Othentik's Credit Push Online Payment Solution:

Efficiency Through Simplicity

Solution Overview

13 December 2004

OTHENTIK Technologies Inc.
5000 Iberville St; Suite 304
Montreal, Quebec
Canada H2H 2S6

Telephone: (514) 333-0550
Fax: (514) 336-2112
e-mail: info@othentik.com
www.othentik.com

CONFIDENTIALITY

This document is proprietary to OTHENTIK Technologies, Inc. and is to be treated on a confidential basis. It may be used solely for purposes approved by OTHENTIK Technologies, Inc.

Use or disclosure of the document, or the information contained therein, for any other purposes is not permitted without prior written authorization.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Othentik Technologies, Inc. provides financial institutions, merchants and consumers with an online payment solution that enables the consumer to "push" a payment to a merchant's bank account through an online banking interaction. Also known as "credit-push" for ACH payments in the U.S., this new online payment option offers the assurances and convenience of online banking access to facilitate secure use of demand deposit accounts (DDAs) for purchases over the Internet. Merchants receive payments expeditiously, guaranteed through the buyer's own bank's authentication processes.

Patent protection for Othentik's unique business process solution for Credit Push payments was filed in May 2000*. The platform support and security for the system is suitable for the rigors and demands of banking network operation.

The Othentik solution facilitates and leverages the investments by financial institutions in their online banking infrastructures. This unique, intuitive, flexible and secure solution covers the full spectrum of needs when it comes to sales of products and services related to business-to-business (B2B) and business-to-consumer (B2C) transactions, as well as person-to-person funds transfers (P2P).

Othentik signed Non Disclosure Agreements (NDA) with some major players in the financial area.

As of today Bank Of America is the only FI with whom Othentik signed an NDA. Due to confidentialy agreements, we are not authorized to disclose the other companie's name.

- B2B: (3.600 Trillion $ in 2003, Gartner Group)
  - ✓ EIPP
  - ✓ B2G
- B2C: (1.06 Trillion $ in 2003, Fortune)
  - ✓ EBPP
- P2P: (37 Billion $ in 2003, Celent)
  - ✓ C2C

**See Intellectual Property Section.*

Consumer

- Buys over the Internet;
- Already has a trusted relationship with the financial institution;
- Needs a secure and reassuring payment option

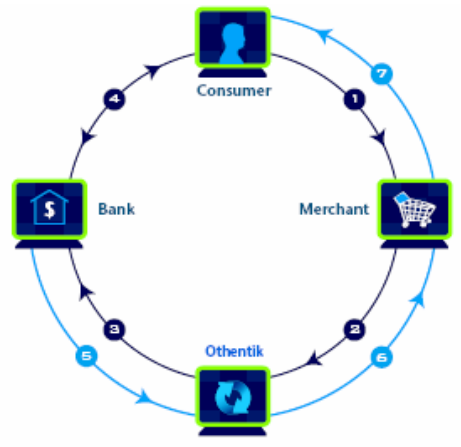
Merchant

- Looking for a simple and cost effective way to sell its products and services over the Internet;
- Wants to capitalize on existing infrastructures and notoriety;
- Needs a reliable confirmation and fast payment

Financial Institution

- Already offering e-banking to its consumers;
- Wants to expand its offering with a direct online payment proprietary solution;
- Built on actual infrastructure to minimize risk and optimize return on investment (ROI).

WHAT HAPPENS DURING AN ONLINE TRANSACTION?



OTHENTIK SOLUTION FLOW CHART

Any person or business with access to their financial institution's online banking services can participate directly with the Othentik system if their financial institution is enabled for use of the product with participating merchants.

Othentik software system authenticates the buyer's payment with the holder of his payment account — typically a financial institution. The holder of the account then collects the funds from that account and pays the seller (a merchant or a biller) privately and securely. In this solution all the parties to the transaction are fully secured and fully satisfied in a natural and logical way.

TRANSACTION PROCESSING STEPS

1. The consumer makes the purchase, is presented the bill by the merchant, selects the Othentik payment method (HTTP POST), and chooses the financial institution through which the payment is to be made—all occuring on the merchant's check-out and payment webpage.
2. These purchase parameters are forwarded from the merchant's proxy or transaction server to Othentik's transaction server via a simple API .
3. Othentik transmits the transaction details to the consumer's financial institution.
4. The consumer logs into the financial institution's online banking website, recovers bill to be paid, and approves of payment by consumer.
5. Transmission of confirmation of transaction completion to Othentik transaction server.
6. Real-time confirmation of transaction completion to merchant.
7. Confirmation of payment by merchant and triggering of shipment; closing of transaction.

CONSUMER INTERFACE

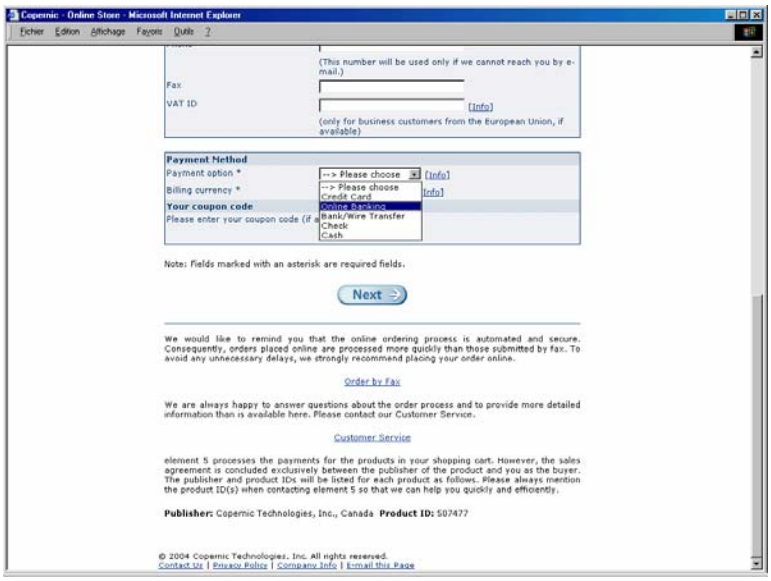
No Plug-in is required by Othentik's solution. We never install any software on customer side. Everything is based on HTML redirection concept. The normal browser it self is the only soft required for the customer.

Following are the five steps of consumer's interaction for payment over the Internet.

Step 1 of 5

To settle an invoice or to pay for an online purchase, the consumer first identifies the financial institution from which the payment is to be made from a selected drop down menu on the merchant's Website.

Figure 1

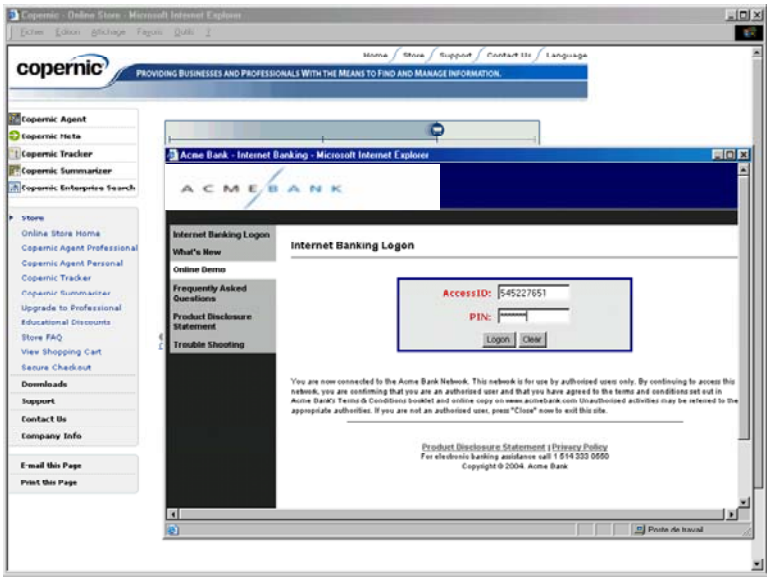


Screens are for illustration purposes only.

Step 2 of 5

The consumer is then redirected from his or her browser to the selected financial institution's secure environment, where log-in can commence, using the normal online banking username and password for authentication.

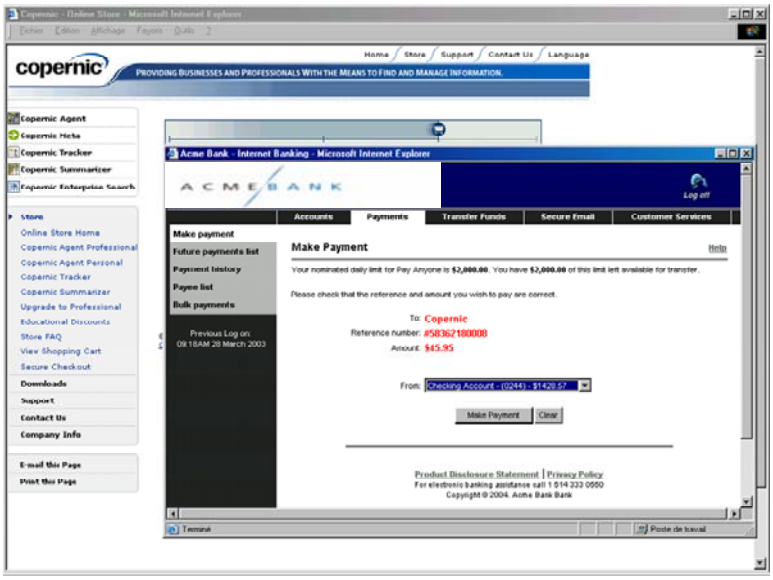
Figure 2



Step 3 of 5

The customer selects the type of account (checking, savings, or credit card) from which to make payment for the online purchase.

Figure 3

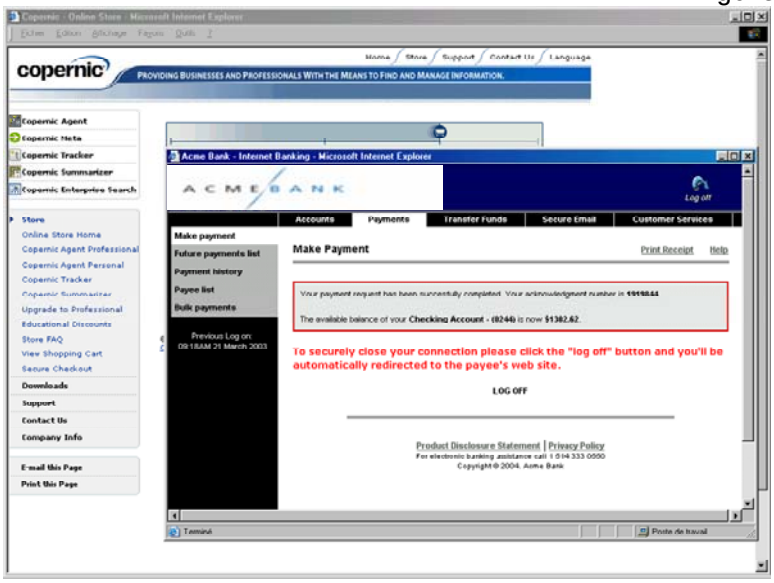


Screens are for illustration purposes only.

Step 4 of 5

When the transaction is completed, a confirmation number is issued certifying that the consumer's payment has been authorized.

Figure 4

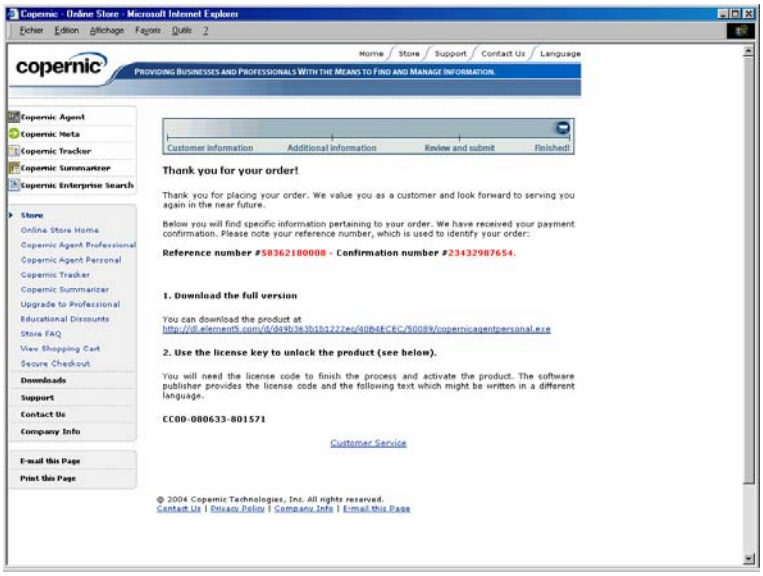


Step 5 of 5

Real-time confirmation of payment status is sent to the merchant.

The consumer's financial institution transfers the funds to the merchant's financial institution through established processing relationships.

Figure 5



Screens are for illustration purposes only.

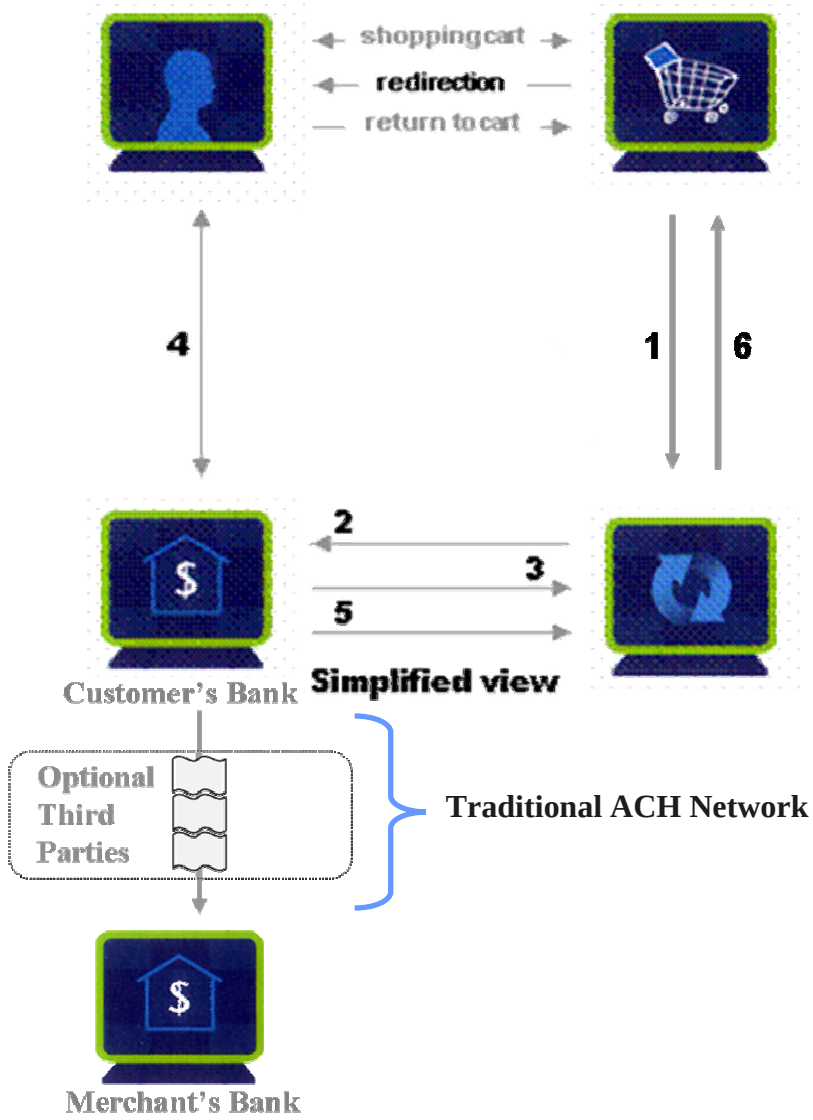
OTHENTIK SOLUTION BACK OFFICE PROCESS

Othentik's solution uses Internet Protocol (IP) and makes use of the http redirection feature on consumer browser.

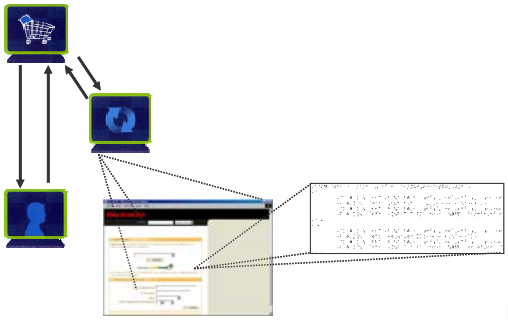
The consumer fills his or her shopping cart on the merchant web site. The customer is now ready to finalize his order.

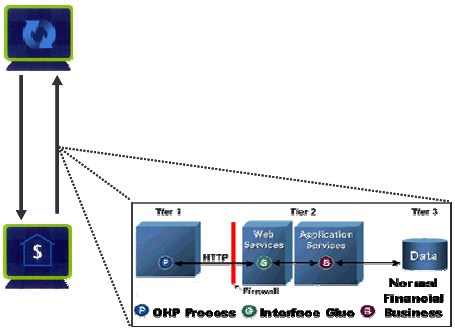
The e-merchant presents the invoice with a payment method selection.

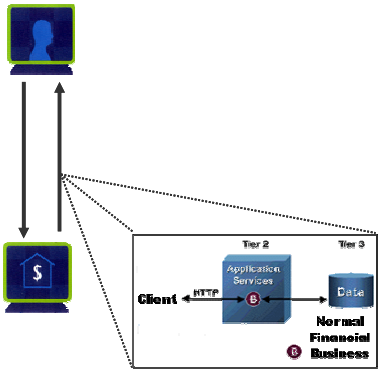
As shown below the process includes six steps:



Screens are for illustration purposes only.







Screens are for illustration purposes only.

BACK-OFFICE PROCESSING STEPS

Step 1 of 6: A normal "http post" is sent to the Othentik system with all parameters required for starting the transactional cycle. No confidential information about the customer is provided to Othentik's system. The "http post" on the merchant Website provides to start the business transaction server. It makes it possible to implement the system for any merchant size (convenience store, …).

Step 2 of 6: The Othentik system validates all parameters and requests the selected financial institution to create an anonymous transaction.

Step 3 of 6: The financial institution sends to Othentik system a specific "url" for the payment and unique, encrypted data "BLOB" containing the transaction identification.

The communication layer between Othentik system and the financial institution is performed using the SSL protocol in mutual authentication mode. All information transmitted to the financial institution must be crypt and securised (SET, SSL, Elliptic cryptography…). Only Othentik and the financial institution are able to open the stored data. All sensitive informations are kept in centralized data basis. In order to identify the merchant/issuer and the financial institution an ID is assigned at the subscription. ID's are used for communication with parties.

Step 4 of 6: The customer is "redirected" to the selected financial institution's specific "url" attached to the "data BLOB" containing the transaction identification.

The financial institution proceeds to the authentication phase and associates the anonymous transaction to the consumer account.

The consumer chooses the payment method: checking account, credit line, credit card, saving account, etc.

Step 5 of 6: Upon consumer logoff, the financial institution "redirects" the consumer to the Othentik system with the "data BLOB" identification.

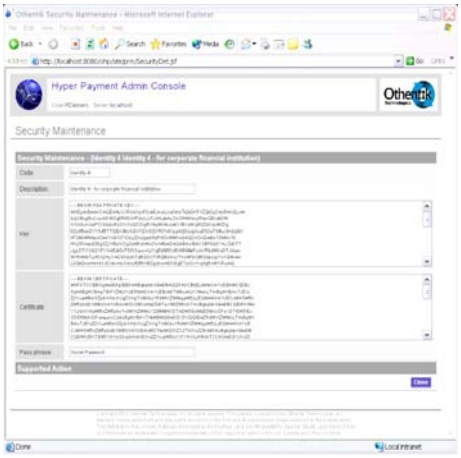
Othentik solution synchronizes the transaction status and completes the transaction transparently.

Step 6 of 6: The Othentik system makes the final "re-direction" to the merchant with the confirmation of the transaction. The transactional cycle is completed. The merchant can also make a request to Othentik to know the transaction status via any security protocol.

Authorization Response Message API is stored in transaction reports data bases. These informations make it possible to communicate statistics and data consolidation to participant merchants upon request.

When the "Credit Push" (HTTP POST) option is selected , the request info is sent to Othentik´s gateway (OLB) which simply redirects the customer to the selected financial institution. Othentik´s gateway formats data, communicates with financial institution, redirects customer,…

All communications with the financial institution are done under SSL protocol (mutual authentication mode). No plugin needed, no software added.



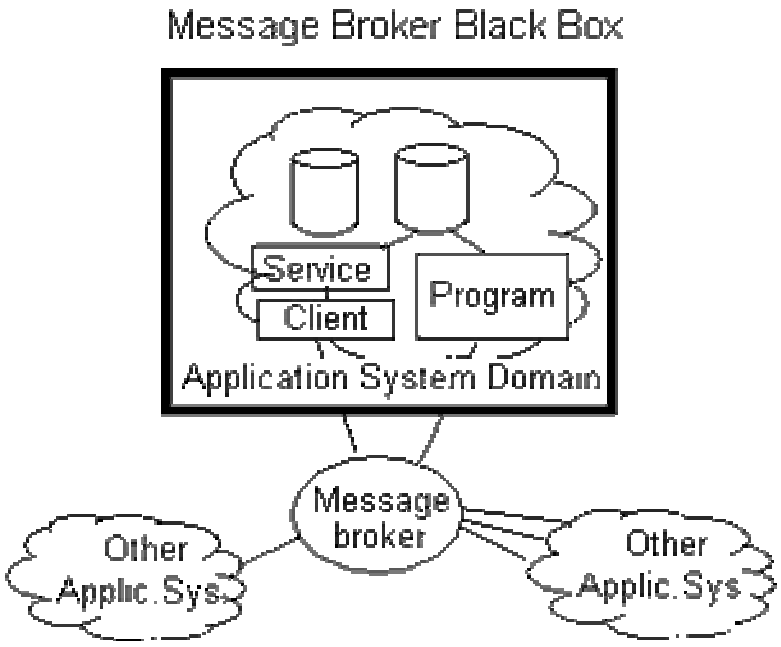
Screens are for illustration purposes only.

THE SYSTEM

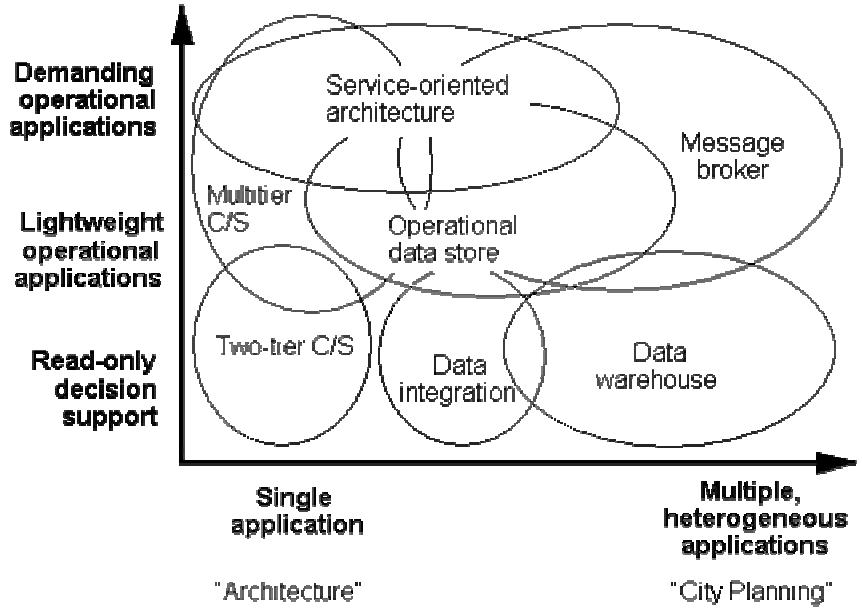
All parameters required to operate Othentik's Credit Push solution are embedded in a complete web application.

The application is used to configure all parameters required for operation: merchant maintenance, financial institution maintenance, communication protocol, security configuration, etc.

The message broker nature of the system is illustrated below:



Our technological orientation makes it possible not only to adapt to and support multiple applications but also to apply demanding operational applications as illustrated by the following graph:



Source: Gartner Group

COMMUNICATION SECURITY

Confidentiality and security of all transactions are the cornerstone of our solution.

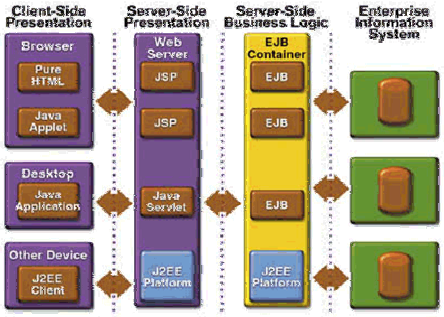
All communication between Othentik's platform and the financial institution are performed under the SSL layer with mutual authentication.

For this purpose, Othentik's application manages a X.509 certificate by point of service.

The transactional identification "data BLOB" is protected with the use of advanced cryptographic software, timestamp and digital signature; only the participating financial institution can understand the transactional "data BLOB" identification.

Screens are for illustration purposes only.

J2EE Software architecture



• CLIENT TIER: This layer represents the two system user's types. The user "consumer" is who uses the system in order to obtain a service. The user "owner" is who exploits/configure the system for the users/ consumers. Typically under J2ee architecture, the consumer uses a standard browser.

• MIDDLE TIER: The Client Tier can be one or more applications or browsers. The J2EE Platform is in the Middle Tier and consists of a Web Server and an EJB Server. These servers are also called "containers." There can be additional sub-tiers in the middle tier. The software layer is divided into several segments. The segment "Web container" is mainly used to interact with the users. Othentik's solution exploits this segment in order to offer the services to consumers. Segment "EJB Container" is the segment offering an access to the external services/functionalities. Typically used within the framework of interface for the accesses: base data, ERP (High volume), transfers inter systems, etc.

• EIS TIER: The Enterprise Information System (EIS) tier has the existing applications, files, and databases.

Screens are for illustration purposes only.

TECHNOLOGY

Othentik's Web application is built in compliance with rapidly evolving state of the art web-based technology.

Othentik believes in and fully supports Java 2 technology and the payment application is fully J2EE compliant.

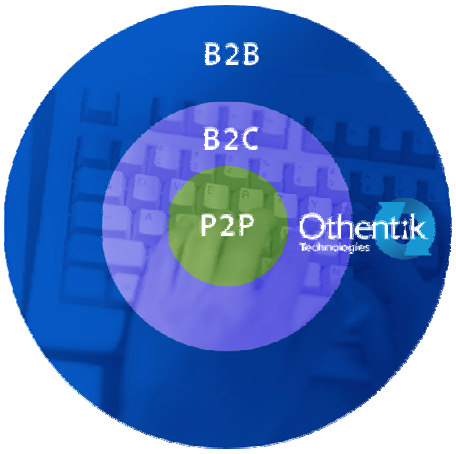
The solution is based on: Java language with Jce extension (strong encryption), Strut Framework and Java server faces (GUI).

Database access is conducted with an object relational mapping (ORM) available through the Hibernate product.

This allows Othentik's application to be ported on any of the following databases:

RDBMS	
DB2	Microsoft SQL Server
DB2 AS/400	SAP DB
DB2 OS390	Informix
PostgreSQL	HypersonicSQL
MySQL	Ingres
Oracle (any version)	Progress
Oracle 9/10g	Mckoi SQL
Sybase	Interbase
Sybase Anywhere	Pointbase
FrontBase	Firebird

Addressing the full e-commerce spectrum



- Real-Time Processing
- Easy to use for consumer, no software to download, needs just a browser
- Easy to integrate for merchant (no software to install other than a simple plug-in API)
- Straightforward for the financial institution (with a plug-in module for the online banking platform to adjudicate and match transactions and route payments to the merchants)
- Solid and reliable
- Built for high volume
- Respect security standards

SUMMARY: Efficiency through simplicity

Othentik is a Montreal-based company which as been in business since 2000. Othentik is privately funded by patient investors with the wherewithal and commitment to ensure long-term adoption of this product.

OTHENTIK's vision is to become the leader in the field of online payment and make Credit Push the standard means of payment processing via the Internet, and in so doing, promoting the growth and success of its clients.

OTHENTIK intends that its customers will consider it as the premier specialized firm in the e-commerce A2A market when it comes to B2B, B2C, B2G and the support of P2P direct payment solutions.

At OTHENTIK TECHNOLOGIES, we are committed to the idea that the best solutions are those for which a need is expressed by consumers. By remaining closely attuned to market realities while investing for the future, we are assured of satisfying our customers.

Othentik's solution is fully suitable to online banking systems. In case of any changes to banking systems, Othentik's solution adapts to new changes without any notification, corruption data, service interruption or any changes on the merchant website. Working like a bridge, adaptation is fast and natural.

Othentik's Credit Push Solution presents the following characteristics:

FUNCTIONALITIES

• Supporting any structure that is compliant with the Internet communication protocol using connector interface

• Compatibility with online banking interfaces

• Corroboration process

• Archiving of all system operations data

• Easy interfacing with existing financial systems

KEY FEATURES

• Optimum security, meeting the most stringent criteria on the market

• Flexible and adaptable, with an intuitive interface

• Modular structure, adapts to TCP/IP communications

• POST method, Webservice Method or any legacy communication system over the Internet

• Internet, PDA, Mobile-trade, etc.

• Manages parameters for banks, businesses and merchants

• Centralized processing

• Transaction monitoring

• Supports accounting systems

• Othentik never accesses in contact with private banking information

INTELLECTUAL PROPERTY

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 November 2001 (15.11.2001)

PCT

(10) International Publication Number
WO 01/86523 A2

(51) International Patent Classification[7]: G06F 17/60

(21) International Application Number: PCT/IB01/00761

(22) International Filing Date: 3 May 2001 (03.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/202,159 5 May 2000 (05.05.2000) US
60/207,751 30 May 2000 (30.05.2000) US

(71) Applicant and
(72) Inventor: **RIOUX, Patrick** [CA/CA]; 200 Montee Ste. Anne, Beauharnois, Quebec J6N 3B8 (CA).

(74) Agent: **FINCHAM, Eric**; 316 ch. Knowlton, Lac Brome, Quebec J0E 1V0 (CA).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with declaration under Article 17(2)(a); without abstract; title not checked by the International Searching Authority*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/86523 A2

(54) Title: METHOD OF CONDUCTING FINANCIAL TRANSACTIONS OVER THE INTERNET

(57) Abstract:

METHOD OF CONDUCTING FINANCIAL TRANSACTIONS OVER THE INTERNET

The present invention relates to e-commerce and more particularly, relates to a method and system for payment when shopping on the web without using a credit card.

The use of the world wide web (the web) for shopping has been increasing at an exponential rate and is forecast to continue this growth for a number of years. Typically, the consumer will look for the wares or goods which they wish to purchase and then either directly, or through an agent, visit the web site of the seller. The purchases can typically be completed by clicking on the items desired, paying for the goods by providing credit card information following which the goods are shipped to the consumer.

A problem associated with shopping on the web is that a valid credit card must be available to the consumer. In many instances, this is not possible either due to the age of the consumer and/or a poor credit rating. Thus, there is a large potential group of consumers which are not able to buy over the web even if they have the money to do so. The alternative is that the consumer must send in a cheque or money order and then wait for the cheque or money order to clear and then receive the goods. This is a long and time consuming process not presenting any advantages over the old economy mail order business.

Even when the consumer does have a credit card, there is a great deal of concern over giving this information via the web. The element of fraud is ever