ICCARD

E-COMMERCE SOFTWARE FOR THE WORLD WIDE WEB
Copyright 2000 Frank E. Haggar / Haggar Consulting Corp., Version 1.8, Nov-2000

Frank Haggar
President
Haggar Consulting Corp
Phone: (561) 239-2486
Email: feh@bellsouth.net

Copyright Notification

Copyright© 2000, Frank E. Haggar / Haggar Consulting Corp.
All Rights Reserved. No part of this publication may be reproduced or transmitted
in any form or by any means without the written permission of Haggar Consulting Corp.

Haggar Consulting Corp. is not affiliated or associated with the following companies or their distributors:

Microsoft Corporation
CyberCash Inc.
Internet Billing Company
CyberSource Corp.
Netscape Communications
O'Reilly & Associates
Flicks Software
Amerinet, Inc.
EuroDebit
The Processing Network
International Commerce Solutions
AT&T's Bell Laboratories

Windows®, WinNT®, Win32®, IIs®, MS-Access®, and SQL Server®
are registered trademarks of Microsoft Corporation
iBill® and Web900® are registered trademarks of Internet Billing Company
Icverify® is a registered trademark of CyberCash Corp.
FastTrack® is the registered trademark of Netscape Communications
WebSite® is the registered trademark of O'Reilly & Associates
Authentix® is the registered trademark of Flicks Software
Telcash™ is a trademark, and debit-it® is a registered trademark of Amerinet, Inc.
ICSPayPoint™ is a trademark of International Commerce Solutions
Unix® is the registered trademark of AT&T's Bell Laboratories
Linux® is the registered trademark of Linus Torvaldis

and, not of Haggar Consulting Corp.

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Haggar Consulting cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Contents

©Copyright 2000, Frank E. Haggar / Haggar Consulting Corp.

1 FEATURES

Introduction

ICCard is an e-commerce software package that is fully capable of providing all the required functionality to perform third-party billing. The ICCard system processes transactions using "physical merchant accounts" for "logical clients". The transactions can be processed using either individual merchant accounts per client, or a group of clients can use a single merchant account. These transactions are then reported per-client, with separate logins per client to view statistics, etc.

This software also integrates with an ACH checking system to allow the acceptance of online checks for payments. All of the standard features accompanying credit card transactions are made available using online check payments (except AVS, since that is not offered in the USA by the ACH network)

ICCard processes Internet transactions in real-time, by interfacing to a variety of processing software and systems and implements fully automatic userid and password management. CGI programs are provided which can run on the remote system containing the password-protected content. These CGIs are called by the ICCard system to add/delete users as needed. The CGIs are easy to install and are compatible with any other previous or existing password management mechanisms.

Types of Payments

This software allows the website to process financial transactions using the following forms of payment:

- Credit cards
- Checking accounts via ACH
- Web 900® (pin codes)
- iBill™ subscriptions by referer
- iBill™ subscriptions by pin codes
- European checking accounts via ACH by EuroDebit

ACH Checking

This software also integrates with an ACH checking system to allow the acceptance of online checks for payments. All of the standard features accompanying credit card transactions are made available using online check payments (except AVS, since that is not offered in the USA by the ACH network).

©Copyright 2000, Frank E. Haggar / Haggar Consulting Corp.

Recurrent Billing / Billing Options

ICCard can perform automatic recurring billing, and a variety of billing options are available. These include free trial periods, paid trial periods, monthly recurring, and multi-monthly recurring. In addition, it is possible to purchase access for a single charge for a single amount for a single time frame (such as a 3 month period).

Real-Time Statistics

Real-time statistics are provided as well. The clients can see how many attempted transactions occurred, and why those transactions were screened or filtered prior to processing. In addition, there are statistics that indicate the transactions that were processed, and the results of that processing (approved/declined).

Fraud

There are also a wide variety of fraud control features. ICCard can take a variety of actions based on the AVS reply for a given transaction. Additional fraud screening features identify risky transactions based on transaction origination information, card issuer comparisons, etc.

Support for automatic use of CyberSource's fraud scoring is also provided. Email confirmation before a sale is accepted for settlement, and automatic receipts can be sent after the sale is processed.

Shopping Carts

ICCard can be integrated with shopping carts by accepting transactions via either HTTP/GET or HTTP/POST protocols. A standard reply can be returned upon approval, or informative replies are returned in all other circumstances.

Customer Support

ICCard includes a customer support GUI, which provides all of the features needed to handle membership and billing questions. In addition, a wide variety of features are provided to allow customer support staffers to offer maximum customer satisfaction to the cardholder.

Risk Management

ICCard's risk management features provide reports that can identify trends and help predict risk factors for recent transactions based on chargeback analysis.

Technical Details

ICCARD has been tested with, and is currently supporting the following servers in production environments:

- Website and Website/Pro, running under Windows 95 and WinNT
- Netscape FASTTRACK server, running under Windows 95 and WinNT
- Microsoft IIs Server running under Windows NT 4.0

ICCARD has also been tested with the following servers:

- Microsoft FrontPage Server

©Copyright 2000, Frank E. Haggar / Haggar Consulting Corp.

- Microsoft Personal Server

It is written in C to provide efficient, durable, and reliable operation.

ICCard uses ODBC to access data, and has been run in production modes with Microsoft Access (smaller operations) and Microsoft SQL Server (larger operations).

ICCARD can be integrated with popular gateways, or "ICVerify" which provides support for almost all Banks, financial institutions, and credit card processors. Customer can make purchases over the Internet by accepting the data from HTML forms, processing the transaction, and sending HTML output back to the Web browser.

Safe and secure administration capabilities are provided with a separate GUI application that manages customer accounts and transactions. Voids, Credits/Returns, and Credit Reversals are available along with the ability to cancel access to a service by removing the Customer's userid and password from a remote site, with a variety of scheduling options.

ICCARD automatically schedules and manages the periodic billing cycle by generating and processing transactions on a monthly basis. Any declined monthly charges are rescheduled up to 4 times, in a weekly fashion. Any charges which have not been approved prior to the next scheduled monthly rebill date will result in disconnection of service to the customer by removal of the userid.

The fillout data from all forms is stored into daily log files in ASCII format, and is used to produce statistical information on site activity, etc. This data is formatted in generic comma-separated, quote-delimited format, and can easily be imported or processed by other software products.

ODBC is also used to store the fillout information into an external database. Almost any ODBC-compliant database system can be supported. MS-Access is currently the default database format. A version for Microsoft SQL Server is also tested and supported.

Configuration settings can be used to control that records are to be stored into the ODBC database. The current set of values allows all records to be stored, all approved records to be stored, or all approved and all declined records to be stored.

A variety of views and summaries of transactional activity are available to the merchant with ICCARD. Additionally, ICCARD includes support for generating "custom" views or summaries in response to queries and requests in SQL format.

©Copyright 2000, Frank E. Haggar / Haggar Consulting Corp.

2 OVERVIEW

Processes

This credit card system's functionality is divided among five separate processes. The "Client," "Monitor," "Supervisor," and "Statistics" programs are designed to perform sales transactions by integration with a background "HOST," such as ICVerify's multi-user program or a supplied host that integrates with popular gateways. Each of these five programs is responsible for performing specific tasks. For example, the "Statistics" program allows merchants to view their transaction activity from a WEB Browser, the "Supervisor" program is run as a local application and can process credits/refunds, disconnect users, etc.

Separation of Responsibility

The separation of responsibility allows multiple WWW-based client processes to request credit card authorizations from a single PC system that is equipped with a single modem. This separation of responsibility also improves the security of the system by minimizing the "client" software's ability to handle sensitive data (such as precluding a remote user from creating credit transactions using a WWW Browser), and allows distribution of functionality across multiple machines to accommodate higher-volume processing.

Although it is technically reasonable to reduce the number of programs, doing so would inhibit the ability to run certain commands from another machine on a local network.

For example, the "monitor" program and the "supervisor" program could be combined into a single application, but this would inhibit the ability to use the "supervisor" capabilities across a local LAN. The "monitor" program displays CGI activity as it occurs on the server, and should only be run as a single instance.

The "supervisor" commands are transaction-oriented, and are implemented to run concurrently with CGI transaction activity in a multi-user shared database environment. Thus, the "supervisor" is perfectly capable of operating across a local area network (as long as the LAN and ODBC drivers are correctly configured on both machines).

Sales and Credits

"Sales" are submitted to the HOST by the "client" programs. The "client" is a CGI program, which is run whenever any customer fills and submits a form using their WEB Browser.

Credits are submitted to the HOST by the "supervisor" program. The "supervisor" is a Windows GUI application and must be run either on the server system, or on any local computer that has Local Area Network access to the server system.

©Copyright 2000, Frank E. Haggar / Haggar Consulting Corp.

Recurring Monthly Charges/Rebills

Recurring monthly charges (aka Rebills) are submitted to the HOST in a daily batch, by the "monitor" program. The "monitor" program runs on the server system, and should be launched automatically whenever the server system is started.

©Copyright 2000, Frank E. Haggar / Haggar Consulting Corp.

3 DESCRIPTION

Introduction

The following is a brief description of the responsibilities and functionality delegated to each of the five programs, the host, the client, the monitor, the supervisor, and the statistics.

The Host

The "HOST" program is either a gateway-specific program provided as part of this package, or the ICVERIFY "host" program, called ICVMUL32.EXE. The host needs to be running at all times.

When the client software (ICCARD.EXE) verifies the CGI data, the data will be sent to the gateway OR written to a file in a specific directory on the disk. The host software monitors that directory for input files. When an input file is detected, the contents of the file are extracted and used to perform an online credit card authorization. The results of this authorization are returned to the client program by writing the reply into another specific directory, which the client software monitors until the host's response is available.

The Client

The "client" program is called ICCARD.EXE. It is launched when a remote user's WEB Browser software submits input data that was filled into an HTML form. The ICCARD.EXE program parses the CGI-formatted input data into fields and values. It then performs various preliminary verification tests on the fields and the data values associated with those fields. A reply is generated, which is formatted into an HTML document.

If the data is incomplete or fails any of the preliminary verification tests, the client software will format a response that contains instructions on how to correct the erroneous or missing data. If the data satisfies all of the requirements, it will be passed on to the host software for further processing. The resulting response from the host will be returned to the WWW Browser software as a reply for the remote user.

The Monitor

The "monitor" program is called MONITOR.EXE. As this program's name suggests, its main use is to monitor and display information representing the "client" CGI activity. Another VERY important feature of the monitor program is to handle any scheduled tasks on a daily basis. Thus, the monitor program will clean up any temporary data in 24-hour cycles. The monitor program is also responsible for the daily rebilling procedures.

The Supervisor

The "supervisor" program is called CREDIT.EXE. As the program's name suggests, it's main use and most significant purpose is to provide an authorized supervisor a mechanism for producing "credit" transactions. The credit card supervisor program can display the authorization information that the host program generates. That information can then be used to create a credit transaction, and can be searched for all activity for a particular credit card number, userid/script, user name, or even a typed-in SQL statement.

©Copyright 2000, Frank E. Haggar / Haggar Consulting Corp.

The Statistics

The "statistics" functionality is actually performed by five separate CGI executables. The SHOWHITS.EXE program processes the transaction logs, which contain a record of all successfully submitted forms' data. The LOGHITS.EXE program performs similar functions on a per-merchant (client id) basis. Depending on the configured options, some or all of this data is stored in an ODBC database.

The SHOWODBC.EXE program produces a report that is similar in layout and contents to the SHOWHITS.EXE output, but SHOWODBC.EXE uses SQL to extract the information from the ODBC database (instead of reading the transaction log files).

The GETQUERY.EXE program accepts generic SQL Query for a specified DataSet Name (DSN), and dynamically generates an HTML table from the names and contents of the fields. The RUNQUERY.EXE performs similar functions to GETQUERY.EXE, but runs off of pre-determined SQL statements and is merchant (client-id) specific.

©Copyright 2000, Frank E. Haggar / Haggar Consulting Corp.

4 FUNCTIONALITY

The Host Program

The “Host” program contains gateway specific host software, and ICVERIFY host software. They perform unique functions.

The gateway-specific "host" software performs the following functions:

- Scanning for request files containing information in ICVerify format, parsing those files
- Connecting to the gateway and sending the transaction data.
- Formatting and returning error messages, informational instructions, or approval results to the WWW Browser based on the results obtained from the gateway-specific host.
- Processing batch input files for rebilling when submitted by the "monitor" program

The ICVERIFY "host" software performs the following functions:

- Scanning for request files containing information in ICVerify format, parsing those files
- Dialing the modem and performing online transactions with the credit card processor using their specific data formats
- Recording the authorized transactions for later settlement
- Processing the result of an online authorization request and generating an appropriate response for the client program to analyze and format into a reply that is returned to the WWW Browser. (The "LONG EVALUATED REPLY" option is required.)
- Automatically performing daily settlements for the authorized transactions.
- -Processing batch input files for rebilling when submitted by the "monitor" program

The Client Software

The "client" software performs the following functions:

- Parsing the CGI input data from the WWW Browser and identifying data fields and their values

©Copyright 2000, Frank E. Haggar / Haggar Consulting Corp.

- Locating key environment variables and extracting/storing these values in the database as part of the transaction.

- Performing preliminary data verification to insure the HTML form has been adequately filled and that the data supplied is acceptable. This includes date-of-birth testing, LUHN Mod10 checksum of the credit card number, verification of a non-zero amount, verification of a script, verification of the credit card's expiration date, verification of a unique USERID for the specific script's system, etc.

- Submitting an acceptable input request to either the gateway, or to the ICVerify "host" for online authorization

- Monitoring for a response from the gateway or the ICVerify host, and cleanly handling situations where ICVerify or the gateway does not respond within a reasonable amount of time

- Formatting and returning error messages, informational instructions, or approval results to the WWW Browser based on the results obtained from the gateway or ICVerify host

- Recording a list of credit cards that have been approved or declined within the last 24 hours, and scanning that list to identify and avoid duplicate authorizations or multiple declines for the same card number

- Recording a local list of script/credit card/USERID/password information as authorization requests are approved, and using this list to determine previously added USERID/PASSWORD information a given script/card combination. This information is used to prevent multiple USERID/PASSWORDS from being added by the same individual for the same script using the same card. The previous USERID/PASSWORD is presented to the customer, overriding any attempt to add secondary USERIDs. This list is temporary, and is reset every 24 hours

- Recording a local list of all USERIDs added for each script as card authorization requests are approved, to allow an expedient check for the uniqueness of a new USERID without the overhead of connecting to the ODBC database to perform a query lookup. This list is permanent, and will not be reset automatically.

- Adding records to an ODBC database for approved transactions. It is also possible to set configuration options that cause the client software to store declined transactions, or all transactions, into the ODBC database.

- Recording daily log files of all submitted form transaction data.

©Copyright 2000, Frank E. Haggar / Haggar Consulting Corp.

The Supervisor Software

The "supervisor" software performs the following functions:

- Displaying views of transactions, searching for specific credit card number transactions, sorting daily transactions by date, card number, script/service, amount, etc
- Generating credit transactions and submitting them to the "host"
- Scheduling the discontinuation of service and removal of the userid/password.

The Monitor Software

The "monitor" software performs the following functions:

- Displaying a view of CGI "client" activity as it occurs
- Presenting elapsed time values for the "monitor" session and an estimated summary of sales, etc
- Automatic daily searching of the ODBC customer database and generating an offline batch for any records that are to be rebilled monthly. The periodic billing cycle will be used as a multiplier to determine the exact amount to authorize, which can be monthly, quarterly, semi-annually, or annually.

  The billing cycle value is currently hardcoded as monthly, but the code's calculation logic supports these other values. The other billing cycle values could easily be added as a new field in the ODBC database if and when we determine the need for support of other than monthly billing.
- Producing reports on the daily ODBC rebilling batch generation. These reports identify invalid card numbers, expired cards, invalid amounts, invalid billing period values, etc.
- Automatic scanning the ODBC database for any records that have been marked for "disconnection" and launching a subtask that will remove these userids from the corresponding password files

©Copyright 2000, Frank E. Haggar / Haggar Consulting Corp.

5 AUTOMATED PROCEDURES

Launching

This section will explain the procedure to launch the ICVERIFY host and MONITOR.EXE program.

Launching the ICVERIFY host (ICVMLT32.EXE) and MONITOR.EXE program:

The current bootstrap procedure is to have the system startup launch the host by placing ICVMLT32.EXE and MONITOR.EXE on the StartUp menu under Win95, or in the STARTUP GROUP under WinNT. One problem with this solution is that on Windows NT, Program Manager will not run until a user logs in. Thus, UNDER Windows NT, you must login before Program Manager opens and initializes it's STARTUP GROUP, which in turn causes ICVMLT32.EXE and MONITOR.EXE to be run.

Starting multiple copies of ICVMLT32.EXE is dangerous, because both running copies will attempt to process any input files that are placed into the input directory. Due to the frequency of checking for input files, it's possible that both running hosts will detect the file, and then both hosts may attempt to process the file and dial the modem at the same time. If so, one of the hosts will block the use of the modem from the other.

(ICVERIFY strongly recommends avoiding starting multiple instances of ICVMLT32.EXE!)

Automatic Batch Rebillings

This section will explain the automatic batch rebillings of ICVERIFY-formatted monthly reoccurring billing data, and automatic processing of the ICVERIFY-formatted response file.
All records containing unacceptable data (such as credit card numbers which do not pass a LUHN Mod10 checksum test) will be placed into a RBYYMMDD.ERR file and will be indicated as invalid in the RBYYMMDD.RPT report.

All expired cards will be submitted with an expiration date of that is incremented one year up from the original expiration date. Any expiration dates that are older than one year will then use the expiration date of "0000". Both of these situations will be identified in the RBYYMMDD.RPT file by the term EXPIRE-FIX or with the term EXPIRED and zero-filled expiration date information, respectively.

Automatic disconnections and removals

Automatic disconnection and removal of UserID/Passwords on the date specified by the ActionDate of the database's transaction record for all records specifically marked to be disconnected on or before that date.

©Copyright 2000, Frank E. Haggar / Haggar Consulting Corp.

INDEX

©Copyright 2000, Frank E. Haggar / Haggar Consulting Corp.