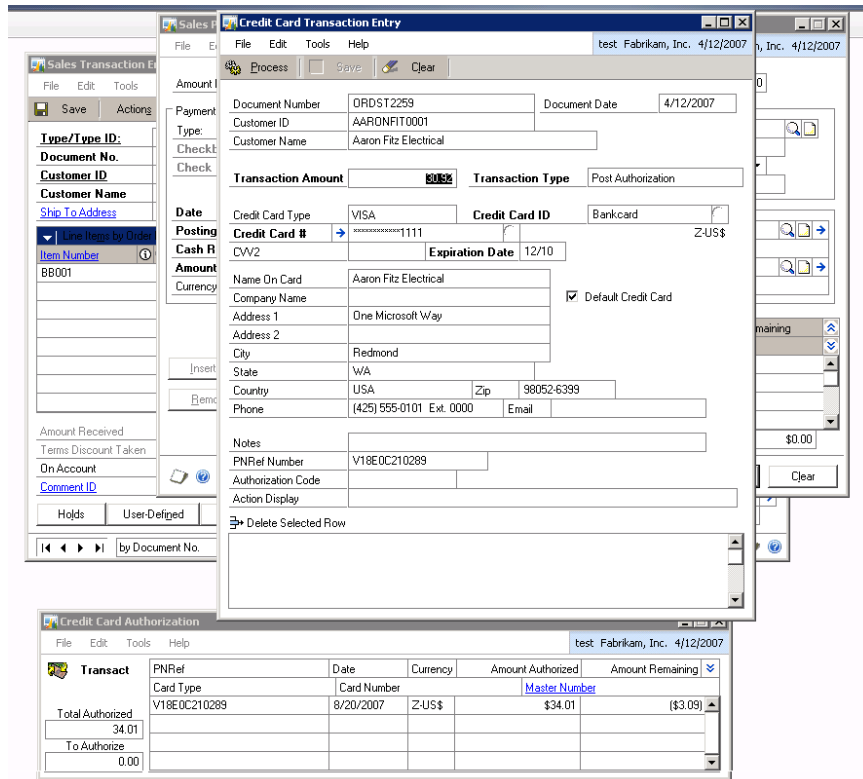
To read the full detailed self assessment questionnaire, visit the Payment Card Industry Security Standard Council website and download the assessment guide [here](#).

It's also important to note that to be compliant companies must also be using applications that are considered PA-DSS certified. To view a list of applications that are PA-DSS validated visit the PCI-SSC website [here](#).

Credit Card Extension

Background

Credit Card Extension (CCE) brings together payment gateways, processors and back-office systems to provide a highly secure and flexible credit card processing solution that is PA-DSS Certified. When using an ERP system like Microsoft Dynamics® GP, it can provide the ability to directly process credit cards immediately, which doesn't exist out of the box. We will explain how this application interacts and processes a credit card transaction through the credit card network later on the next page.



Integration Points

Credit Card Extension is a very flexible tool that can be integrated in a number of different ways. Credit Card Extension can be integrated with the following:

- Microsoft Dynamics® GP Sales Order Processing and Receivable Management modules
- K-eCommerce: B2B, B2C, and Sales Portal sites
- Multiple gateways
 - Authorize.Net
 - PPI – Paymover
 - Moneris
 - Admeris
 - PayPal Payflow Pro
 - CyberSource
 - Chase Paymentech
 - Global Payments
 - Beanstream
 - Sage

Credit Card Extension Data Flow

The diagram below represents the data flow between Credit Card Extension, the gateway, merchant's bank and credit card bank. The process is very similar to the illustration shown earlier.

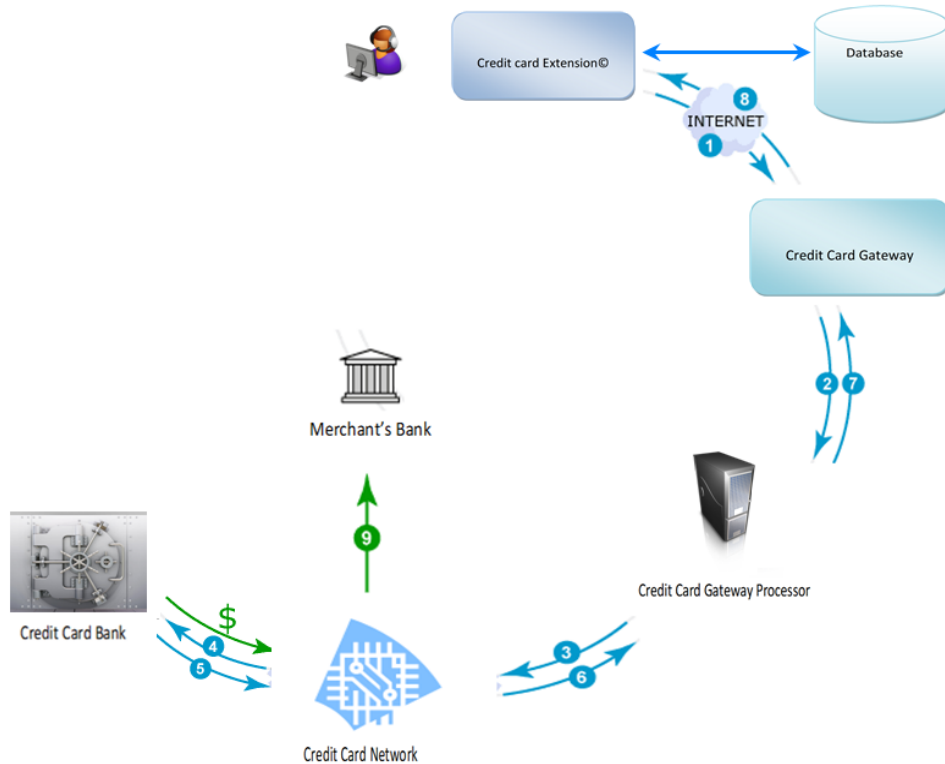


Figure 1: Credit Card Data Flow

1. The merchant submits a credit card transaction to the credit card gateway on behalf of a customer using Credit Card Extension.
2. Credit card gateway receives the transaction information and passes it via a secure connection to the merchant bank's processor.
3. The merchant bank's processor submits the transaction to the credit card network (a system of financial entities that communicate to manage the processing, clearing, and settlement of credit card transactions).
4. The credit card network routes the transaction to the customer's credit card issuing bank.
5. The customer's credit card issuing bank approves or declines the transaction based on the customer's available funds and passes the transaction results back to the credit card network.
6. The credit card network relays the transaction results to the merchant bank's processor.
7. The merchant bank's processor relays the transaction results to the credit card gateway.
8. The credit card gateway stores the transaction results and sends them to Credit Card Extension. Credit Card Extension stores the transaction results in the database and then displays it to the user.
9. The customer's credit card issuing bank sends the appropriate funds for the transaction to the credit card network, which passes the funds to the merchant's bank. The bank then deposits the funds into the merchant's bank account. This step is known as the settlement process and typically the transaction funds are deposited into your primary bank account within two to four business days.

Conclusion

Benefits of Credit Card Processing in Microsoft Dynamics® GP

With more and more companies wanting to reduce the time needed to collect invoice payments and increase cash flow, it makes sense from a business efficiency standpoint to utilize an ERP system to help facilitate the payment collection process and get paid faster. Keeping customer records and accounts all in one system makes it easier to access and manage information. Credit Card Extension has been developed to solve this problem by providing integrated credit card processing inside Microsoft Dynamics® GP.

Being secure when dealing with electronic transactions is another priority for organizations and that is why adhering to the PCI Compliance Standards is so important. By using software that is compliant, organizations can significantly help themselves along the path of gaining compliance.

To learn more about integrated payment processing visit www.k-ecommerce.com or call our team at 734-928-6004.

Glossary: Common Terms Associated With Payment Processing

There are numerous parties involved when it comes to processing credit card transactions whether payments are taken online or via phone. The following is a glossary of common credit card processing terms:

Merchant: The entity that is selling the goods or services.

Cardholder: The individual who is making a purchase using a credit card.

Payment Application: An application used by the merchant that stores, processes, or transmits credit card data.

Merchant Account: A bank or financial institution that allows businesses to charge and accept payments from customers that use credit cards. There are different merchant accounts that apply to different businesses. Some specialize in physical point of sale business and others may specialize in eCommerce. The banks accept the responsibility of transferring the funds from customers' credit cards to a business' checking account.

Payment Gateway: Connects online stores with their merchant account and corresponding payment processors.

Payment Processor: A payment processor is a company used by acquiring banks to route transactions to the appropriate bank card organizations for authorization and settlement.

PCI-SSC: Payment Card Industry Security Standards Council is the governing organization that oversees the PCI Data Security Standard (PCI-DSS) and the Payment Application Data Security Standard (PA-DSS).

PCI-DSS: Payment Card Industry Data Security Standards is a set of guidelines that provide requirements for security management, policies, procedures, network architecture, software design and other security measures related to information or card holder data.

PA-DSS: Payment Application Data Security Standard, formerly the Payment Applications Best Practices (PABP), is a set of global security guidelines established by the PCI-SSC to help software and other vendors develop payment applications that keep information safe and in compliance with the PCI-DSS.

Authorization: Process of verifying a credit card has sufficient funds that are available to cover the transaction cost.

Post-Authorization: Charges a credit card

Sale: Directly charges money on a customer credit card.

Void: A void is to cancel a post-authorization or sale transaction before it is settled and the funds have been transferred from the issuing bank to the customer's bank.

Issuing Bank: The issuing bank is the financial institution that holds the contractual agreement with the card holder and issues the card. The issuing bank holds an issuing license.

Batch: Group of captured credit card transactions in a merchant's terminal.

About k-eCommerce

k-eCommerce is dedicated to developing integrated eCommerce and ePayment solutions for Microsoft Dynamics® AX, GP, NAV and CRM as well as SAP® Business One. We develop fully integrated B2B, B2C, Sales Portal and mobile-optimized eCommerce websites. Our solutions are quick and easy to deploy on premise or in our private, PCI Certified cloud. k-eCommerce also provides secure PA-DSS certified credit card/ACH processing and an online bill pay portal.

- *Integrated eCommerce*
- *Responsive Online Experience*
- *Omni-Channel Solution*

For more information:
www.k-eCommerce.com
sales@k-eCommerce.com
734.928.6010